CRÉDIT AGRICOLE ASSICURAZIONI

CA Assicurazioni S.p.A.

Modello di organizzazione, gestione e controllo *ex* D.Lgs. 231/2001

DICEMBRE 2012

PARTE GENERALE

INDICE

DEFINIZIONI

- "Attività Sensibili": le attività di Credit Agricole Assicurazioni S.p.a. nel cui ambito sussiste il rischio di commissione dei Reati.
- "CCNL": il Contratto Collettivo Nazionale di Lavoro (contratto delle imprese di assicurazione) attualmente in vigore ed applicato da CAA.
- "CAA" o la "Società": Credit Agricole Assicurazioni S.p.a. con sede legale in Pordenone, Piazza XX Settembre, 2 e sede amministrativa in Milano, Piazza G. Missori, 2.
- "Compliance Officer": soggetto incaricato di valutare, coerentemente con quanto disposto dalla normativa regolamentare ISVAP (Regolamento n.20 del 26 marzo 2008 recante "Disposizioni in materia di controlli interni, gestione dei rischi, *compliance* ed esternalizzazione delle attività delle imprese di assicurazione, ai sensi degli articoli 87 e 191, comma 1, del decreto legislativo 7 settembre 2005, n.209 – codice delle assicurazioni private"), che l'organizzazione e le procedure interne della Società siano idonee a prevenire il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite patrimoniali o danni di reputazione, in conseguenza di violazioni di leggi, regolamenti o provvedimenti delle Autorità di vigilanza ovvero di norme di autoregolamentazione.
- "Consulenti": coloro che agiscono in nome e/o per conto di CAA sulla base di un mandato ovvero coloro che collaborano con la Società in forza di un contratto di collaborazione di qualsiasi natura.
- "Decreto Sicurezza": il decreto legislativo 9 aprile 2008, n.81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro".
- "Destinatari": i Dipendenti, i Dipendenti di per i servizi prestati a CAA in virtù dei contratti di servizio, i Consulenti, la Rete Distributiva, i Partner e gli Organi Sociali della Società.
- "Dipendenti": tutti i dipendenti di CAA (compresi i dirigenti).

- "D.Lgs. 231/2001" o "Decreto": il Decreto Legislativo n. 231 dell'8 giugno 2001 e successive modifiche ed integrazioni.

- "Esponenti Aziendali": gli Organi Sociali e i Dipendenti della Società.

- "Gruppo Cariparma Crédit Agricole", "Gruppo Cariparma": Cariparma S.p.a. (e le società da questa controllate), Friuladria S.p.A. e Cassa di Risparmio della Spezia S.p.A..

- "Linee Guida ANIA": le Linee Guida ANIA per la costruzione dei modelli di organizzazione, gestione e controllo *ex* D. Lgs. 231/2001 aggiornate al 18 marzo 2008.

- "Modello": il modello di organizzazione, gestione e controllo previsto dal D.Lgs. 231/2001.

- "Operazione Sensibile": operazione o atto che si colloca nell'ambito delle Attività Sensibili.

- "Organi Sociali": i membri del Consiglio di Amministrazione e del Collegio Sindacale di CAA.

- "Organismo di Vigilanza" o "OdV": organismo interno preposto alla vigilanza sul funzionamento e sull'osservanza del Modello (come qui di seguito definito) e al relativo aggiornamento.

- "P.A.": la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio:

- "Partner": controparti contrattuali di CAA, quali ad es. fornitori, distributori, ecc. sia persone fisiche sia persone giuridiche, con cui la società addivenga ad una qualunque forma di collaborazione contrattualmente regolata (associazione temporanea d'impresa - ATI, *joint venture*, consorzi, ecc.), ove destinati a cooperare con la società nell'ambito dei Attività Sensibili.

- "Reati": i reati ai quali si applica la disciplina prevista dal D. Lgs. 231/2001.

- "Rete Distributiva": i soggetti con i quali CAA ha stipulato specifici mandati/accordi per la distribuzione dei propri prodotti.

- Credit Agricole Vita S.p.A. (CA Vita) che svolge attività in ambito di servizi amministrativo-contabili, corporate governante legale e reclami, risorse umane,

marketing e commerciale, finanza, facility management, organizzazione ed IT, risk management, internal audit e compliance in favore di CAA.

CAPITOLO 1

IL REGIME DI RESPONSABILITÀ AMMINISTRATIVA PREVISTO A CARICO DELLE PERSONE GIURIDICHE, SOCIETÀ ED ASSOCIAZIONI

1.1 Il Decreto Legislativo n. 231/2001 e la normativa di riferimento

In data 4 luglio 2001, in attuazione della delega di cui all'art. 11 della legge 29 settembre 2000 n. 300, è entrato in vigore il Decreto Legislativo 8 giugno 2001, n. 231, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" – pubblicato in Gazzetta Ufficiale n. 140, del 13 giugno 2001, Serie Generale.

Scopo del Decreto era adeguare l'ordinamento giuridico interno ad alcune convenzioni internazionali, cui l'Italia aveva aderito, quali la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità Europee, la Convenzione di Bruxelles del 26 maggio 1997 sulla lotta alla corruzione in cui sono coinvolti funzionari della Comunità Europea e degli Stati Membri e la Convenzione OCSE del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche e internazionali.

Esaminando nel dettaglio il contenuto del D.Lgs. 231/2001, l'articolo 5, comma 1, sancisce la responsabilità della società qualora determinati reati (reati cd. presupposto) siano stati commessi nel suo interesse o a suo vantaggio:

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

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

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

Sotto il profilo sanzionatorio, per tutti gli illeciti commessi è sempre prevista a carico della persona giuridica l'applicazione di una sanzione pecuniaria; per le ipotesi di maggiore gravità è prevista anche l'applicazione di sanzioni interdittive, quali

l'interdizione dall'esercizio dell'attività, la sospensione o la revoca di autorizzazioni, licenze o concessioni, il divieto di contrarre con la P.A., l'esclusione da finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni e servizi.

La responsabilità prevista dal suddetto Decreto si configura anche in relazione ai reati commessi all'estero, purché per gli stessi non proceda lo Stato del luogo in cui è stato commesso il reato medesimo.

Quanto alla tipologia dei reati destinati a comportare il suddetto regime di responsabilità amministrativa, il Decreto - nel suo testo originario - si riferiva ad una serie di reati commessi nei rapporti con la Pubblica Amministrazione.

Successivamente, l'art. 6, L. 23 novembre 2001, n. 409, recante "Disposizioni urgenti in vista dell'introduzione dell'euro", ha inserito nell'ambito del Decreto l'art. 25-*bis*, che mira a punire il reato di "falsità in monete, in carte di pubblico credito e in valori di bollo".

In seguito, l'art. 3, D.Lgs. 11 aprile 2002, n. 61, in vigore dal 16 aprile 2002, ha introdotto il nuovo art. 25-*ter* del D.Lgs 231/2001, estendendo il regime di responsabilità anche ai c.d. reati Societari, così come configurati dallo stesso Decreto n. 61/2002.

L'art. 3, L. 14 gennaio 2003, n. 7, ha, poi, introdotto l'art. 25-*quater*, il quale dispone la punibilità dell'ente per i delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali. Mentre l'art. 25-*quinquies*, introdotto dall'art. 5, L. 11 agosto 2003, n. 228, ha esteso la responsabilità ai reati contro la personalità individuale.

L'art. 9 della L. 18 aprile 2005, n. 62 (di seguito la "Legge Comunitaria 2004") ha, inoltre, inserito l'art. 25-sexies volto ad estendere la responsabilità ai nuovi reati di abuso di informazioni privilegiate e di manipolazione del mercato.

La Legge Comunitaria 2004 ha, inoltre, modificato il TUF introducendo una specifica disposizione, l'art. 187–*quinquies*, ai sensi della quale la società è responsabile del pagamento di una somma pari all'importo della sanzione amministrativa irrogata per gli illeciti amministrativi di abuso di informazioni privilegiate (art. 187-bis TUF) e di manipolazione del mercato (art. 187-*ter* TUF) commessi nel suo interesse o a suo vantaggio da: a) persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria

o funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

La L. 28 dicembre 2005, n. 262 ("Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari") ha poi integrato e modificato sia il TUF sia il Codice Civile, introducendo, tra l'altro, il nuovo art. 2629-*bis* cod. civ. relativo al reato di "Omessa comunicazione del conflitto di interessi", applicabile esclusivamente alle società quotate. Tale reato è stato introdotto, ad opera della medesima legge n. 262/2005, nell'art. 25-*ter* del D.Lgs. 231/2001.

Successivamente, con Legge 16 marzo 2006, n. 146 di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati rispettivamente il 15 novembre 2000 ed il 31 maggio 2001, la responsabilità amministrativa degli Enti è stata estesa, ai sensi dell'art. 10, ad alcune tipologie di reati, purché commessi a livello transnazionale.

Ai sensi dell'art. 3 della Legge 16 marzo 2006, n. 146, si considera "transnazionale" il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

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

Con la Legge 3 agosto 2007, n. 123, recante "Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia" è stato introdotto nel Decreto l'art. 25-septies, come sostituito nella sua attuale stesura dall'art. 300, D.Lgs. 9 aprile 2008, n. 81, che ha esteso il novero dei reati cd. presupposto all'omicidio colposo ed alle lesioni colpose gravi o gravissime commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

In seguito, il D.Lgs. n. 231/07 di recepimento 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 ha inserito nel Decreto, ai sensi

dell'art. 63, comma 3, l'art. 25-octies che include nel catalogo dei Reati anche la ricettazione, riciclaggio ed impiego di denaro, beni o utilità di provenienza illecita.

Infine, per effetto dell'entrata in vigore della Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione del Consiglio di Europa sulla criminalità informatica sottoscritta a Budapest il 23 novembre 2001, è stato introdotto nel Decreto l'art. 24 – bis che estende l'elenco dei Reati ai cd. delitti informatici.

Ad oggi, quindi, tra i reati cd. presupposto sono contemplati:

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

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

(iii) i reati societari;

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

(v) i reati contro la personalità individuale;

(vi) i reati e gli illeciti amministrativi di abuso di mercato;

(vii) i reati transnazionali;

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

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

(x) i delitti informatici e il trattamento illecito dei dati;

(xi) i reati di frode in commercio;

(xii) i reati di contraffazione;

(xiii) i reati di criminalità organizzata;

(xiv) il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.

1.2 L'adozione "modello di organizzazione, gestione e controllo" quale possibile esimente dalla responsabilità amministrativa.

L'articolo 6 del Decreto introduce una particolare forma di esonero dalla responsabilità in oggetto qualora la società dimostri:

a) di aver adottato ed efficacemente attuato attraverso il suo organo dirigente, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;

b) di aver affidato ad un organismo interno, dotato di autonomi poteri di iniziativa e di controllo, il compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curare il loro aggiornamento;

c) che le persone che hanno commesso il reato hanno agito eludendo fraudolentemente il suddetto Modello;

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

Il Decreto prevede, inoltre, che – in relazione all'estensione dei poteri delegati ed al rischio di commissione dei reati – il Modello debba rispondere alle seguenti esigenze:

1. individuare le aree a rischio di commissione dei reati previsti dal Decreto;
2. predisporre specifici protocolli al fine di programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
3. prevedere modalità di individuazione e di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
4. prescrivere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
5. configurare un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Lo stesso Decreto dispone che il Modello può essere adottato, garantendo le esigenze di cui sopra, sulla base di codici di comportamento (i. e. "Linee Guida") redatti da associazioni rappresentative di categoria.

CAPITOLO 2

ADOZIONE DEL MODELLO DA PARTE DI CAA.

2.1 Adozione del Modello.

Il presente Modello è stato adottato dal Consiglio di Amministrazione di CAA con delibera del 12 marzo 2009. Con la medesima delibera è stato istituito l'Organismo di Vigilanza cui è attribuito il compito di vigilare sul funzionamento, sull'efficacia e sull'osservanza del Modello stesso, nonché di curarne l'aggiornamento.

CAA è una compagnia di bancassicurazione che ha per oggetto l'esercizio dell'attività assicurativa, in particolare la collocazione di prodotti assicurativi, quali ad esempio l'auto, l'abitazione, gli infortuni, attraverso il Gruppo Cariparma, rivolgendosi ai clienti di Cariparma e Friuladria, reti bancarie del Gruppo Crédit Agricole, con l'obiettivo di ampliare la tradizionale offerta bancaria.

2.1.1 Le Linee Guida ANIA.

Nella predisposizione del presente Modello CAA si è ispirata alle Linee Guida ANIA per il settore assicurativo quale utile strumento di orientamento per l'interpretazione e l'analisi delle implicazioni giuridiche ed organizzative derivanti dall'introduzione del D.Lgs. 231/2001.

I punti fondamentali individuati dalle Linee Guida ANIA per la costruzione dei Modelli possono essere così sintetizzati:

- individuazione delle **aree di rischio**, volta a verificare in quale area/settore aziendale sia possibile la realizzazione dei Reati;
- previsione di obblighi di **informazione** dell'organismo di vigilanza, volti a soddisfare l'attività di controllo sul funzionamento, l'efficacia e l'osservanza del Modello;
- predisposizione di un **sistema di controllo** ragionevolmente in grado di prevenire o ridurre il rischio di commissione dei Reati attraverso l'adozione di appositi protocolli/procedure. A tal fine soccorre l'insieme ben coordinato di strutture organizzative, attività e regole attuate – su impulso dell'organo decisionale – dal management e dal personale aziendale, volto a fornire una ragionevole sicurezza in merito al raggiungimento delle finalità rientranti nelle seguenti categorie:

- efficacia ed efficienza delle operazioni gestionali;
- adeguato controllo dei rischi;
- attendibilità delle informazioni aziendali, sia verso terzi sia all'interno;
- salvaguardia del patrimonio;
- conformità alle leggi, regolamenti, norme e politiche interne.

In particolare, le componenti più rilevanti del sistema di controllo possono essere individuate nei seguenti elementi:

- codice etico e codici di comportamento,
- sistema organizzativo, procedure manuali ed informatiche;
- poteri autorizzativi e di firma;
- sistemi di controllo e gestione;
- comunicazione al personale;
- formazione del personale;
- meccanismi disciplinari.

Le componenti del sistema di controllo devono essere informate ai seguenti principi:

- verificabilità, documentabilità, coerenza e congruenza di ogni operazione;
- applicazione del principio di separazione delle funzioni (nessuno può gestire in autonomia un intero processo);
- applicazione di regole e criteri improntate a principi di trasparenza;
- documentazione dei controlli;
- previsione di un adeguato sistema sanzionatorio per la violazione delle regole e delle procedure previste dal Modello;
- individuazione dei requisiti dell'organismo di vigilanza, riassumibili come segue (e come sarà meglio specificato al Capitolo 4 della presente Parte Generale del Modello):

- autonomia e indipendenza;
- professionalità;
- continuità di azione;
- assenza di cause di incompatibilità, di conflitti di interesse o rapporti di parentela con gli organi di vertice.

Va comunque considerato che, essendo il settore assicurativo soggetto a specifica e capillare vigilanza, l'attenta applicazione della normativa di settore costituisce già un primo strumento di salvaguardia della Società.

Inoltre, nell'ambito dei gruppi assicurativi, rimangono fermi i principi dell'autonomia e delle responsabilità proprie di qualunque società. Conseguentemente ciascuna di esse sarà tenuta ad adottare un proprio Modello e ad individuare un proprio Organismo di Vigilanza. E' possibile tuttavia che, all'interno del gruppo, vengano adottate forme di comportamento sostanzialmente univoche, pur nel rispetto delle peculiarità connesse ai diversi settori merceologici di appartenenza dei singoli enti.

2.2 Funzione e scopo del Modello.

CAA è sensibile alle aspettative dei propri azionisti e degli *stakeholders* ed è altresì consapevole del valore che agli stessi può derivare da un sistema di controllo interno idoneo a prevenire la commissione di reati da parte dei propri Dipendenti, Organi Sociali, Rete Distributiva, Consulenti e Partner.

L'adozione e l'efficace attuazione del Modello migliorano il sistema di *Corporate Governance* della Società in quanto limitano il rischio di commissione dei reati e consentono di beneficiare dell'esimente prevista dal D.Lgs. 231/2001, pertanto, scopo del presente Modello è la predisposizione di un sistema strutturato ed organico di prevenzione, dissuasione e controllo finalizzato alla riduzione del rischio di commissione dei Reati mediante l'individuazione di attività sensibili e dei principi di comportamento che devono essere rispettati dai Destinatari. A tal fine viene individuata e descritta la costante attività dell'Organismo di Vigilanza finalizzata a garantire il rispetto del sistema organizzativo adottato e la vigilanza sull'operato dei Destinatari, anche attraverso il ricorso ad idonei strumenti sanzionatori, sia disciplinari che contrattuali.

I principi contenuti nel presente Modello sono volti, da un lato, a determinare una piena consapevolezza del potenziale autore del Reato di commettere un illecito (la cui commissione è fortemente condannata da CAA perché contraria alle norme di deontologia cui essa di ispira e ai suoi interessi, anche quando apparentemente la Società potrebbe trarne un vantaggio), dall'altro, grazie ad un monitoraggio costante dell'attività, a consentire a CAA di reagire tempestivamente nel prevenire od impedire la commissione del Reato stesso.

Tra le finalità del Modello vi è, quindi, quella di sviluppare nei Dipendenti, negli Organi Sociali, nella Rete Distributiva, nei Consulenti e nei Partner che operano nell'ambito delle Attività Sensibili e, pertanto, dei Destinatari in generale, la consapevolezza di poter determinare - in caso di comportamenti non conformi alle prescrizioni del Modello e alle altre norme e procedure aziendali (oltre che alla legge) - illeciti passibili di conseguenze penalmente rilevanti non solo per se stessi, ma anche per la Società.

A tal riguardo, le procedure aziendali già adottate e quelle di futura emanazione, così come i principi procedurali indicati nel presente Modello, si caratterizzano per:

- separazione all'interno di ciascun processo tra il soggetto che lo inizia, e/o lo esegue ed il soggetto che lo controlla;
- traccia scritta di ciascun passaggio rilevante del processo;
- adeguato livello di formalizzazione.

2.3 La costruzione del Modello e la sua struttura.

La predisposizione del presente Modello è stata preceduta da una serie di attività preparatorie, suddivise in differenti fasi, tutte finalizzate alla costruzione di un sistema di prevenzione e gestione dei rischi in linea e ispirato, oltre che alle norme contenute nel D.Lgs. 231/2001, anche ai contenuti e suggerimenti dettati dalle Linee Guida ANIA e alla *best practice* italiana esistente.

Si riporta qui di seguito una breve descrizione delle fasi in cui si è articolato il lavoro di individuazione delle aree a rischio, a seguito delle quali si è poi giunti alla predisposizione del presente Modello:

1. Identificazione delle Attività Sensibili ("as-is analysis").

Tale fase di identificazione delle Attività Sensibili è stata attuata attraverso due distinte attività:

a) esame preliminare della documentazione aziendale, tra cui a titolo esemplificativo: organigramma societario, statuto sociale, verbali di consiglio del amministrazione (in particolare relativi al conferimento di deleghe e procure), procedure aziendali su tematiche sensibili in relazione ai reati previsti dal Decreto (es. redazione del bilancio, gestione dei rapporti commerciali, rapporti con i fornitori, documentazione in tema di sicurezza sul lavoro (ad es., nomina del RSPP, DVR, procedure di sicurezza, verbali di riunione periodica sulla sicurezza), codice etico, ecc.;

b) interviste ai soggetti chiave della struttura aziendale mirate all'approfondimento dei processi sensibili e del controllo sugli stessi (procedure esistenti, verificabilità, documentabilità, congruenza e coerenza delle operazioni, separazione delle responsabilità, documentabilità dei controlli, ecc.) tra cui, a titolo esemplificativo: Presidente, Amministratore Delegato, Direttori delle principali funzioni aziendali (e, in particolare, i responsabili delle funzioni di controllo, affari legali, funzioni coinvolte nella redazione di scritture contabili, ecc.).

E' stata, inoltre, portata a termine una ricognizione sulla passata attività della Società allo scopo di verificare l'esistenza di eventuali situazioni a rischio e le relative cause. Sono state altresì esaminate le procedure aziendali già adottate e attuate dalla Società.

2. Effettuazione della "Gap Analysis".

Sulla base della situazione aziendale esistente nella Società a seguito della "*as-is analysis*" (Attività Sensibili individuate e descrizione delle criticità in esse riscontrate) e alla luce delle previsioni e finalità del D.Lgs. 231/2001, sono state individuate le azioni di miglioramento da attuare nell'ambito delle Attività Sensibili sia a livello di procedure interne che di requisiti organizzativi al fine di pervenire alla definizione per la Società del Modello *ex* D.Lgs.231/01.

I risultati dell'analisi svolta sia nella fase di "Identificazione delle Attività Sensibili" che in quella di "Effettuazione della *Gap Analysis*" sono stati riassunti in un documento all'uopo predisposto (cd. "*Analisi dei Rischi e Suggerimenti*").

3. Predisposizione del Modello.

Il presente Modello è costituito dai seguenti documenti:

i. una "Parte Generale", contenente l'insieme delle regole e dei principi generali dettati dal Modello;

ii. n. 8 "Parti Speciali" predisposte per alcune diverse categorie di reato contemplate nel D.Lgs. 231/2001 e astrattamente ipotizzabili in relazione all'attività svolta dalla Società,ossia:

- "Parte Speciale A", denominata "Reati commessi nei rapporti con la Pubblica Amministrazione", la quale riguarda le tipologie specifiche di Reati previste ai sensi degli artt. 24 e 25 del D.Lgs. 231/2001;
- "Parte Speciale B", denominata "Reati Societari", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 25-*ter* del D.Lgs. 231/2001.
- "Parte Speciale C", denominata "Reati di terrorismo e di eversione dell'ordine democratico", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 25-*quater* del D.Lgs. 231/2001.
- "Parte Speciale. D", denominata "Reati contro la personalità individuale", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 25-*quinquies* del D.Lgs. 231/2001.
- "Parte Speciale E", denominata "Reati ed illeciti amministrativi di abuso di mercato", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 25-*sexies* del D.Lgs. 231/2001.
- "Parte Speciale F", denominata "Reati di Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 25-*septies* del D.Lgs. 231/2001.
- "Parte Speciale G", denominata "Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 25-*octies* del D.Lgs. 231/2001.
- "Parte Speciale. H", denominata "Delitti informatici e trattamento illecito di dati", la quale è dedicata alle tipologie specifiche di Reati previste ai sensi dell'art. 24-*bis* del D.Lgs. 231/2001.

- "Parte Speciale I", denominata "Delitti di criminalità organizzata";

- "Parte Speciale L", denominata "Delitti contro l'industria e il commercio e reati di contraffazione".

2.4 Principi generali cui si ispira il Modello

Nella predisposizione del presente Modello si è tenuto conto delle procedure e dei sistemi di controllo operanti in azienda (rilevati in fase di "*as-is analysis*"), ove considerati idonei a valere anche come misure di prevenzione dei Reati e strumenti di controllo sulle Attività Sensibili. Detto Modello si pone, pertanto, quale ulteriore componente del sistema di controllo interno adottato dalla Società.

In particolare, quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni della Società anche in relazione ai Reati da prevenire, CAA ha individuato i seguenti:

1) i principi di *corporate governance* generalmente seguiti dalla Società;

2) il Codice Etico adottato dalla Società con deliberazione del Consiglio di Amministrazione del 18 dicembre 2008;

3) la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale e organizzativa della Società;

4) la normativa aziendale che la Società ha predisposto nell'ambito delle Attività Sensibili (ad esempio, procedure per la gestione dei rapporti con la P.A., procedure per la redazione delle scritture contabili, documentazione aziendale in materia di sicurezza sul lavoro, ecc.);

5) la formazione del personale e della Rete Distributiva;

6) il sistema sanzionatorio di cui al CCNL.

Le regole, procedure e principi di cui agli strumenti sopra elencati, non vengono riportati dettagliatamente nel presente Modello, ma fanno parte del più ampio sistema di organizzazione e controllo che lo stesso intende integrare.

Principi cardine cui il Modello si ispira, oltre a quanto sopra indicato, sono:

1. le Linee Guida ANIA e la *best practice* italiana esistente in materia, in base alle quali è stata predisposta la mappatura delle **Attività Sensibili** di CAA;

2. i requisiti indicati dal D.Lgs. 231/2001 ed in particolare:
    - l'attribuzione ad un **organismo di vigilanza** interno a CAA del compito di attuare in modo efficace e corretto il Modello anche attraverso il monitoraggio dei comportamenti aziendali ed il diritto ad una informazione costante sulle attività rilevanti ai fini del D.Lgs. 231/2001;
    - la messa a disposizione dell'organismo di vigilanza di **risorse aziendali** di numero e valore ragionevole e proporzionato ai compiti affidatigli e ai risultati attesi e ragionevolmente ottenibili;
    - l'attività di **verifica del funzionamento** del Modello con conseguente aggiornamento periodico (controllo *ex post*);
    - l'attività di **sensibilizzazione e diffusione** a tutti i livelli aziendali delle regole comportamentali e delle procedure istituite;
3. i principi generali di un adeguato sistema di controllo interno ed in particolare:
    - la **verificabilità e documentabilità** di ogni operazione rilevante ai fini del D.Lgs. 231/2001;
    - il rispetto del principio della **separazione delle funzioni**;
    - la definizione di **poteri autorizzativi** coerenti con le responsabilità assegnate;
    - la **comunicazione all'organismo di vigilanza** delle informazioni rilevanti;
4. il sistema dei controlli interni che monitora le aree in cui vi è un'alta probabilità di commissione dei Reati ed un alto valore dello Operazioni Sensibili.

2.5 Il sistema dei controlli interni

Il sistema dei controlli interni in essere presso la Società si caratterizza per la presenza dei seguenti organi e funzioni:

a) Collegio Sindacale;

b) Controllo contabile;

c) Funzione di Compliance;

d) Funzione Internal Audit;

e) Funzione Risk Management..

a) Collegio sindacale

Il Collegio Sindacale esercita le funzioni previste dall'art. 2403 codice civile, e si compone di tre Sindaci Effettivi e due Supplenti nominati dall'assemblea per tre esercizi.

Tutti i componenti il Collegio Sindacale devono possedere i requisiti richiesti dalle vigenti disposizioni di legge e regolamenti.

L'assemblea provvede anche alla designazione del Presidente del Collegio Sindacale e a quant'altro occorra, sempre a termini di legge.

Ai sindaci è attribuito un compenso fissato dall'assemblea.

Le riunioni del Collegio Sindacale possono svolgersi per tele o videoconferenza.

Inoltre, ai sensi del Regolamento ISVAP 26 marzo 2008, n. 20, il Collegio Sindacale:

a) acquisisce, all'inizio del mandato, conoscenze sull'assetto organizzativo aziendale ed esamina i risultati del lavoro della società di revisione per la valutazione del sistema di controllo interno e del sistema amministrativo contabile;

b) verifica l'idoneità della definizione delle deleghe, nonché l'adeguatezza dell'assetto organizzativo prestando particolare attenzione alla separazione di responsabilità nei compiti e nelle funzioni;

c) valuta l'efficienza e l'efficacia del sistema dei controlli interni, con particolare riguardo all'operato della funzione di revisione interna della quale deve verificare la sussistenza della necessaria autonomia, indipendenza e funzionalità;

d) mantiene un adeguato collegamento con la funzione di revisione interna;

e) cura il tempestivo scambio con la società di revisione dei dati e delle informazioni rilevanti per l'espletamento dei propri compiti, esaminando anche le periodiche relazioni della società di revisione;

f) segnala all'organo amministrativo le eventuali anomalie o debolezze dell'assetto organizzativo e del sistema dei controlli interni indicando e sollecitando idonee misure correttive; nel corso del mandato pianifica e svolge, anche coordinandosi con la società

di revisione, periodici interventi di vigilanza volti ad accertare se le carenze o anomalie segnalate siano state superate e se, rispetto a quanto verificato all'inizio del mandato, siano intervenute significative modifiche dell'operatività della società che impongano un adeguamento dell'assetto organizzativo e del sistema dei controlli interni;

g) assicura i collegamenti funzionali ed informativi con gli organi di controllo delle altre imprese appartenenti al medesimo gruppo assicurativo;

h) conserva una adeguata evidenza delle osservazioni e delle proposte formulate e della successiva attività di verifica dell'attuazione delle eventuali misure correttive.

b) Controllo contabile

Tale controllo, ai sensi dello Statuto della Società, è affidato ad una società di revisione ai sensi dell'art. 2409-bis c.c.

c) Funzione di Compliance

Introdotta con Regolamento ISVAP 26 marzo 2008, n. 20, recante "Disposizioni in materia di controlli interni, gestione dei rischi, compliance ed esternalizzazione delle attività delle imprese di assicurazione, ai sensi degli articoli 87 e 191, comma 1, del decreto legislativo 7 settembre 2005, n.209 – codice delle assicurazioni private", con la funzione di verificare che l'organizzazione e le procedure interne della Società siano idonee a prevenire il rischio di incorrere in sanzioni giudiziarie o amministrative, perdite patrimoniali o danni di reputazione, in conseguenza di violazioni di leggi, regolamenti o provvedimenti delle Autorità di vigilanza ovvero di norme di autoregolamentazione.

In ottemperanza alle previsioni regolamentari di settore la funzione *Compliance svolge* i seguenti compiti:

- identificare in via continuativa le norme applicabili all'impresa di assicurazione e valutare il loro impatto sui processi e le procedure aziendali;
- valutare l'adeguatezza e l'efficacia delle misure organizzative adottate per la prevenzione del rischio di non conformità alle norme e proporre le modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio del rischio;

- valutare l'efficacia degli adeguamenti organizzativi conseguenti alle modifiche suggerite;
- predisporre adeguati flussi informativi diretti agli organi sociali dell'impresa e alle altre strutture coinvolte.

La funzione di Compliance presenta agli organi aziendali, con periodicità almeno annuale, le relazioni sull'attività svolta che illustrano le verifiche effettuate e i risultati emersi nonché le misure adottate per rimediare a eventuali carenze rilevate e le attività pianificate.

d) Funzione di Revisione Interna (o Internal Audit)

La funzione di revisione interna deve presentare le seguenti caratteristiche:

a) la collocazione della funzione nell'ambito della struttura organizzativa deve essere tale da garantirne l'indipendenza e l'autonomia, affinché non ne sia compromessa l'obiettività di giudizio; la funzione di revisione interna non dipende gerarchicamente da alcun responsabile di aree operative; ai soggetti preposti alla funzione di revisione interna non devono essere affidate responsabilità operative o incarichi di verifica di attività per le quali abbiano avuto in precedenza autorità o responsabilità se non sia trascorso un ragionevole periodo di tempo;

b) il responsabile della funzione è nominato dall'organo amministrativo: egli deve avere

specifica competenza e professionalità per lo svolgimento dell'attività; i compiti attribuiti al responsabile della funzione sono chiaramente definiti ed approvati con delibera del consiglio, che ne fissa anche poteri, responsabilità e modalità di reportistica all' organo amministrativo stesso;

c) agli incaricati della funzione deve essere consentita libertà di accesso a tutte le strutture aziendali e alla documentazione relativa all'area aziendale oggetto di verifica, incluse le informazioni utili per la verifica dell'adeguatezza dei controlli svolti sulle funzioni aziendali esternalizzate;

d) la funzione deve avere collegamenti organici con tutti i centri titolari di funzioni di controllo interno; il responsabile della funzione è dotato dell'autorità necessaria a garantire l'indipendenza della stessa;

e) la struttura dedicata deve essere adeguata in termini di risorse umane e tecnologiche alle dimensioni dell'impresa ed agli obiettivi di sviluppo che la stessa intende perseguire.

Gli addetti alla struttura devono possedere competenze specialistiche e deve essere curato l'aggiornamento professionale.

La funzione di revisione interna uniforma la propria attività agli standard professionali comunemente accettati a livello nazionale ed internazionale e verifica:

a) i processi gestionali e le procedure organizzative;

b) la regolarità e la funzionalità dei flussi informativi tra settori aziendali;

c) l'adeguatezza dei sistemi informativi e la loro affidabilità affinché non sia inficiata la qualità delle informazioni sulle quali il vertice aziendale basa le proprie decisioni;

d) la rispondenza dei processi amministrativo contabili a criteri di correttezza e di regolare tenuta della contabilità;

e) l'efficienza dei controlli svolti sulle attività esternalizzate.

La funzione di revisione interna pianifica, inoltre, l'attività in modo da identificare le aree da sottoporre prioritariamente ad audit. Il piano di audit è sottoposto all'approvazione dell'organo amministrativo e individua, almeno, le attività a rischio, le operazioni e i sistemi da verificare, descrivendo i criteri sulla base dei quali questi sono stati selezionati e specificando le risorse necessarie all'esecuzione del piano. Analogo procedimento è seguito in caso di variazioni significative ai piani approvati, che comunque sono organizzati in modo da fronteggiare le esigenze impreviste.

A seguito dell'analisi sull'attività oggetto di controllo, la funzione procede, secondo le modalità e la periodicità fissata dall'organo amministrativo, a rispettare idonei flussi informativi verso il vertice aziendale.

e) Funzione di Risk Management

La funzione di *Risk Management* svolge le seguenti attività:

a) concorre alla definizione delle metodologie di misurazione dei rischi;

b) concorre alla definizione dei limiti operativi assegnati alle strutture operative e definisce le procedure per la tempestiva verifica dei limiti medesimi;

c) valida i flussi informativi necessari ad assicurare il tempestivo controllo delle esposizioni ai rischi e l'immediata rilevazione delle anomalie riscontrate nell'operatività;

d) predispone la reportistica nei confronti dell'organo amministrativo, dell'alta direzione e dei responsabili delle strutture operative circa l'evoluzione dei rischi e la violazione dei limiti operativi fissati;

e) verifica la coerenza dei modelli di misurazione dei rischi con l'operatività svolta dall'impresa;

f) concorre all'effettuazione di ulteriori presidi di controllo (ad esempio, le prove di *stress test*).

Le funzioni *Compliance*, *Internal Audit* e *Risk Management* sono presenti in CAA a fronte di un contratto di servizi con Credit Agricole Vita S.p.a..

2.6 La procedura di adozione del Modello

Sebbene l'adozione del Modello sia prevista dalla legge come facoltativa e non obbligatoria, CAA ha ritenuto comunque necessario procedere alla predisposizione del presente Modello, la cui adozione è sottoposta a deliberazione del Consiglio di Amministrazione.

Essendo il Modello un atto di emanazione dell'organo dirigente (in conformità alle prescrizioni dell'art. 6, comma 1, lettera a) del D.Lgs. 231/2001) le successive modifiche e integrazioni sono rimesse alla competenza del Consiglio di Amministrazione di CAA, salva la facoltà di quest'ultimo di delegare per le modifiche di minor entità l'Amministratore Delegato, sentito l'Organismo di Vigilanza.

Il Consiglio di Amministrazione delibera annualmente sulla eventuale ratifica di tutte le modifiche e le integrazioni che siano state apportate dall'Amministratore Delegato, sentito l'Organismo di Vigilanza. La pendenza della ratifica da parte del Consiglio di Amministrazione non sospende, tuttavia, l'efficacia provvisoria delle modifiche e delle integrazioni nel frattempo apportate dall'Amministratore Delegato.

2.7 Destinatari del Modello

Le regole contenute nel presente Modello si rivolgono:

a) alle persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Società;

b) alle persone che esercitano, anche di fatto, la gestione ed il controllo della Società stessa;

c) a tutti i dipendenti della Società sottoposti alla direzione o alla vigilanza dei soggetti di cui sopra;

d) limitatamente a quanto specificamente indicato nei relativi accordi contrattuali, ai Consulenti, Partner (commerciali/finanziari), Fornitori, agenti, procuratori e, in genere, ai terzi che operano per conto o comunque nell'interesse della Società.

Il Modello ed i contenuti dello stesso sono comunicati ai soggetti interessati con modalità idonee ad assicurarne l'effettiva conoscenza, secondo quanto indicato al successivo Capitolo 5 della presente Parte Generale, pertanto, i Destinatari del Modello sono tenuti a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di correttezza e diligenza derivanti dal rapporto giuridico da essi instaurato con la Società.

CAPITOLO 3

LE ATTIVITA' SENSIBILI DI CAA

Dall'analisi dei rischi aziendali condotta ai fini del D.Lgs. 231/2001 sull'attività svolta da CAA, è emerso che le Attività Sensibili della Società - allo stato - riguardano principalmente le seguenti tipologie di reati:

a) reati commessi nei rapporti con la P.A.;

b) reati societari;

c) reati di terrorismo e di eversione dell'ordine democratico;

d) reati contro la personalità individuale;

e) reati ed illeciti amministrativi di abuso di mercato;

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

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

h) reati informatici e trattamento illecito di dati.

In particolare, nella realtà aziendale di CAA, le Attività Sensibili emerse dall'approfondita analisi effettuata in previsione dell'adozione del Modello risultano principalmente essere le seguenti:

a) **Attività Sensibili nei rapporti con la P.A.:**

- rapporti contrattuali con la P.A. e soggetti incaricati di un pubblico servizio;
- rapporti con le istituzioni e autorità di vigilanza;
- gestione degli acquisti, delle consulenze, delle liberalità e delle sponsorizzazioni;
- gestione dei contenziosi
- liquidazione sinistri per le polizze stipulate con gli enti pubblici.
- gestione delle verifiche / ispezioni (amministrative, fiscali, previdenziali, ecc.)
- gestione dei fondi pubblici erogati alla Società.

b) **Attività Sensibili nella gestione amministrativa della società (reati Societari)**:

- comunicazioni esterne;

- tenuta della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di Autorità di Vigilanza;
- gestione dei rapporti con il Collegio Sindacale, società di revisione e altri organi Sociali, nonché redazione, tenuta e conservazione dei documenti su cui gli stessi potrebbero esercitare il controllo;
- gestione delle incombenze societarie; operazioni sul capitale e operazioni su azioni;
- influenza sull'assemblea.

c) **Attività Sensibili con riferimento alle fattispecie di reato di terrorismo e di eversione dell'ordine democratico:**

- attività di consulenza prestata a favore delle clientela;
- rapporti con i fornitori;
- ricerca e selezione del personale, agenti, sub-agenti, broker;
- gestione della vendita delle polizze assicurative;
- identificazione, registrazione e conservazione dati per ciascun cliente.

d) **Attività Sensibili con riferimento alle fattispecie di reato contro la personalità individuale:**

- organizzazione di iniziative turistiche per viaggi all'estero e/o Paesi esotici al fine di motivare/gratificare i Dipendenti e la Rete Distributiva;
- contratti di consulenza finanziaria prestata a favore di Clienti o affidamento di contratti di fornitura di servizi e appalto a soggetti che - direttamente o indirettamente – gestiscano attività illecite come il traffico di minori o impongano condizioni lavorative ai propri dipendenti tali da configurare vere e proprie forme di schiavitù;

e) **Attività Sensibili con riferimento alle fattispecie di abuso di mercato**:

- comunicazioni all'esterno (ISVAP, azionisti, giornalisti, etc.);
- gestione dei rapporti con i giornalisti e con altri rappresentanti dei mezzi di comunicazione di massa;
- impartire ordini di acquisto e/o di vendita alla società di *asset management*.

f) **Attività Sensibili con riferimento alle fattispecie di reato di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro:**

- attività svolte dal personale dipendente presso la sede della Società alla quale sono connessi i tipici rischi d'ufficio (ad es. postura, videoterminale);
- attività svolte da personale esterno presso la sede della Società, quali ad esempio i Fornitori di servizi in base a contratti di appalto, d'opera o di somministrazione (art. 26 del Decreto Sicurezza).

g) **Attività Sensibili con riferimento alle fattispecie di reato di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita:**

- accensione e chiusura di rapporti con la clientela anche attraverso la Rete Distributiva (es. vendita di polizze vita e capitalizzazione attraverso la rete di agenti);
- esecuzione di operazioni disposte dalla clientela (ad es. i versamenti aggiuntivi);
- individuazione e segnalazione delle operazioni sospette;
- rapporto con i fornitori.

h) **Attività Sensibili con riferimento alle fattispecie di delitti informatici e trattamento illecito di dati ed i delitti in violazione del diritto d'autore:**

- in riferimento ai **delitti informatici e trattamento illecito di dati ,** corretto utilizzo ed idonea protezione dei sistemi informatici, come di seguito indicato:

  a) utilizzo della rete aziendale, del servizio di posta elettronica e accesso ad internet;

  b) gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa IT nonché sicurezza informatica;

  c) erogazione di servizi di installazione e servizi professionali di supporto al personale (ad esempio, assistenza, manutenzione, gestione della rete, manutenzione e *security*).

- in riferimento ai delitti in violazione del diritto d'autore sono state individuate le seguenti Attività Sensibili:

  a) utilizzo degli applicativi informatici aziendali, in considerazione del potenziale

utilizzo senza licenza di *software* coperti da altrui diritto d'autore;

b) gestione dei contenuti multimediali sulla rete aziendale e in particolare sul sito internet aziendale, in considerazione, tra l'altro, del possibile illegittimo utilizzo all'interno di quest'ultimo di composizioni musicali, immagini o altre opere dell'ingegno coperte da altrui diritto d'autore;

c) riproduzione di opere dell'ingegno coperte dal diritto d'autore.

i) Attività Sensibili con riferimento alle fattispecie di delitti di criminalità organizzata.

- *la selezione del personale;*
- *la selezione delle controparti contrattuali;*
- *la formazione delle scritture contabili, gestione della contabilità e degli adempimenti fiscali*

l) Attività Sensibili con riferimento alle fattispecie di delitti contro l'industria e il commercio e reati di contraffazione".

L'Amministratore Delegato ha il potere di individuare eventuali ulteriori attività a rischio che – a seconda dell'evoluzione legislativa o dell'attività della Società – potranno essere comprese nel novero delle Attività Sensibili.

CAPITOLO 4

L'ORGANISMO DI VIGILANZA

4.1 Identificazione dell'organismo di vigilanza

Ai sensi dell'art. 6, lett. b), D.Lgs. 231/2001, condizione indispensabile per la concessione dell'esimente dalla responsabilità amministrativa è l'attribuzione ad un organismo della Società, dotato di autonomi poteri di iniziativa e di controllo, del compito di vigilare sul funzionamento e l'osservanza del Modello, nonché di curarne l'aggiornamento.

Sul tema le Linee Guida ANIA, interpretando le disposizioni del Decreto, ne suggeriscono l'individuazione in un organo interno alla struttura della società, caratterizzato da autonomia, indipendenza, efficienza operativa e continuità di azione, nonché in possesso di professionalità ed onorabilità adeguate al ruolo.

Volendo nello specifico analizzare i singoli requisiti che devono caratterizzare l'Organismo di Vigilanza, si precisa quanto segue.

a) Autonomia e indipendenza.

Il requisito di autonomia e indipendenza presuppone che l'OdV risponda, nello svolgimento di questa sua funzione, solo al massimo vertice gerarchico (ad esempio, Amministratore Delegato, Consiglio di Amministrazione e Collegio Sindacale).

In sede di costituzione dell'OdV, la sua indipendenza è assicurata dall'obbligo, in capo all'organo dirigente, di approvare una dotazione annua adeguata di risorse finanziarie, anche su proposta dell'Organismo di Vigilanza stesso, della quale quest'ultimo potrà disporre per ogni esigenza necessaria al corretto svolgimento dei propri doveri (es. consulenze specialistiche, trasferte, etc.).

L'indipendenza, infine, presuppone che i membri dell'Organismo di Vigilanza non si trovino in una posizione, neppure potenziale di conflitto d'interessi con la Società, né siano titolari all'interno della stessa di funzioni di tipo operativo che ne minerebbero l'obiettività di giudizio nel momento delle verifiche sul rispetto del Modello.

b) Onorabilità e cause di ineleggibilità.

Non possono essere eletti membri dell'Organismo di Vigilanza e, se lo sono, decadono necessariamente ed automaticamente dalla carica:

i. coloro che si trovano nelle condizioni previste dall'articolo 2382 codice civile, ovverosia gli inabilitati, interdetti, falliti o condannati ad una pena che comporti l'interdizione, anche temporanea, da uffici pubblici o l'incapacità ad esercitare uffici direttivi;

ii. coloro che siano stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423 (legge sulle misure di prevenzione nei confronti delle persone pericolose per la sicurezza e per la pubblica moralità) o della legge 31 maggio 1965, n. 575 (legge contro la mafia);

iii. coloro che sono stati condannati a seguito di sentenza ancorché non ancora definitiva, o emessa ex artt. 444 e ss. codice procedura penale o anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:

1) per uno dei delitti previsti nel titolo XI del libro V del codice civile (Disposizioni penali in materia di società e consorzi) e nel Regio Decreto 16 marzo 1942, n. 267, e sue successive modifiche od integrazioni (disciplina del fallimento, del concordato preventivo, dell'amministrazione controllata e della liquidazione coatta amministrativa);

2) a pena detentiva, non inferiore ad un anno, per uno dei reati previsti dalle norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento (tra questi si segnalano, a titolo esemplificativo e non esaustivo, i reati di abusivismo bancario e finanziario di cui agli artt. 130 e seguenti del Testo Unico Bancario, i reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate di cui all'art. 453 codice penale, i reati di fraudolento danneggiamento dei beni assicurati e mutilazione fraudolenta della propria persona di cui all'art. 642 codice penale);

3) per un delitto contro la pubblica amministrazione, o alla reclusione per un tempo non inferiore ad un anno per un delitto contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria;

4) alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo;

5) in ogni caso e a prescindere dall'entità della pena per uno o più illeciti tra quelli tassativamente previsti dal D.Lgs. 231/01;

iv. coloro che hanno rivestito la qualifica di componente dell'OdV in società nei cui confronti siano state applicate le sanzioni previste dall'art. 9, D.Lgs. 231/01, salvo che siano trascorsi 5 anni dalla inflizione in via definitiva delle sanzioni e il componente non sia incorso in condanna penale ancorché non definitiva;

v. coloro nei cui confronti siano state applicate le sanzioni amministrative accessorie previste dall'art. 187-*quater* TUF (D.lgs n. 58/1998).

c) Comprovata professionalità, capacità specifiche in tema di attività ispettiva e consulenziale.

L'Organismo di Vigilanza deve possedere, al suo interno, competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite alla sua indipendenza, ne garantiscono l'obiettività di giudizio; è necessario, pertanto, che all'interno dell'Organismo di Vigilanza siano presenti soggetti con professionalità adeguate in materia economica, di controllo e gestione dei rischi aziendali. L'Organismo di Vigilanza potrà, inoltre, anche avvalendosi di professionisti esterni, dotarsi di risorse competenti in materia giuridica di organizzazione aziendale, revisione, contabilità e finanza.

d) Continuità d'azione.

L'Organismo di Vigilanza svolge in modo continuativo le attività necessarie per la vigilanza in merito alla corretta applicazione del Modello con adeguato impegno e con i necessari poteri di indagine; è una struttura interna alla società, in modo da garantire la dovuta continuità nell'attività di vigilanza; cura l'attuazione del Modello assicurandone il costante aggiornamento; non svolge mansioni operative che possano condizionare e contaminare quella visione d'insieme sull'attività aziendale che ad esso si richiede.

In ottemperanza a quanto stabilito dal Decreto, e da tutto quanto sopra indicato, il Consiglio di Amministrazione della Società ha ritenuto che la composizione dell'Organismo di Vigilanza che meglio risponde ai requisiti indicati dal Decreto è la seguente:

a. un professionista esterno con comprovata esperienza in ambito giuridico e legale, e, in particolare, di *compliance* al D.Lgs. 231/01;

b. il responsabile della funzione Internal Audit;

c. il Compliance Officer.

Tale scelta è stata determinata dal fatto che le suddette figure sono state riconosciute come le più adeguate ad assumere il ruolo dell'OdV in quanto, oltre ai requisiti di autonomia, indipendenza, professionalità, onorabilità e continuità d'azione che si richiedono per tale funzione, e alle capacità specifiche in tema di attività ispettive e consulenziali, possiedono altresì quei requisiti soggettivi formali che garantiscano ulteriormente l'autonomia e l'indipendenza richiesta dal compito affidato, quali onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice.

4.2 Durata in carica

Il Consiglio di Amministrazione provvede alla nomina dell'Organismo di Vigilanza mediante apposita delibera consiliare: a tal riguardo, al momento della nomina dovranno essere forniti nel corso della riunione consiliare adeguati chiarimenti in merito alla professionalità dei suoi componenti, il cui *curriculum vitae* verrà allegato al relativo verbale.

L'OdV viene nominato per un periodo di tre anni, coincidente con quello previsto per la durata del Collegio Sindacale in carica al momento della nomina.

Alla scadenza dell'incarico, l'OdV potrà continuare a svolgere le proprie funzioni e ad esercitare i poteri di propria competenza, come in seguito meglio specificati, sino alla nomina dei nuovi componenti da parte del Consiglio di Amministrazione.

Al fine di garantire i requisiti di indipendenza e di autonomia, dal momento della nomina e per tutta la durata della carica, i componenti dell'Organismo:

a) non devono rivestire incarichi esecutivi o delegati nel Consiglio di Amministrazione della Società;

b) non devono svolgere funzioni operative o di business all'interno della Società;

c) non devono intrattenere significativi rapporti d'affari con la Società, con società da essa controllate o ad essa collegate, salvo il rapporto di lavoro subordinato o l'eventuale appartenenza al Collegio Sindacale, né intrattenere significativi rapporti d'affari con gli amministratori muniti di deleghe (amministratori esecutivi);

d) non devono avere rapporti con o far parte del nucleo familiare degli amministratori esecutivi, dovendosi intendere per nucleo familiare quello costituito dal coniuge non separato legalmente, dai parenti ed affini entro il quarto grado;

e) non devono risultare titolari, direttamente o indirettamente, di partecipazioni nel capitale della Società;

f) devono avere e mantenere i requisiti di onorabilità indicati nella lettera b) del paragrafo 4.1 che precede.

I componenti dell'Organismo di Vigilanza sono tenuti a sottoscrivere, all'atto della nomina e successivamente con cadenza annuale, una dichiarazione attestante l'esistenza e la successiva persistenza dei requisiti di indipendenza di cui sopra e, comunque, a comunicare immediatamente al Consiglio e agli altri componenti dell'Organismo di Vigilanza l'insorgere di eventuali condizioni ostative.

Rappresentano ipotesi di decadenza automatica le incompatibilità di cui alle precedenti lettere da a) ad e), le circostanze di cui alla lettera f), la sopravvenuta incapacità e la morte; fatte salve le ipotesi di decadenza automatica, i membri dell'Organismo non possono essere revocati dal Consiglio di Amministrazione se non per giusta causa.

Rappresentano ipotesi di giusta causa di revoca:

a) una sentenza di condanna della Società ai sensi del Decreto o una sentenza di patteggiamento, passata in giudicato, ove risulti dagli atti l'omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza, secondo quanto previsto dall'art. 6, comma 1, lett. d) del Decreto;

b) la violazione degli obblighi di riservatezza di cui al successivo paragrafo 3.9;

c) la mancata partecipazione a più di tre riunioni consecutive senza giustificato motivo;

d) grave negligenza nell'adempimento dei propri compiti;

e) in caso di soggetti interni alla struttura aziendale, le eventuali dimissioni o licenziamento.

In caso di dimissioni o di decadenza automatica di un membro effettivo dell'Organismo di Vigilanza, quest'ultimo ne darà comunicazione tempestiva al Consiglio di Amministrazione, che prenderà senza indugio le decisioni del caso.

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

4.3 Funzione e poteri dell'organo di controllo interno

All'OdV è affidato il compito di vigilare:

a. sull'osservanza del Modello da parte dei Dipendenti, degli Organi Sociali, della Rete Distributiva, dei Consulenti e dei Partner;

b. sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei Reati;

c. sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate condizioni aziendali e/o normative.

Su di un piano più operativo all'OdV è affidato il compito di:

i. *Aggiornamenti, potestà normativa, segnalazioni:*

   a. suggerire e promuovere l'emanazione di disposizioni procedurali attuative dei principi e delle regole contenute nel Modello;

   b. interpretare la normativa rilevante e verificare l'adeguatezza del Modello a tali prescrizioni normative, segnalando al Consiglio di Amministrazione le possibili aree di intervento;

   c. valutare le esigenze di aggiornamento del Modello, segnalando al Consiglio di Amministrazione (o, per le modifiche minori, all'Amministratore Delegato) le possibili aree di intervento;

   d. indicare nella relazione annuale al Consiglio di Amministrazione di cui al paragrafo 4.6 le opportune integrazioni ai sistemi di gestione delle risorse finanziarie (sia in entrata che in uscita), già presenti in CAA, per introdurre alcuni accorgimenti idonei a rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto;

   e. indicare nella relazione annuale al Consiglio di Amministrazione di cui al paragrafo 4.6 l'opportunità di emanare particolari disposizioni procedurali attuative dei principi contenuti nel Modello, che potrebbero non essere coerenti con quelle in vigore attualmente nella Società, curando altresì il coordinamento delle stesse con quanto esistente.

ii. *Verifiche e controlli:*

   a. condurre – attraverso i componenti aziendali interni all'OdV – ricognizioni sull'attività aziendale ai fini dell'aggiornamento della mappatura delle Attività Sensibili;

   b. in ottemperanza a quanto previsto nel calendario annuale delle attività dell'organismo, effettuare – attraverso i componenti aziendali interni all'OdV – periodiche verifiche mirate su determinate operazioni o specifici atti posti in essere da CAA, soprattutto nell'ambito delle

Attività Sensibili, i cui risultati devono essere riassunti in un apposito rapporto da esporsi in sede di *reporting* agli organi Sociali deputati;

c. raccogliere, elaborare e conservare le informazioni rilevanti in ordine al rispetto del Modello, nonché aggiornare la lista di informazioni che devono essere ad esso trasmesse o tenute a propria disposizione (vedi in dettaglio il successivo par. 4.7);

d. coordinarsi con le altre funzioni aziendali (anche attraverso apposite riunioni) per il miglior monitoraggio delle attività in relazione alle procedure stabilite nel Modello. A tal fine, l'OdV ha libero accesso a tutta la documentazione aziendale (sia cartacea sia informatica) che ritiene rilevante e deve essere costantemente informato dal *management*: a) sugli aspetti dell'attività aziendale che possono esporre CAA al rischio di commissione di uno dei Reati; b) sui rapporti con la Rete Distributiva, i Consulenti e i Partner che operano per conto della Società nell'ambito di Operazioni Sensibili;

e. attivare e svolgere le inchieste interne, raccordandosi di volta in volta con le funzioni aziendali interessate per acquisire ulteriori elementi di indagine;

f. sollecitare l'attuazione delle procedure di controllo previste dal Modello anche tramite l'emanazione o proposizione di disposizioni (normative e/o informative) interne;

iii. *Formazione:*

a. coordinarsi con gli incaricati della gestione delle Risorse Umane per la definizione dei programmi di formazione per il personale stesso e del contenuto delle comunicazioni periodiche da farsi ai Dipendenti e agli Organi Sociali, finalizzate a fornire ai medesimi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D.Lgs. 231/2001;

b. coordinarsi con il responsabile dell'Ufficio del Personale della Rete Distributiva del Gruppo Cariparma per la definizione dei programmi di formazione della Rete Distributiva e del contenuto delle comunicazioni periodiche da farsi alla medesima, finalizzate a fornire

ai medesimi la necessaria sensibilizzazione e le conoscenze di base della normativa di cui al D.Lgs. 231/2001;

c. monitorare le iniziative per la diffusione della conoscenza e della comprensione del Modello e predisporre la documentazione interna necessaria al fine della sua efficace attuazione, contenente istruzioni d'uso, chiarimenti o aggiornamenti dello stesso;

d. far predisporre ed aggiornare con continuità, dalla Comunicazione e Immagine e la funzione Marketing Strategico, lo spazio nell'Intranet del Gruppo contenente tutte le informazioni relative al D.Lgs. 231/2001 e al Modello;

iv. *Sanzioni:*

a. coordinarsi con il *management* aziendale per valutare o proporre l'adozione di eventuali sanzioni o provvedimenti, fermo restando la competenza di quest'ultimo - e in particolare degli incaricati della gestione delle Risorse Umane - in merito alla decisione e alla irrogazione dei medesimi (si rinvia in merito a questo punto al successivo Capitolo 6 della presente Parte Generale).

4.4 Poteri dell'Organismo di Vigilanza

L'OdV ha, *ex lege*, autonomi poteri di iniziativa e controllo ai fini di vigilare sul funzionamento e l'osservanza del Modello, ma non ha poteri coercitivi o di intervento sulla struttura aziendale o sanzionatori, poteri questi che sono demandati ai competenti Organi Sociali o alle funzioni aziendali competenti.

Tenuto conto delle peculiarità delle attribuzioni e degli specifici contenuti professionali richiesti, nello svolgimento dei compiti di vigilanza e controllo l'OdV sarà costantemente supportato anche da tutti i dirigenti e dal management della Società. In capo a questi ultimi, nell'ambito delle rispettive funzioni e nei limiti delle deleghe assegnate, ricade una responsabilità primaria per quanto concerne: 1) il controllo delle attività e delle aree di competenza; 2) l'osservanza del Modello da parte dei Dipendenti sottoposti alla loro direzione; 3) la tempestiva e puntuale informazione verso l'OdV su eventuali anomalie, problematiche riscontrate e/o criticità rilevate.

L'OdV potrà richiedere ai dirigenti specifiche attività di controllo sul corretto e preciso funzionamento del Modello.

Tutti i soggetti coinvolti all'interno della struttura aziendale sono tenuti a vigilare ed informare l'OdV sulla corretta applicazione del presente Modello, ciascuno nell'ambito delle proprie competenze operative.

L'OdV può avvalersi, ogni qualvolta lo ritiene necessario all'espletamento della propria attività di vigilanza e di tutto quanto previsto nel presente Modello, della collaborazione di ulteriori risorse, prescelte nell'ambito delle varie funzioni aziendali, senza limitazioni di tempo e di numero.

L'autonomia e l'indipendenza che necessariamente devono connotare le attività dell'OdV hanno reso necessario introdurre alcune forme di tutela in suo favore, al fine di garantire l'efficacia del Modello e di evitare che la sua attività di controllo possa ingenerare forme di ritorsione a suo danno. Pertanto, le decisioni in merito a remunerazione, promozioni, trasferimento o sanzioni relative all'OdV e ai suoi membri, allorquando essi siano dipendenti della Società, sono attribuite alla competenza esclusiva del Consiglio di Amministrazione, sentiti, laddove necessario, gli incaricati della gestione delle Risorse Umane.

Pertanto, il Consiglio di Amministrazione della Società conferisce all'OdV i seguenti poteri:

- potere di accedere a tutti i documenti e a tutte le informazioni relative alla Società;
- potere di avvalersi di tutte le strutture della Società, che sono obbligate a collaborare, dei revisori e di consulenti esterni;
- potere di raccogliere informazioni presso tutti i Dipendenti e i Collaboratori, inclusa la società di revisione, in relazione a tutte le attività della Società;
- potere di richiedere, attraverso i canali e le persone appropriate, la riunione del Consiglio di Amministrazione e del Collegio Sindacale per affrontare questioni urgenti;
- potere di richiedere ai titolari delle funzioni di partecipare, senza potere deliberante, alle sedute dell'Organismo di Vigilanza;

- potere di avvalersi di consulenti esterni ai quali delegare circoscritti ambiti di indagine o attività. A tale proposito, il Consiglio di Amministrazione dovrà approvare ogni anno un budget di spesa per l'OdV, il quale ne potrà disporre liberamente in relazione alle proprie attività, salvo richieste integrazioni per eventuali necessità sopravvenute.

4.5 Regole di convocazione e di funzionamento

L'Organismo di Vigilanza disciplina con specifico regolamento le modalità del proprio funzionamento, sulla base dei principi di seguito riportati:

- l'Organismo di Vigilanza si riunisce trimestralmente e la documentazione relativa viene distribuita almeno 3 giorni prima della seduta;
- le sedute si tengono di persona, per video o tele conferenza (o in combinazione);
- il Presidente, l'Amministratore Delegato, il Consiglio di Amministrazione e il Collegio Sindacale possono richiedere che l'Organismo di Vigilanza si riunisca in qualsiasi momento;
- per la validità delle sedute è richiesto l'intervento della maggioranza dei membri in carica;
- possono essere effettuate sedute *ad hoc* e tutte le decisioni prese durante queste sedute devono essere riportate nella successiva seduta trimestrale;
- le decisioni vengono assunte sulla base di decisioni unanimi; in caso di mancanza di unanimità, prevale la decisione maggioritaria e ciò viene riportato immediatamente al Consiglio di Amministrazione;
- i verbali delle sedute riportano tutte le decisioni prese dall'organo e riflettono le principali considerazioni effettuate per raggiungere la decisione; tali verbali vengono conservati dall'Organismo di Vigilanza nel proprio archivio.

Fino alla formalizzazione da parte dell'Organismo di Vigilanza del regolamento di cui sopra, la convocazione e il funzionamento dello stesso si basano sui principi sopra indicati.

4.6 Flussi informativi dell'OdV verso il vertice aziendale

L'OdV riferisce in merito all'attuazione del Modello e all'emersione di eventuali criticità.

L'OdV ha due differenti tipologie di flussi informativi:

- la prima, su base continuativa, non appena ve ne sia la necessità, direttamente verso l'Amministratore Delegato;
- la seconda, su base almeno semestrale, nei confronti del Consiglio di Amministrazione e del Collegio Sindacale.

Tali flussi informativi hanno ad oggetto:

1. l'attività svolta dall'ufficio dell'OdV;

2. le eventuali criticità (e spunti per il miglioramento) emerse sia in termini di comportamenti o eventi interni a CAA, sia in termini di efficacia del Modello. Qualora l'OdV rilevi criticità riferibili a qualcuno dei soggetti referenti, la corrispondente segnalazione è da destinarsi prontamente ad uno degli altri soggetti sopra individuati.

Inoltre, l'OdV predispone annualmente una relazione scritta per il Consiglio di Amministrazione ove sia contenuta:

(a) un'analisi sintetica di tutta l'attività svolta nel corso dell'anno (indicando in particolare i controlli effettuati e l'esito degli stessi, le verifiche specifiche di cui al successivo Capitolo 7 della presente Parte Generale e l'esito delle stesse, l'eventuale aggiornamento della mappatura delle Attività Sensibili, ecc.);

(b) un piano di attività prevista per l'anno successivo.

Gli incontri con gli organi cui l'OdV riferisce devono essere verbalizzati e copie dei verbali devono essere custodite dall'OdV.

Il Consiglio di Amministrazione e il Presidente del Consiglio di Amministrazione, hanno la facoltà di convocare in qualsiasi momento l'OdV che, a sua volta, ha la facoltà di richiedere, attraverso le funzioni o i soggetti competenti, la convocazione dei predetti organi per motivi urgenti.

L'OdV deve, inoltre, coordinarsi con le funzioni competenti presenti in Società per i diversi profili specifici e precisamente:

- con la funzione Corporate governante, legale e compliance per gli adempimenti Sociali che possono avere rilevanza ai fini della commissione dei Reati;
- con gli incaricati della gestione delle Risorse Umane in ordine alla formazione del personale ed ai procedimenti disciplinari;
- con il responsabile della funzione Commerciale in ordine alla formazione della Rete Distributiva ed ai relativi provvedimenti;
- con il responsabile della funzione Amministrazione e Controllo in ordine alla gestione dei flussi finanziari;
- con l'RSPP per le tematiche relative alla sicurezza sul lavoro;
- con le funzioni di controllo (Compliance, Internal Audit e Risk Management) per il coordinamento dell'attività di verifica e controllo.

4.7 Flussi informativi verso l'OdV: informazioni di carattere generale ed informazioni specifiche obbligatorie

L'OdV deve essere informato, mediante apposite segnalazioni da parte dei Dipendenti, dei Dipendenti di CAV, degli Organi Sociali, della Rete Distributiva, dei Consulenti e dei Partner in merito ad eventi che potrebbero ingenerare responsabilità di CAA ai sensi del D.Lgs. 231/2001.

Valgono al riguardo le seguenti prescrizioni di carattere generale:

- i Dipendenti e gli Organi Sociali devono segnalare all'OdV le notizie relative alla commissione, o alla ragionevole convinzione di commissione, dei Reati;
- i Dipendenti con la qualifica di dirigente hanno l'obbligo di segnalare all'OdV anche le violazioni delle regole di comportamento o procedurali contenute nel presente Modello di cui vengano a conoscenza;
- la Rete Distributiva, i Consulenti ed i Partner sono tenuti ad effettuare le segnalazioni con le modalità e nei limiti previsti contrattualmente.

Le segnalazioni devono esser eseguite, in forma scritta, con le seguenti modalità:

(a) dai Dipendenti al superiore gerarchico, che provvederà a indirizzarle verso l'OdV. In caso di mancata canalizzazione verso l'OdV da parte del superiore gerarchico o

comunque nei casi in cui il Dipendente si trovi in una situazione di disagio psicologico nell'effettuare la segnalazione al superiore gerarchico, la segnalazione potrà essere fatta direttamente all'OdV, che potrà tenere in considerazione anche le denunce anonime purché sufficientemente circostanziate e tali da risultare credibili a suo insindacabile giudizio.

(b) la Rete Distributiva, i Consulenti e i Partner, per quanto riguarda la loro attività svolta nei confronti di CAA, effettuano la segnalazione direttamente all'OdV.

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

In ogni caso, CAA garantisce i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione ed assicura la massima riservatezza circa la loro identità, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Oltre alle segnalazioni sopra descritte, gli Organi Sociali, i Dipendenti, i Dipendenti di CAV e, nei modi e nei limiti previsti contrattualmente, la Rete Distributiva, i Consulenti e i Partner devono **obbligatoriamente ed immediatamente** trasmettere all'OdV le informazioni concernenti:

- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i Reati qualora tali indagini coinvolgano CAA o suoi Dipendenti, Organi Sociali, Rete Distributiva, Consulenti e Partner;
- i rapporti preparati dalle funzioni competenti nell'ambito della loro attività di controllo e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D.Lgs. 231/2001;
- le notizie relative ai procedimenti sanzionatori svolti e alle eventuali sanzioni irrogate (ivi compresi i provvedimenti verso i Dipendenti) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di Reati o violazione delle regole di comportamento o procedurali del Modello.

Periodicamente l'OdV propone, se del caso, al Consiglio di Amministrazione o all'Amministratore Delegato eventuali modifiche della lista sopra indicata relativa alle informazioni obbligatorie.

In ogni caso, qualora un Destinatario non adempia agli obblighi informativi di cui al presente paragrafo 4.7, allo stesso sarà irrogata una sanzione disciplinare che varierà a seconda della gravità dell'inottemperanza agli obblighi sopra menzionati e che sarà comminata secondo le regole indicate nel capitolo 6 del presente Modello.

L'OdV, inoltre, ha il diritto di richiedere informazioni in merito al sistema di deleghe adottato da CAA, secondo modalità dallo stesso stabilite.

4.8 Modalità delle segnalazioni.

Qualora un Esponente Aziendale desideri effettuare una segnalazione tra quelle sopra indicate, dovrà riferire al suo diretto superiore (o al suo riporto) il quale canalizzerà la suddetta segnalazione all'OdV. Qualora la segnalazione non dia esito, o l'Esponente Aziendale potrà riferire direttamente all'OdV.

L'OdV valuta le segnalazioni ricevute ascoltando eventualmente l'autore della segnalazione e/o il responsabile della presunta violazione e motivando per iscritto eventuali rifiuti di procedere ad una indagine interna.

Per ciò che concerne i Collaboratori, Fornitori e Partner, gli stessi potranno fare le segnalazioni di cui al precedente paragrafo 4.7 direttamente all'OdV.

Per quanto concerne le segnalazioni dirette all'OdV, le stesse potranno infine essere effettuate anche tramite e-mail all'indirizzo di posta elettronica che sarà indicato agli Esponenti Aziendali – unitamente ad ulteriori eventuali modalità per poter inviare le proprie segnalazioni all'Organismo di Vigilanza – secondo le politiche aziendali in materia di informativa ai dipendenti.

4.9 Obblighi di riservatezza.

I componenti dell'Organismo di Vigilanza assicurano la riservatezza delle informazioni di cui vengano in possesso, in particolare se relative a segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello.

I componenti dell'OdV si astengono, altresì, dall'utilizzare informazioni riservate per fini diversi da quelli di cui al precedente paragrafo 4.3 e comunque per scopi non conformi alle funzioni proprie di un organismo di vigilanza, fatto salvo il caso di espressa e consapevole autorizzazione.

L'inosservanza di tali obblighi costituisce giusta causa di revoca della carica.

4.10 Raccolta e conservazione delle informazioni.

Ogni informazione raccolta e ogni report ricevuto o preparato dall'Organismo di Vigilanza è conservato per 10 anni in un apposito archivio tenuto dall'OdV in formato cartaceo o elettronico.

CAPITOLO 5

LA FORMAZIONE DELLE RISORSE E LA DIFFUSIONE DEL MODELLO

5.1 Formazione ed informazione dei Dipendenti

Ai fini dell'efficacia del presente Modello, è precipuo obiettivo di CAA quello di garantire una corretta conoscenza delle regole di condotta ivi contenute sia alle risorse già presenti in Società sia a quelle future. Il livello di conoscenza è realizzato con differente grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse medesime nelle Attività Sensibili.

- *La comunicazione iniziale*

L'adozione del presente Modello è comunicata a tutti i Dipendenti presenti in azienda al momento della sua adozione.

Ai nuovi assunti, invece, viene consegnato un set informativo (ad es. CCNL, Modello Organizzativo, Decreto Legislativo 231/2001, ecc.), con il quale assicurare agli stessi le conoscenze considerate di primaria rilevanza.

- *La formazione*

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al D.Lgs. 231/2001 è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei destinatari, del livello di rischio dell'area in cui operano, dell'avere o meno i destinatari funzioni di rappresentanza della Società.

In particolare, CAA cura l'adozione e l'attuazione di un adeguato livello di formazione mediante idonei strumenti di diffusione e, in particolare attraverso:

- meeting aziendali;

- corsi istituzionali (in aula ovvero web-based) aventi ad oggetto specifiche aree sensibili del Decreto.

Il sistema di informazione e formazione è supervisionato ed integrato dall'attività realizzata in questo campo dall'OdV avvalendosi della collaborazione degli incaricati della gestione delle Risorse Umane.

La mancata partecipazione all'attività di formazione senza giustificazione da parte degli Esponenti Aziendali costituisce una violazione dei principi contenuti nel presente Modello e, pertanto, sarà sanzionata ai sensi di quanto indicato nel capitolo 6 che segue.

5.2 Selezione ed informazione della Rete Distributiva, dei Consulenti e dei Partner

Relativamente alla Rete Distributiva, ai Consulenti ed ai Partner, sentito l'OdV e in collaborazione con il responsabile dell'Ufficio del Personale, sono istituiti appositi sistemi in grado di orientare la selezione dei medesimi secondo criteri che tengano in debito conto i principi di prevenzione ed integrità di cui al presente Modello, principi di cui gli stessi verranno adeguatamente informati.

CAPITOLO 6

SISTEMA SANZIONATORIO

6.1 Funzione del sistema sanzionatorio

La definizione di un sistema di sanzioni (commisurate alla violazione e dotate di adeguata efficacia deterrente) applicabili in caso di violazione delle regole di cui al presente Modello, rende effettiva l'azione di vigilanza dell'OdV ed ha lo scopo di garantirne l'efficace attuazione.

La definizione di tale sistema sanzionatorio costituisce, infatti, ai sensi dell'art. 6, comma 1, lett. *e)*, D.Lgs. 231/2001, un requisito essenziale del Modello medesimo ai fini dell'esimente rispetto alla responsabilità della Società.

L'applicazione del sistema sanzionatorio e dei relativi provvedimenti è indipendente dallo svolgimento e dall'esito del procedimento penale che l'autorità giudiziaria abbia eventualmente avviato nel caso in cui il comportamento da censurare valga anche ad integrare una fattispecie di reato rilevante ai sensi del D.Lgs. 231/2001.

Il presente capitolo contiene la descrizione delle misure sanzionatorie adottate dalla Società in caso di violazione del Modello da parte dei Destinatari, in coordinamento con il sistema disciplinare di cui al Contratto Collettivo Nazionale di Lavoro applicato da CAA, nel rispetto delle procedure previste dall'art. 7, legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori).

6.2 Dipendenti soggetti al CCNL

6.2.1 Sistema sanzionatorio

La violazione da parte dei Dipendenti delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare. Quanto di seguito riportato è esteso anche ai dipendenti e dirigenti di CA Vita per i servizi prestati a CAA in virtù dei contratti di servizio.

I provvedimenti sanzionatori irrogabili nei riguardi di detti lavoratori – nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) e delle eventuali normative speciali applicabili – sono quelli previsti dall'apparato sanzionatorio del CCNL applicato da CAA (in particolare, gli artt. 26 e ss.,

nonché artt. 75 e ss del CCNL relativi alla cessazione del rapporto di lavoro per giusta causa) e del relativo regolamento interno dalla Società adottato, e precisamente:

a) rimprovero verbale;

b) biasimo inflitto per iscritto;

c) sospensione dal servizio e dal trattamento economico per un periodo fino a 10 giorni;

d) risoluzione del rapporto di lavoro a seguito del recesso del datore di lavoro per giusta causa.

Restano ferme - e si intendono qui richiamate - tutte le previsioni dei richiamati CCNL e regolamento interno, relativamente alla procedure ed agli obblighi da osservare nell'applicazione delle sanzioni.

Restano invariati i poteri già conferiti al *management* aziendale per quanto riguarda l'accertamento delle infrazioni, i procedimenti sanzionatori e l'irrogazione delle relative sanzioni.

6.2.2 Violazioni del Modello e relative sanzioni

Fermi restando gli obblighi per la Società nascenti dallo Statuto dei Lavoratori, i comportamenti sanzionabili sono i seguenti:

1) violazione di procedure interne previste dal presente Modello (ad esempio, non osservanza delle procedure prescritte, omissione di comunicazioni all'OdV in merito a informazioni prescritte, omissione di controlli, ecc.) o adozione, nell'espletamento di attività connesse alle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello;

- sanzione: rimprovero verbale

2) violazione di procedure interne previste dal presente Modello o adozione, nell'espletamento di attività connesse alle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello stesso che espongano la Società ad una situazione oggettiva di rischio di commissione di uno dei Reati;

- sanzione: biasimo inflitto per scritto

3) adozione, nell'espletamento di attività connesse alle Attività Sensibili, di comportamenti non conformi alle prescrizioni del presente Modello e diretti dolosamente e in modo univoco al compimento di uno o più Reati, anche se poi non effettivamente perfezionati quale fattispecie criminosa;

- sanzione: sospensione dal servizio e del trattamento economico

4) adozione, nell'espletamento di attività connesse alle Attività Sensibili, di comportamenti palesemente in violazione delle prescrizioni del presente Modello, tale da determinare la concreta applicazione a carico della Società di sanzioni previste dal D. Lgs. 231/2001;

- sanzione: risoluzione del rapporto di lavoro per recesso per giusta causa del datore di lavoro.

Le sanzioni verranno commisurate al livello di responsabilità ed autonomia del Dipendente, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità del suo comportamento nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Società può ragionevolmente ritenersi esposta - ai sensi e per gli effetti del D.Lgs. 231/2001 - a seguito della condotta censurata.

Il sistema sanzionatorio è soggetto a costante verifica e valutazione da parte dell'OdV e degli incaricati della gestione delle Risorse Umane, rimanendo quest'ultimi responsabili della concreta applicazione dei provvedimenti necessari su eventuale segnalazione dell'OdV e sentito il superiore gerarchico dell'autore della condotta censurata.

6.3 Misure nei confronti dei dirigenti

In caso di violazione, da parte di Dipendenti che ricoprano la qualifica di dirigenti, delle procedure previste dal presente Modello o di adozione, nell'espletamento di attività connesse con le Attività Sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, la Società provvede ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dalla legge e dalla Contrattazione Collettiva applicabile.

La sanzione minima consisterà in una contestazione verbale o scritta al Dirigente.

Nelle ipotesi più gravi, come ad esempio la commissione di un Reato, sarà valutata l'ipotesi del licenziamento.

I comportamenti sanzionabili che costituiscono violazione del presente del Modello sono, a titolo esemplificativo, i seguenti:

a) adozione, nell'espletamento delle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello e diretti in modo univoco al compimento di uno o più Reati riconducibili alla Società;

b) violazione di procedure interne previste dal presente Modello o adozione, nell'espletamento delle Attività Sensibili, di comportamenti non conformi alle prescrizioni del Modello stesso che espongano la Società ad una situazione oggettiva di rischio imminente di commissione di uno dei reati.

Per quanto riguarda l'accertamento delle infrazioni e l'irrogazione delle sanzioni restano invariati i poteri già conferiti, nei limiti della rispettiva competenza, agli Organi Societari ed alle competenti direzioni aziendali.

6.4 Misure nei confronti degli Amministratori

In caso di violazione del Modello da parte di uno o più membri del Consiglio di Amministrazione, l'OdV informa il Collegio Sindacale e l'intero Consiglio di Amministrazione i quali prendono gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee previste dalla legge.

Inoltre, al momento della nomina dei nuovi amministratori, gli stessi procederanno a sottoscrivere impegni unilaterali di rispetto degli obblighi previsti dal Modello nonché un impegno a rassegnare le proprie dimissioni, rinunciando al proprio compenso relativo all'esercizio in corso, nel caso di condanna, anche di primo grado, per uno dei Reati.

6.5 Misure nei confronti dei Sindaci

In caso di violazione del presente Modello da parte di uno o più Sindaci, l'OdV informa l'intero Collegio Sindacale e il Consiglio di Amministrazione i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la convocazione dell'assemblea dei soci al fine di adottare le misure più idonee previste dalla legge.

6.6 Misure nei confronti dei membri dell'OdV

In caso di violazione del presente Modello da parte di uno o più membri dell'OdV, gli altri membri dell'OdV ovvero uno qualsiasi tra i Sindaci o tra gli Amministratori, informerà immediatamente il Collegio Sindacale e il Consiglio di Amministrazione i quali prenderanno gli opportuni provvedimenti tra cui, ad esempio, la revoca dell'incarico ai membri dell'OdV che hanno violato il Modello e la conseguente nomina di nuovi membri in sostituzione degli stessi ovvero la revoca dell'incarico all'intero organo e la conseguente nomina di un nuovo OdV.

6.7 Misure nei confronti della Rete Distributiva, dei Consulenti e dei Partner

Ogni violazione da parte della Rete Distributiva, dei Consulenti o dei Partner delle regole di cui al presente Modello agli stessi applicabili o di commissione dei Reati è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.

Resta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni concreti alla Società, come nel caso di applicazione alla stessa da parte dell'autorità giudiziaria delle misure previste dal D.Lgs. 231/2001.

CAPITOLO 7

VERIFICHE SULL'ADEGUATEZZA DEL MODELLO

Oltre all'attività di vigilanza che l'OdV svolge continuamente sull'effettività del Modello (e che si concreta nella verifica della coerenza tra i comportamenti concreti dei Destinatari ed il Modello stesso), questo periodicamente effettua specifiche verifiche sulla reale capacità del Modello alla prevenzione dei Reati, coadiuvandosi con soggetti terzi in grado di assicurare una valutazione obiettiva dell'attività svolta.

Tale attività si concretizza in una verifica a campione dei principali atti societari e dei contratti di maggior rilevanza conclusi o negoziati da CAA in relazione alle Attività Sensibili e alla conformità degli stessi alle regole di cui al presente Modello.

Inoltre, viene svolta una *review* di tutte le segnalazioni ricevute nel corso dell'anno, delle azioni intraprese dall'OdV, degli eventi considerati rischiosi e della consapevolezza dei Dipendenti e degli Organi Sociali rispetto alla problematica della responsabilità penale dell'impresa con verifiche a campione.

Per le verifiche l'OdV si avvale, di norma, anche del supporto di quelle funzioni interne che, di volta in volta, si rendano a tal fine necessarie.

Le verifiche e il loro esito sono oggetto di *report* annuale al Consiglio di Amministrazione. In particolare, in caso di esito negativo, l'OdV esporrà, nel piano relativo all'anno, i miglioramenti da attuare.

PARTI SPECIALI

PARTE SPECIALE – A –

Reati nei rapporti con la Pubblica Amministrazione

CAPITOLO A.1

Criteri per la definizione di pubblica amministrazione, di pubblici ufficiali e di soggetti incaricati di un pubblico servizio

I reati di cui alla presente Parte Speciale trovano tutti come presupposto l'instaurazione di rapporti con la P.A. (comprendendo in tale definizione anche la P.A. di Stati esteri).

Si indicano pertanto qui di seguito alcuni criteri generali per la definizione di "Pubblica Amministrazione", "Pubblici Ufficiali" e "Incaricati di Pubblico Servizio".

A.1.1 Enti della Pubblica Amministrazione

Agli effetti della legge penale, viene comunemente considerato come "Ente della Pubblica Amministrazione" qualsiasi persona giuridica che abbia in cura interessi pubblici e che svolga attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.

A titolo esemplificativo, si possono indicare quali soggetti della Pubblica Amministrazione, i seguenti Enti o categorie di Enti:

- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Agenzia delle Entrate, Magistratura ordinaria e amministrativa);

- Regioni, Province e Comuni;

- Società municipalizzate;

- Autorità di Vigilanza (quali ad esempio Banca d'Italia, Consob, AGCM);

- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;

- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAI, INPDAP, ISTAT, ENASARCO);

- ASL;

- Enti e Monopoli di Stato;

- Soggetti di diritto privato che esercitano un pubblico servizio (ad esempio, Cassa Depositi e Prestiti, Ferrovie dello Stato);

- Fondazioni di previdenza ed assistenza.

Fermo restando la natura puramente esemplificativa di tale elenco, si evidenzia come non tutte le persone fisiche che agiscono nella sfera ed in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di Reati nei rapporti con la P.A.

In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali" e degli "Incaricati di Pubblico Servizio".

A.1.2 Pubblici Ufficiali

L'art. 357 c.p. definisce **pubblici ufficiali** "*coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa*", precisando che "*è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi*".

Il Codice Penale prevede quindi 3 tipi di pubbliche funzioni: legislativa, giudiziaria ed amministrativa.

Le prime due (legislativa e giudiziaria) non sono definite espressamente dall'art. 357 c.p. perché presentano caratteristiche tipiche che consentono una loro immediata individuazione; infatti:

- la funzione legislativa è l'attività svolta dagli organi pubblici (Parlamento, Regioni e Governo) che, secondo la Costituzione italiana, hanno il potere di emanare atti aventi valore di legge;
- la funzione giudiziaria è l'attività svolta dagli organi giudiziari (civili, penali e amministrativi) e dai loro ausiliari (cancelliere, segretario, perito, interprete, etc.), per l'applicazione della legge al caso concreto.

La funzione amministrativa, così come definita dal comma secondo dell'art. 357 è un'attività che si caratterizza per il fatto di essere disciplinata da norme di diritto pubblico o da atti autoritativi della P.A. (e ciò la differenzia dalle attività di natura privatistica che sono disciplinate da strumenti di diritto privato, quali il contratto) e per la circostanza di essere accompagnata dalla titolarità di almeno uno dei seguenti tre poteri:

- potere di formare e manifestare la volontà della P.A. (ad es.: sindaco o assessore

di un comune, componenti di commissioni di gare di appalto, dirigenti di aziende pubbliche, etc.);

- potere autoritativo, che comporta l'esercizio di potestà attraverso le quali si esplica il rapporto di supremazia della P.A. nei confronti dei privati cittadini (ad esempio, gli appartenenti alle forze dell'ordine, i componenti delle commissioni di collaudo di lavori eseguiti per un ente pubblico, i funzionari degli organismi di vigilanza – Banca d'Italia e Consob – etc.);
- potere certificativo, vale a dire potere di redigere documentazione alla quale l'ordinamento giuridico attribuisce efficacia probatoria privilegiata (ad es. notai).

Per fornire infine un contributo pratico alla risoluzione di eventuali "casi dubbi", può essere utile ricordare che assumono la qualifica di pubblici ufficiali non solo i soggetti al vertice politico - amministrativo dello Stato o di enti territoriali, ma anche tutti coloro che, in base allo statuto, nonché alle deleghe che esso consenta, ne formino legittimamente la volontà e/o la portino all'esterno in forza di un potere di rappresentanza.

A.1.3 Incaricati di un pubblico servizio

La definizione della categoria di "soggetti incaricati di un pubblico servizio" si rinviene all'art. 358 c.p. il quale recita che "*sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio.*

Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale".

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

Esempi di incaricati di pubblico servizio sono: i dipendenti delle autorità di vigilanza che non concorrono a formare la volontà dell'autorità e che non hanno poteri autoritativi, i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati, gli impiegati degli uffici pubblici, etc.

CAPITOLO A.2

Le fattispecie dei reati nei rapporti con la Pubblica Amministrazione (artt. 24 e 25 del D.Lgs. 231/2001)

La presente Parte Speciale si riferisce ai reati realizzabili nell'ambito dei rapporti tra la Società e la P.A.. Si descrivono brevemente qui di seguito le singole fattispecie contemplate nel D.Lgs. 231/2001 agli artt. 24 e 25.

A.2.1 Reati di tipo corruttivo

CORRUZIONE PER UN ATTO D'UFFICIO E AMBITO APPLICATIVO (ARTT. 318 E 320 C.P.)

L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale, per compiere un atto di propria competenza riceve, per sé o per un terzo, in denaro o altra utilità, una retribuzione che non gli è dovuta o ne accetta la promessa (si pensi ad esempio al caso in cui al fine di velocizzare l'ottenimento di un'autorizzazione da parte della Consob, un Esponente Aziendale prometta al pubblico ufficiale competente l'assunzione o l'attribuzione di una consulenza fittizia ad un suo familiare).

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da sei mesi a tre anni.

Ai sensi dell'art. 320 c.p. le disposizioni di cui all'art. 318 c.p. si applicano anche alla persona incaricata di un pubblico servizio, qualora rivesta la qualità di pubblico impiegato: in tali casi, tuttavia, le pene previste dal legislatore sono ridotte fino ad un terzo rispetto alle fattispecie delittuose che vedono coinvolto un pubblico ufficiale.

CORRUZIONE PER UN ATTO CONTRARIO AI DOVERI DI UFFICIO, CIRCOSTANZE AGGRAVANTI E AMBITO APPLICATIVO (ARTT. 319, 319 BIS E 320 C.P.)

L'ipotesi di reato di cui all'art. 319 c.p. si configura nel caso in cui il pubblico ufficiale, per compiere un atto contrario ai suoi doveri di ufficio o per omettere o ritardare un atto del suo ufficio riceve, per sé o per un terzo, in denaro o altra utilità, una retribuzione che non gli è dovuta o ne accetta la promessa (si pensi ad esempio ad ipotesi corruttive nei confronti dei funzionari ISVAP da parte di Esponenti Aziendali o a mezzo di Consulenti per impedire la comminazione di sanzioni pecuniarie).

Ai fini della configurabilità di tale reato in relazione al compimento di un atto contrario ai doveri di ufficio vanno considerati sia gli atti illegittimi o illeciti (vietati, cioè, da norme imperative o contrastanti con norme dettate per la loro validità ed efficacia) sia quegli atti che, pur formalmente regolari, siano stati posti in essere dal pubblico ufficiale violando il dovere d'imparzialità o asservendo la sua funzione ad interessi privati o comunque estranei a quelli proprio della Pubblica Amministrazione.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da due a cinque anni.

Per questa fattispecie di reato la pena può essere aumentata ai sensi dell'art. 319 *bis* c.p. qualora l'atto contrario ai doveri di ufficio abbia ad oggetto il conferimento di pubblici impieghi, stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene.

Ai sensi dell'art. 320 c.p., le disposizioni dell'art. 319 c.p. si applicano anche all'incaricato di un pubblico servizio: in tali casi, tuttavia, le pene previste dal legislatore sono ridotte fino ad un terzo rispetto alle fattispecie delittuose che vedono coinvolto un pubblico ufficiale.

*****

Ai sensi dell'art. 321 c.p. le pene previste dagli artt. 318 e 319 c.p. si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il danaro o altra utilità.

Si sottolinea infine come le ipotesi di reato di cui agli artt. 318 e 319 c.p. si differenzino dalla concussione in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato del pubblico servizio.

CORRUZIONE IN ATTI GIUDIZIARI (ART. 319 TER C.P.)

Tale ipotesi di reato si configura nel caso in cui, per favorire o danneggiare una parte in un procedimento giudiziario, si corrompa un pubblico ufficiale, e dunque un magistrato, un cancelliere o altro funzionario dell'autorità giudiziaria (si pensi ad esempio al caso in cui un Esponente Aziendale della Società faccia "pressioni" su un Pubblico Ministero per ottenere una richiesta di archiviazione di un procedimento penale).

E' importante sottolineare come il reato possa configurarsi a carico della Società indipendentemente dal fatto che la stessa sia parte del procedimento.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da tre a venti anni, a seconda se dal fatto derivi un'ingiusta condanna e del tipo di ingiusta condanna inflitta.

ISTIGAZIONE ALLA CORRUZIONE (ART. 322 C.P.)

Tale ipotesi di reato si configura nel caso in cui venga offerto o promesso danaro o altra utilità ad un pubblico ufficiale o incaricato di pubblico servizio (per indurlo a compiere, omettere o ritardare un atto di sua competenza o compiere un atto contrario ai suoi doveri di ufficio) e tale offerta o promessa non venga accettata.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la pena prevista per la fattispecie di cui all'art. 318 c.p., ridotta di un terzo, qualora l'offerta o la promessa sia fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio a compiere un atto del suo ufficio; qualora invece l'offerta o la promessa sia fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o ritardare un atto del suo ufficio, la pena è quella prevista per la fattispecie di cui all'art. 319 c.p., ridotta di un terzo.

*****

Con riferimento alle fattispecie di reato di cui al presente paragrafo A.2.1, profili di rischio in capo alla Società si individuano essenzialmente nelle ipotesi in cui gli Esponenti Aziendali e/o i Consulenti della stessa agiscano quali corruttori nei confronti di pubblici ufficiali o incaricati di pubblico servizio.

Per quanto riguarda invece la cd. corruzione passiva, la Società non potrebbe commettere il reato in proprio in quanto essa è sprovvista della necessaria qualifica pubblicistica; potrebbe tuttavia concorrere in un reato di corruzione commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, nel caso in cui fornisse un qualsiasi di sostegno, materiale o morale ai sensi dell'art. 110 c.p., al pubblico funzionario per la commissione del reato. A tal riguardo, si precisa che sussiste l'ipotesi del concorso nel reato di corruzione, anche quando si agisca quale mediatore tra il privato e il pubblico funzionario.

A.2.2 La concussione

CONCUSSIONE (ART. 317 C.P.)

La concussione consiste nella strumentalizzazione, da parte del pubblico ufficiale o dell'incaricato del pubblico servizio, della propria qualifica soggettiva o delle attribuzioni ad essa connesse, al fine di costringere o indurre taluno alla dazione o alla promessa di prestazioni non dovute (denaro o altre utilità).

Anche la concussione, al pari della corruzione, è un reato bilaterale, in quanto richiede la condotta di due distinti soggetti, il concussore ed il concusso.

Tuttavia, a differenza della corruzione, solo il concussore è assoggettato a pena, in quanto il concusso è la vittima del reato: pertanto, per la natura privatistica dell'attività svolta dalla Società, i suoi esponenti non potrebbero commettere il reato in proprio in quanto sprovvisti della necessaria qualifica pubblicistica; i medesimi potrebbero tutt'al più concorrere in un reato di concussione commesso da un pubblico ufficiale o da un incaricato di pubblico servizio ai sensi dell'art. 110 c.p.

Inoltre, è astrattamente possibile che un dipendente della Società rivesta, al di fuori dell'attività lavorativa, una pubblica funzione o svolga un pubblico servizio: si pensi al dipendente della Società che svolga l'incarico di componente di una giunta comunale. In tale ipotesi, questi, nello svolgimento del proprio ufficio o servizio, dovrà astenersi dal tenere comportamenti che, in violazione dei propri doveri d'ufficio e/o con abuso delle proprie funzioni, siano idonei a recare un vantaggio alla Società.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da quattro a dodici anni.

A.2.3 Le ipotesi di truffa

TRUFFA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ART. 640, COMMA 2, N. 1 C.P.)

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifizi e raggiri (intendendosi inclusa in tale definizione anche l'eventuale omissione di informazioni che, se conosciute, avrebbero certamente

determinato in senso negativo la volontà dello Stato, di altro ente pubblico o dell'Unione Europea) tali da indurre in errore e da arrecare un danno (di tipo patrimoniale) a tali enti.

Si pensi, in particolare, alla trasmissione all'amministrazione finanziaria di documentazione contenente false informazioni al fine di ottenere un rimborso fiscale non dovuto; ovvero, più in generale, all'invio ad enti previdenziali o amministrazioni locali di comunicazioni contenenti dati falsi in vista di un qualsiasi vantaggio o agevolazione per la Società.

Si pensi, ancora, alla falsa prospettazione dolosa di determinati vantaggi a seguito della sottoscrizione di uno strumento finanziario che già *ex ante* non possiede tali caratteristiche vantaggiose.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da uno a cinque anni e la multa da Euro 309 a Euro 1.549.

TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (ART. 640 BIS C.P.)

Il reato in oggetto si perfeziona allorquando i fatti di cui al precedente art. 640 c.p. riguardano l'ottenimento di contributi, finanziamenti o altre erogazioni concesse dallo Stato, da altri enti pubblici o dall'Unione Europea.

Si pensi ad esempio alle ipotesi di indebito ottenimento di un finanziamento pubblico finalizzato al sostegno delle attività imprenditoriali in determinati settori, mediante la produzione di falsa documentazione attestante la sussistenza dei requisiti per l'ottenimento del finanziamento.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da uno a sei anni.

FRODE INFORMATICA (ART. 640 TER C.P.)

Si configura il reato di frode informatica quando, al fine di procurare a sé o ad altri un ingiusto profitto, venga alterato in qualsiasi modo il funzionamento di un sistema informatico, o si intervenga, senza diritto, su dati, informazioni o programmi contenuti in un sistema informatico.

Ad esempio, integra il reato la modificazione delle informazioni relative alla situazione contabile di un rapporto contrattuale in essere con un ente pubblico, ovvero l'alterazione dei dati fiscali e/o previdenziali contenuti in una banca dati facente capo alla P.A..

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da sei mesi a cinque anni.

A.2.4 Le ipotesi di malversazione e di indebita percezione di erogazioni

MALVERSAZIONE A DANNO DELLO STATO (ART. 316 BIS C.P.)

Tale ipotesi di reati su configura nei confronti di chiunque, avendo ottenuto dallo Stato, da altro ente pubblico o dall'Unione Europea contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destina a tali attività.

Per l'integrazione del reato è sufficiente che anche solo una parte delle attribuzioni ricevute sia stata impiegata per scopi diversi da quelli previsti, non rilevando, in alcun modo, che l'attività programmata sia stata comunque svolta. Risultano altresì irrilevanti le finalità che l'autore del reato abbia voluto perseguire, poiché l'elemento soggettivo del reato medesimo è costituito dalla volontà di sottrarre risorse destinate ad uno scopo prefissato.

Tipico esempio è rappresentato dall'ottenimento di un finanziamento pubblico erogato in vista dell'assunzione presso la società di personale appartenente a categorie privilegiate successivamente disattesa.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da sei mesi a quattro anni.

INDEBITA PERCEZIONE DI EROGAZIONI A DANNO DELLO STATO (ART. 316 TER C.P.)

Tale ipotesi di reato si configura nei casi in cui - mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o attestanti cose non vere ovvero mediante l'omissione di informazioni dovute - si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominati, concessi o erogati dallo Stato, da altri enti pubblici o dalla Unione Europea.

In questo caso, contrariamente a quanto visto in merito al reato precedente, a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie di cui all'art. 640 *bis* c.p. (truffa aggravata per il conseguimento di erogazioni pubbliche), nel

senso che si configura solo nei casi in cui la condotta non integri gli estremi del reato di cui a quest'ultima disposizione.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da sei mesi a tre anni e, nei casi meno gravi, una sanzione amministrativa tra Euro 5.164 ed Euro 25.822.

*****

Per ciò che concerne i reati di cui agli artt. 316 *bis,* 316 *ter* e 640 *bis* c.p., si precisa che i contributi e le sovvenzioni sono attribuzioni pecuniarie a fondo perduto che possono avere carattere periodico o *una tantum,* in misura fissa o determinata in base a parametri variabili, natura vincolata all'*an* o al *quantum* o di pura discrezionalità; i finanziamenti sono atti negoziali caratterizzati dall'obbligo di destinazione delle somme o di restituzione o da ulteriori e diversi oneri; i mutui agevolati sono erogazioni di somme di denaro con obbligo di restituzione per il medesimo importo, ma con interessi in misura minore a quelli praticati sul mercato.

***

INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA (ART. 377 BIS C.P.)

La Legge 3 agosto 2009, n. 116 ha introdotto un ulteriore art. 25-nonies per il reato di "induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" come previsto all'art. 377-bis c.p., applicando in tal caso all'ente la sanzione pecuniaria sino a cinquecento quote.

Ai sensi di tale ultimo articolo, salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere, è punito con la reclusione da due a sei anni.

CAPITOLO A.3

Attività Sensibili nei rapporti con la P.A.

Di seguito sono elencate le attività già esposte nella Parte Generale del presente Modello e che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001:

1. **Rapporti contrattuali con la P.A. o con soggetti incaricati di un pubblico servizio.**

   - *Negoziazione, stipulazione ed esecuzione di contratti/convenzioni con soggetti pubblici mediante procedure negoziate (affidamento o trattativa privata)*: si tratta dell'attività di negoziazione/stipulazione/esecuzione di Polizze e/o convenzioni con Enti Pubblici (Ente sottoscrittore e beneficiario / Ente sottoscrittore e beneficiari i dipendenti), Polizze con dipendenti o rappresentanti di Enti Pubblici quando tale loro ruolo sia noto (nell'ambito di un rapporto privatistico - "privati sensibili"), Polizze fidejussorie a soggetti privati in favore di Enti Pubblici e altri contratti non assicurativi con Enti Pubblici (es. consulenze, forniture, vendite di beni, ecc. a Enti Pubblici).

   - *Negoziazione/Stipulazione/esecuzione di contratti/convenzioni con soggetti pubblici ai quali si perviene mediante procedure ad evidenza pubblica (aperte o ristrette)*: si tratta di partecipazione a gare con Enti pubblici. Sebbene la Società partecipi a gare pubbliche solo occasionalmente, l'attività si considera potenzialmente a rischio in relazione alla possibilità di commettere reati di natura corruttiva al fine di aggiudicarsi una gara.

2. **Rapporti con le istituzioni e con le autorità di vigilanza.**

   - *Rapporti con organismi di vigilanza relativi allo svolgimento di attività regolate dalla normativa di riferimento e gestione dei rapporti per l'ottenimento di autorizzazioni e licenze per l'esercizio delle attività aziendali:* si tratta della gestione dei rapporti con ISVAP, UIF, GARANTE PRIVACY, CONSOB, ANTITRUST, BANCA D'ITALIA sia nell'attività ordinaria che in caso di ispezioni, degli adempimenti antiriciclaggio, e delle autorizzazioni, licenze per operazioni straordinarie nell'esercizio di attività aziendali.

- *Rapporti con l'amministrazione finanziaria:* si tratta della gestione degli adempimenti tributari e fiscali.
- *Rapporti con Enti previdenziali e assistenziali:* si tratta dell'amministrazione degli aspetti retributivi e previdenziali connessi al personale dipendente e ai collaboratori esterni e dei rapporti con enti previdenziali ed assistenziali (INPS, INAIL, Ufficio di Collocamento, ecc.).
- *Rapporti con i soggetti pubblici per gli aspetti che riguardano la sicurezza e l'igiene sul lavoro (D.Lgs. 81/08):* si tratta degli adempimenti legati alla normativa sulla sicurezza sul posto di lavoro e relativi rapporti con le autorità preposte al controllo, anche in caso di ispezioni.

3. **Gestione degli acquisti, delle consulenze, delle liberalità e delle sponsorizzazioni**

- *Promozioni commerciali e sponsorizzazioni ad Enti Pubblici:* si tratta della gestione delle richieste e dei contratti di sponsorizzazione per la realizzazione di restauri di immobili di interesse storico/artistico e per la realizzazione di iniziative di carattere culturale, sportivo, ecc. patrocinate da Enti Pubblici.

4. **Gestione dei contenziosi.**

- *Gestione dei contenziosi giudiziali in genere*: si tratta della gestione di un contenzioso relativo a qualunque tipologia di vertenza, escluso l'ambito della liquidazione tecnica (cause di lavoro, vertenze tributarie, contenzioso commerciale con agenti/broker, contenzioso societario nonché procedimenti penali per reati commessi nell'ambito delle attività aziendali ecc.).
- *Gestione del contenzioso relativo ai premi ed ai sinistri/liquidazioni danni:* si tratta della gestione di un contenzioso relativo alla attività di riscossione dei premi e di liquidazione dei sinistri vita e danni.

5. **Liquidazione sinistri per le polizze stipulate con gli enti pubblici.**

- La rischiosità astratta dell'attività è legata ad eventuali utilizzi distorti dello strumento polizza, nella misura in cui tale attività fosse finalizzata a

riconoscere una trattamento di maggior favore verso particolari soggetti al fine unico o prevalente di influenzarne l'imparzialità e l'autonomia di giudizio.

6. **Gestione delle verifiche / ispezioni (amministrative, fiscali, previdenziali, ecc.)**

   - Il rischio teorico è quello dell'utilizzo di strumenti volti ad indirizzare indebitamente gli esiti delle verifiche, ovvero ad agevolare l'iter di perfezionamento delle autorizzazioni richieste dalla legge.

7. **Gestione dei fondi pubblici erogati alla Società**

   - *Gestione di contributi/sovvenzioni/finanziamenti concessi da Enti Pubblici a favore della società:* si tratta della gestione delle richieste di contributi/sovvenzioni da soggetti pubblici.

8. **Gestione finanziaria**

   - Nell'ambito della gestione finanziaria della Compagnia potrebbe presentarsi la necessità di ottenere specifiche autorizzazioni dall'Autorità di Vigilanza per eventuali operazioni finanziarie di natura straordinaria (es. prestiti subordinati).

Attività strumentali alla commissione dei reati di tipo corruttivo

Alcune attività che non comportano rapporti diretti con la P.A. possono tuttavia essere strumentali alla commissione della tipologia di reati di tipo corruttivo.

Ciò può accadere:

1) quando l'attività costituisce strumento di creazione di disponibilità occulte, da utilizzare per la corruzione di pubblici ufficiali.

   Si pensi ad esempio al caso in cui la Società acquisti beni o servizi da Fornitori o affidi incarichi a Consulenti, pagando somme superiori al valore effettivo della

prestazione, con l'accordo che il fornitore/collaboratore restituirà parte del prezzo pagato attraverso modalità non regolari.

2) quando l'attività costituisce il mezzo per corrispondere, direttamente o per interposta persona, ai funzionari pubblici, in forma occulta o indiretta, denaro o altra utilità in cambio di interessamenti indebiti.

   Si indicano di seguito alcune tipologie di attività che possono comportare rischi nel senso sopra indicato:

   - *selezione del personale*: si pensi, ad esempio, alla prospettata assunzione di un familiare del pubblico funzionario (o, in futuro, dello stesso pubblico funzionario) presso la Società, in vista del compimento di atti in suo favore;
   - *gestione del personale*: può presentare profili di rischio nell'ipotesi in cui siano riconosciute ad un eventuale congiunto di un pubblico funzionario, dipendente della Società, privilegi o vantaggi professionali indebiti o non dovuti e collegati all'interessamento del pubblico funzionario medesimo in una pratica relativa alla Società;
   - *consulenza*: l'attribuzione di consulenze, può essere altresì utilizzata quale forma di retribuzione di prestazioni indebite erogate da pubblici funzionari; si pensi alla stipulazione di un contratto di consulenza a favore di un familiare di un pubblico funzionario, quale corrispettivo dell'interessamento da parte del medesimo in una pratica relativa alla Società;
   - *omaggistica*: la gestione delle prestazioni gratuite erogate in qualsiasi forma dalla Società a titolo di omaggio a favore della clientela o di terzi (omaggi in occasione di ricorrenze; pranzi e viaggi; servizi di qualsiasi natura etc.) si presenta a rischio, in quanto possibile forma di corresponsione di utilità non dovute a pubblici funzionari o soggetti ad essi collegati; si pensi all'invio ad un pubblico funzionario, in occasione della conclusione di un contratto o delle festività natalizie, di un omaggio quale corrispettivo all'interessamento di detto funzionario nella pratica relativa alla Società.

Eventuali modifiche o integrazioni delle suddette Aree a Rischio sono rimesse alla competenza dell'Amministratore Delegato e sottoposte annualmente al Consiglio di

Amministrazione che potrà procedere con la successiva attività di ratifica secondo quanto indicato nella Parte Generale del Modello.

CAPITOLO A.4

Regole e principi generali

A.4.1 Il sistema in linea generale

Obiettivo della presente Parte Speciale è che, da un lato, i Dipendenti, gli Organi Sociali, i soggetti che operano a livello periferico (agenti, sub-agenti, personale d'agenzia, promotori, broker), i dipendenti di CA Vita per i servizi prestati a CAA in virtù del contratto di servizio e, dall'altro, i Consulenti ed i Partner della Società, nei limiti delle rispettive pattuizioni contrattuali, che adottino regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire il verificarsi dei Reati in essa considerati.

Tutte le Attività Sensibili devono essere svolte conformandosi alle leggi vigenti, alle procedure ed ai regolamenti aziendali rilevanti nonché alle regole ed ai principi contenuti nel presente Modello.

In linea generale, il sistema di organizzazione della Società deve rispettare i requisiti fondamentali di formalizzazione e chiarezza, comunicazione e separazione dei ruoli in particolare per quanto attiene l'attribuzione di responsabilità, di rappresentanza, di definizione delle linee gerarchiche e delle attività operative.

La Società deve essere dotata di strumenti organizzativi (organigrammi, comunicazioni organizzative, procedure, ecc.) improntati a principi generali di:

a) conoscibilità all'interno della Società;

b) chiara e formale delimitazione dei ruoli, con una completa descrizione dei compiti di ciascuna funzione e dei relativi poteri;

c) chiara descrizione delle linee di riporto.

Le procedure interne della Società devono essere formalizzate in modo tale che siano rispettate le seguenti regole di carattere generale:

a) separatezza, all'interno di ciascun processo, tra il soggetto che lo inizia (impulso decisionale), il soggetto che lo esegue e lo conclude, e il soggetto che lo controlla;

b) traccia scritta di ciascun passaggio rilevante del processo;

c) adeguato livello di formalizzazione;

d) evitare che i sistemi premianti dei soggetti con poteri di spesa o facoltà decisionali a rilevanza esterna siano basati su *target* di performance sostanzialmente irraggiungibili.

A.4.2 Il sistema di deleghe e procure

In linea di principio, il sistema di deleghe e procure deve essere caratterizzato da elementi di "sicurezza" ai fini della prevenzione dei Reati (rintracciabilità ed evidenziabilità delle Operazioni Sensibili) e, nel contempo, consentire comunque la gestione efficiente dell'attività aziendale.

Si intende per "delega" quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative. Si intende per "procura" il negozio giuridico unilaterale con cui la Società attribuisce dei poteri di rappresentanza nei confronti dei terzi. Ai titolari di una funzione aziendale che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza viene conferita una "procura" di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la "delega".

I requisiti essenziali del sistema di **deleghe**, ai fini di una efficace prevenzione dei Reati sono i seguenti:

a) tutti coloro (Dipendenti e Organi Sociali) che intrattengono per conto della Società rapporti con la P.A. devono essere dotati di delega formale in tal senso (la Rete Distributiva, i Consulenti e i Partner Commerciali devono essere in tal senso incaricati nello specifico mandato-accordo distributivo, contratto di consulenza o *partnership*);

b) le deleghe devono coniugare ciascun potere di gestione alla relativa responsabilità e ad una posizione adeguata nell'organigramma ed essere aggiornate in conseguenza dei mutamenti organizzativi;

c) ciascuna delega deve definire in modo specifico ed inequivoco:

- i poteri del delegato;
- il soggetto (organo o individuo) cui il delegato riporta gerarchicamente o *ex lege* o statutariamente;

d) i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali;

e) il delegato deve disporre di poteri di spesa adeguati alle funzioni conferitegli.

Il sistema di deleghe esistente nella Società è declinato nell'organigramma e funzionigramma aziendale, il quale si ispira ai principi e alle regole sopra indicate. In caso

di assunzione di nuove responsabilità, trasferimento a diverse mansioni incompatibili con quelle per cui la delega è stata conferita ovvero dimissioni, licenziamento o altra causa, tale organigramma e funzionigramma deve essere tempestivamente aggiornato dalle funzioni *Organizzazioni* deputate all'aggiornamento dell'organigramma e funzionigramma aziendale, su segnalazione del dirigente responsabile del soggetto interessato e la procura notarile viene revocata nel primo C.d.A. utile. Il documento aggiornato sarà successivamente trasmesso da parte del predetto Ufficio a tutti i dirigenti responsabili della Società e all'OdV.

* * *

I requisiti essenziali del sistema di attribuzione delle **procure**, ai fini di una efficace prevenzione dei Reati sono i seguenti:

a) le procure funzionali sono conferite esclusivamente per il compimento di specifiche attività a soggetti dotati di delega interna che descriva i relativi poteri di gestione;

b) le procure eventualmente rilasciate a funzioni esternalizzate, anche presso CAV a favore di CAA, sono conferite esclusivamente per il compimento di specifiche attività funzionali allo svolgimento dell'incarico;

c) le procure che dovessero eventualmente essere rilasciate alla Rete Distributiva, anche nell'ambito dei contratti di distribuzione, sono conferite esclusivamente per il compimento di un affare specifico o per oggetti determinati funzionali alla realizzazione di un determinato affare;

d) le procure devono essere tempestivamente aggiornate in caso di assunzione di nuove responsabilità, trasferimento a diverse mansioni incompatibili con quelle per cui era stata conferita, dimissioni, licenziamento, ecc. A tale aggiornamento provvede funzione Affari legali e societari, su segnalazione del dirigente responsabile del soggetto interessato;

e) le procure che attribuiscono un potere di firma singola fissano limiti di spesa; sono inoltre accompagnate da apposita disposizione interna che fissa, oltre ai limiti di spesa, l'estensione dei poteri di rappresentanza;

L'OdV verifica periodicamente, con il supporto delle altre funzioni competenti, il rispetto del sistema di deleghe e procure attuato dalla Società e la loro coerenza con i principi e le regole generali sopra indicate. Nel contempo, all'esito delle verifiche l'OdV

raccomanda le eventuali modifiche o integrazioni allorquando il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti al procuratore o vi siano altre anomalie.

A.4.3 Principi generali di comportamento

I seguenti principi di carattere generale si applicano ai Destinatari, come meglio individuati nel paragrafo A.4.1.

In via generale, è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate; sono altresì proibite le violazioni ai principi ed alle procedure aziendali previste nella presente Parte Speciale.

In particolare:

a) è fatto divieto di accordare vantaggi di qualsiasi natura (denaro, promesse di assunzione, ecc.) in favore di rappresentanti della P.A. italiana o straniera, o a loro familiari, rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale o che possa comunque influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda;

b) è fatto divieto di distribuire omaggi al di fuori di quanto previsto dalle *policy* aziendali (vale a dire ogni forma di omaggio offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi forma di omaggio a rappresentanti della P.A. o a loro familiari che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore e, pertanto, non potranno essere superiori a Euro 250 annuali per singolo destinatario, salvo deroghe approvate per iscritto (a livello generale per categorie di omaggi o in modo specifico per singoli omaggi) dall'Amministratore Delegato con l'indicazione della motivazione sottesa al compimento dell'atto di liberalità, sentito l'OdV;

c) è vietato eseguire erogazioni liberali e donazioni in favore di enti pubblici o soggetti incaricati di un pubblico servizio in difformità a quanto previsto dalle apposite procedure interne (emanate sulla base del principio procedurale di cui al successivo

paragrafo A.5.1, punto 8) e dalle regole aziendali al riguardo dettate dall'OdV o dagli Organi Sociali;

d) è fatto divieto di accettare qualsiasi tipo di regalo d'affari e/o di vantaggio che possa compromettere l'indipendenza, l'imparzialità e l'integrità dei dipendenti (o dei componenti degli Organi Sociali) della Società. A questo fine, la Società ha fissato un importo pari a Euro 150 quale limite massimo di valore per gli omaggi ricevuti sia da clienti sia da fornitori sia da terzi in genere. Tale limite si intende su base annua;

e) è vietato effettuare prestazioni in favore dei Consulenti e dei Partner Commerciali che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi, nonché riconoscere compensi in favore medesimi che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti nel settore;

f) per i contratti di assicurazione contro i danni, è vietato ricevere denaro contante a titolo di pagamento di premi di importo superiore a Euro 750,00 annui (Euro settecentocinquanta) per ciascun contratto; il limite di incasso di premi in contanti per il ramo r.c. auto è invece di 1.000,00 euro (Euro mille).

g) **CAPITOLO A.5**

Principi procedurali specifici

A.5.1 Principi procedurali specifici generalmente applicabili

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente cap. 4, devono rispettarsi gli specifici principi procedurali qui di seguito descritti, oltre alle regole e principi generali contenuti nella Parte Generale del Modello. Le regole qui di seguito descritte, devono essere rispettate sia nell'esplicazione dell'attività di CAA in territorio italiano, sia eventualmente all'estero.

1. Ai Dipendenti, Organi Sociali, Rete Distributiva, dipendenti di CA Vita per i servizi prestati a CAA, Consulenti e Partner che materialmente intrattengono rapporti con la P.A. per conto di CAA deve essere formalmente conferito potere in tal senso dalla stessa Società (con apposita delega per i Dipendenti e gli Organi Sociali ovvero nel relativo mandato, contratto di consulenza o di partnership per gli altri soggetti indicati). Ove sia necessaria, sarà rilasciata ai soggetti predetti specifica procura scritta che rispetti tutti i criteri elencati al precedente Capitolo A.4.2;

2. di qualunque criticità o conflitto di interesse sorga nell'ambito del rapporto con la P.A. deve esserne informato tempestivamente l'OdV con nota scritta;

3. i contratti tra CAA e la Rete Distributiva, i Consulenti e Partner devono essere definiti per iscritto in tutte le loro condizioni e termini e rispettare quanto indicato ai successivi punti;

4. i contratti con la Rete Distributiva, i Consulenti e i Partner devono contenere clausole standard, definite di comune accordo dall'Amministratore Delegato sentito l'OdV, al fine del rispetto da parte degli stessi del D. Lgs. 231/2001 e del Codice Etico;

5. i Consulenti e Partner Commerciali devono essere scelti con metodi trasparenti e meritocratici;

6. nei contratti con la Rete Distributiva, i Consulenti e i Partner deve essere contenuta apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D. Lgs. 231/2001 e delle sue implicazioni per la Società, di non essere mai stati implicati in procedimenti giudiziari relativi ai Reati nello stesso contemplati (o se lo sono stati, devono comunque dichiararlo ai fini di una maggiore attenzione da parte della Società in caso si addivenga all'instaurazione del rapporto di distribuzione

assicurativa, consulenza o partnership), di impegnarsi a tenere un comportamento tale da non incorrere nei Reati previsti dal D.Lgs. 231/2001;

7. nei contratti con la Rete Distributiva, i Consulenti e i Partner deve essere contenuta apposita clausola che regoli le conseguenze della commissione (o tentativo di commissione) da parte degli stessi dei Reati di cui al D.Lgs. 231/2001 (es. clausole risolutive espresse o penali);

8. nei contratti con i legali esterni ai quali vengono conferiti incarichi di natura contenziosa devono essere apposte specifiche clausole che prevedano il rispetto dei principi etici adottati dalla Società e la facoltà della stessa di revocare i mandati in questione nel caso di violazione di tale obbligo;

9. le erogazioni liberali e donazioni in favore di enti pubblici devono essere deliberate dal Consiglio di Amministrazione e deve essere indicata la motivazione sottesa al compimento dell'atto di liberalità;

10. alle ispezioni o verifiche condotte da pubbliche autorità (es. relative al D.Lgs. 81/08, verifiche tributarie, INPS, ISVAP, ecc.) devono partecipare i soggetti a ciò espressamente delegati. Di tutto il procedimento relativo all'ispezione o verifica devono essere redatti e conservati gli appositi verbali interni che tengano conto delle problematiche emerse nel corso del procedimento ispettivo. Nel caso il verbale conclusivo evidenziasse criticità, l'OdV ne deve essere informato con nota scritta da parte del responsabile della funzione coinvolta;

11. l'ottenimento di fondi pubblici deve essere basato su principi di correttezza e trasparenza;

12. la gestione dei fondi ricevuti da entità pubbliche deve essere coerente con gli scopi per i quali il finanziamento è stato chiesto ed ottenuto;

13. la liquidazione dei sinistri deve essere eseguita nel rispetto delle procedure aziendali che ne regolano l'*iter*.

A.5.2 Principi procedurali specifici nel caso di particolari Attività Sensibili

Le operazioni di negoziazione/stipulazione/esecuzione di contratti/convenzioni con soggetti pubblici o incaricati di un pubblico servizio mediante procedure negoziate (affidamento diretto o trattativa privata) o mediante procedure ad evidenza pubblica

(aperte o ristrette) e, in generale tutti i rapporti con la Pubblica Amministrazione, devono avere debita evidenza ed uniformità di gestione, essendo queste considerate, alla luce del Modello, come Attività Sensibili.

In particolare, i Responsabili delle Funzioni aziendali che sono coinvolte nello svolgimento delle operazioni sensibili di cui sopra devono:

- comunicare - attraverso la redazione di report informativi - all'Organismo di Vigilanza qualunque anomalia o criticità riscontrata nel corso dello svolgimento dell'attività nell'ambito della funzione di competenza;

- verificare la concreta ed efficace attuazione – nell'ambito delle Direzioni e/o funzioni di competenza – delle procedure aziendali e dei principi di cui al presente Modello di organizzazione, gestione e controllo.

- prevedere idonei sistemi di controllo (anche attraverso flussi informativi) che consentano di verificare la regolarità delle richieste di informazioni avanzate dalla Società nei confronti degli uffici competenti della Pubblica Amministrazione, ovvero delle richieste avanzate nei confronti di CAA da esponenti della Pubblica Amministrazione;

- assicurare la correttezza e veridicità dei documenti e delle informazioni fornite dalla Società nei confronti della Pubblica Amministrazione o di altro Ente Pubblico;

- documentare in modo idoneo, su supporto cartaceo o informatico, i principali adempimenti eseguiti dalla funzione aziendale preposta nel corso delle relazioni o dei contatti stretti con la Pubblica Amministrazione o con altro Ente pubblico.

CAPITOLO A.6

I controlli dell'OdV

A.6.1 Il controllo in generale

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui agli artt. 24 e 25 del Decreto, commessi nell'interesse o a vantaggio della Società anche tramite la rete distributiva del Gruppo Cariparma, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

I compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati di cui agli artt. 24 e 25 del Decreto sono i seguenti:

(i) proporre che vengano costantemente aggiornate le procedure aziendali per prevenire la commissione dei reati nei rapporti con la Pubblica Amministrazione, di cui alla presente Parte Speciale; con riferimento a tale punto l'Organismo di Vigilanza condurrà controlli a campione sulle attività potenzialmente a rischio di commissione dei suddetti reati, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere; o proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Aree Sensibili individuate nella presente Parte Speciale;

(ii) monitoraggio sul rispetto delle procedure interne per la prevenzione dei reati oggetto della presente Parte Speciale. Sulla base dei flussi informativi ricevuti l'Organismo di Vigilanza condurrà verifiche mirate su determinate operazioni effettuate nell'ambito delle aree a rischio, volte ad accertare da un lato il rispetto di quanto stabilito nel Modello e nei protocolli, dall'altro l'effettiva adeguatezza delle prescrizioni in essi contenute a prevenire i reati potenzialmente commissibili;

(iii) esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute. L'Organismo di Vigilanza, inoltre, è

tenuto alla conservazione dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

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

PARTE SPECIALE – B –

Reati Societari

CAPITOLO B.1

Le fattispecie dei reati societari (art. 25-*ter* del D.Lgs. 231/2001).

La presente Parte Speciale si riferisce ai reati societari.

Si provvede qui di seguito a fornire una breve descrizione dei reati contemplati nella presente Parte Speciale, così come indicati all' art. 25-*ter* del Decreto (di seguito i "Reati Societari").

B.1.1 Le ipotesi di falsità

FALSE COMUNICAZIONI SOCIALI (ART. 2621 C.C.)

FALSE COMUNICAZIONI SOCIALI IN DANNO DELLA SOCIETÀ, DEI SOCI O DEI CREDITORI (ART. 2622 C.C.)

L'ipotesi di reato di cui all'art. 2621 c.c. si configura nel caso in cui nell'intento di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, vengano esposti, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero vengano omesse informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione.

L'ipotesi di reato di cui all'art. 2622 c.c. si configura nel caso in cui, nell'intento di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, vengano esposti nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, ovvero vengano omesse informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionando un danno patrimoniale alla società, ai soci o ai creditori.

Pertanto, le due ipotesi di reato di cui agli articoli 2621 e 2622 c.c., prevedono una condotta che coincide quasi totalmente e si differenziano solo per il verificarsi (art. 2622 c.c.) o meno (art. 2621 c.c.) di un danno patrimoniale alla società, ai soci o ai creditori.

Si precisa che:

- le informazioni false o omesse devono essere tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene;
- la responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

Si rileva altresì come l'esposizione di fatti non rispondenti al vero o l'occultamento di informazioni può essere realizzata non soltanto attraverso la materiale alterazione di dati contabili ma anche attraverso una valutazione artificiosa di beni o valori inseriti in dette comunicazioni.

Soggetti attivi di tali reati sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori.

La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.

In ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscano in misura non superiore al 10 per cento da quella corretta.

La pena prevista per il soggetto che realizzi la fattispecie criminosa di cui all'art. 2621 c.c. è l'arresto fino a due anni e la reclusione da sei mesi a sei anni per la fattispecie criminosa di cui all'art. 2622 c.c.

OMESSA COMUNICAZIONE DEL CONFLITTO DI INTERESSI (ART. 2629 BIS C.C.)

Tale ipotesi di reato, non ipotizzabile per CAA in quanto società non quotata nei mercati regolamentati, consiste nella violazione degli obblighi previsti dall'art. 2391, primo comma c.c. da parte dell'amministratore di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea (ovvero di altri soggetti sottoposti a vigilanza), se dalla predetta violazione siano derivati danni alla società o a terzi.

L'art. 2391, primo comma c.c. impone agli amministratori delle società per azioni di dare notizia agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata. Gli amministratori delegati devono altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale. L'amministratore unico deve darne notizia anche alla prima assemblea utile.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione da uno a tre anni se dalla violazione siano derivati danni alla società o a terzi.

B.1.2 La tutela del capitale sociale

INDEBITA RESTITUZIONE DEI CONFERIMENTI (ART. 2626 C.C.)

Il reato in questione, come quello previsto dal successivo art. 2627 c.c., riguarda la tutela dell'integrità del capitale sociale e si compie quando gli amministratori, in assenza di legittime ipotesi di riduzione del capitale sociale, provvedono a restituire, anche per equivalente, i conferimenti effettuati dai soci ovvero liberano i soci dall'obbligo di eseguirli. Il reato in esame assume rilievo solo quando, per effetto degli atti compiuti dagli amministratori, si intacca il capitale sociale e non i fondi o le riserve. Per questi ultimi, eventualmente, sarà applicabile il reato contemplato dal successivo art. 2627 c.c.

La restituzione dei conferimenti può essere palese (quando gli amministratori restituiscono beni ai soci senza incasso di alcun corrispettivo o rilasciano dichiarazioni dirette a liberare i soci dai loro obblighi di versamento) ovvero, più probabilmente, simulata (quando per realizzare il loro scopo gli amministratori utilizzano stratagemmi o artifici quali, per esempio, la distribuzione di utili fittizi con somme prelevate dal capitale sociale e non dalle riserve, oppure la compensazione del credito vantato dalla società con crediti inesistenti vantati da uno o più soci).

Soggetti attivi del reato possono essere solo gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della restituzione o della liberazione, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione fino ad un anno.

ILLEGALE RIPARTIZIONE DEGLI UTILI E DELLE RISERVE (ART. 2627 C.C.)

Tale ipotesi di reato consiste nella ripartizione di utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, ovvero nella ripartizione di riserve (anche non costituite con utili) che non possono per legge essere distribuite.

Si fa presente che la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio estingue il reato.

Soggetti attivi del reato sono gli amministratori. La legge, cioè, non ha inteso punire anche i soci beneficiari della ripartizione degli utili o delle riserve, escludendo il concorso necessario. Resta, tuttavia, la possibilità del concorso eventuale, in virtù del quale risponderanno del reato, secondo le regole generali del concorso di cui all'art. 110 c.p., anche i soci che hanno svolto un'attività di istigazione o di determinazione della condotta illecita degli amministratori.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è l'arresto fino ad un anno.

ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE (ART. 2628 C.C.)

Tale ipotesi di reato consiste nel procedere – fuori dai casi consentiti dalla legge – all'acquisto o alla sottoscrizione di azioni o quote emesse dalla società (o dalla società controllante) che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

La norma è diretta alla tutela dell'effettività e integrità del capitale sociale e non può prescindere dall'analisi di cui all'art. 2357 c.c. il quale prevede che la società per azioni non può acquistare azioni proprie, nemmeno tramite società fiduciaria o interposta persona, se non nei limiti degli utili distribuibili o delle riserve disponibili risultanti dall'ultimo bilancio regolarmente approvato. La norma prevede che le azioni devono essere interamente liberate e che, inoltre, non possono essere acquistate azioni eccedenti la decima parte del capitale sociale, tenuto conto anche delle azioni possedute dalle società controllate.

Tra le fattispecie tramite le quali può essere realizzato l'illecito vanno annoverate non solo le ipotesi di semplice acquisto ma anche quelle di trasferimento della proprietà delle azioni, per esempio, mediante permuta o contratti di riporto, o anche quelle di trasferimento senza corrispettivo, quale la donazione.

Soggetti attivi del reato sono gli amministratori. Inoltre, è configurabile una responsabilità a titolo di concorso degli amministratori della controllante con quelli della controllata, nell'ipotesi in cui le operazioni illecite sulle azioni della controllante medesima siano effettuate da questi ultimi su istigazione dei primi.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione fino ad un anno.

OPERAZIONI IN PREGIUDIZIO DEI CREDITORI (ART. 2629 C.C.)

Tale ipotesi di reato consiste nell'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o di fusioni con altra società o di scissioni, tali da cagionare danno ai creditori.

Si fa presente che:

- il risarcimento del danno ai creditori prima del giudizio estingue il reato.

Il reato è punibile a querela di parte.

Soggetti attivi del reato sono, anche in questo caso, gli amministratori.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione da sei mesi a tre anni.

FORMAZIONE FITTIZIA DEL CAPITALE (ART. 2632 C.C.)

Tale ipotesi di reato è integrata dalle seguenti condotte:

a) formazione o aumento in modo fittizio del capitale sociale, anche in parte, mediante attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale;

b) sottoscrizione reciproca di azioni o quote;

c) sopravvalutazione rilevante dei conferimenti di beni in natura, di crediti, ovvero del patrimonio della società nel caso di trasformazione.

Soggetti attivi del reato sono gli amministratori ed i soci conferenti.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione fino ad un anno.

B.1.3 La tutela del corretto funzionamento della società

IMPEDITO CONTROLLO (ART. 2625 C.C.)

Tale ipotesi di reato consiste nell'impedire od ostacolare, mediante occultamento di documenti o con altri idonei artifici, lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali, ovvero alle società di revisione.

Si pensi ad esempio all'occultamento di documenti essenziali per la verifica, in corso di esercizio, della regolare tenuta della contabilità sociale e la corretta rilevazione nelle scritture contabili dei fatti di gestione da parte della società di revisione.

L'illecito può essere commesso esclusivamente dagli amministratori.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la sanzione amministrativa pecuniaria fino ad Euro 10.392 e, qualora la condotta abbia cagionato un danno ai soci, la reclusione fino ad un anno.

ILLECITA INFLUENZA SULL'ASSEMBLEA (ART. 2636 C.C.)

Tale ipotesi di reato consiste nel determinare la maggioranza in assemblea con atti simulati o fraudolenti, allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Tra gli interventi che sono suscettibili di integrare il reato in questione, si possono annoverare ad esempio l'ammissione al voto di soggetti non aventi diritto (perché ad esempio, in conflitto di interessi con la delibera in votazione) o la minaccia o l'esercizio della violenza per ottenere dai soci l'adesione alla delibera o la loro astensione.

Il reato è costruito come un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione da sei mesi a tre anni.

B.1.4 La tutela penale contro le frodi

AGGIOTAGGIO (ART. 2637 C.C.)

Tale ipotesi di reato consiste nel diffondere notizie false ovvero nel realizzare 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 nell'incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o gruppi bancari.

Si pensi ad esempio al caso in cui vengano diffuse dalla Società degli studi su società non quotate con previsioni di dati e suggerimenti esagerati e/o falsi.

Anche questo è un reato comune, che può essere commesso da "chiunque" ponga in essere la condotta criminosa.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione da uno a cinque anni.

Sulla portata di tale condotta in relazione a strumenti finanziari quotati e sulle misure da predisporre per evitarne il verificarsi, si veda quanto riportato nella Parte Speciale relativa ai reati ed illeciti di abuso di mercato.

B.1.5 La tutela delle funzioni di vigilanza

OSTACOLO ALL'ESERCIZIO DELLE FUNZIONI DELLE AUTORITÀ PUBBLICHE DI VIGILANZA (ART. 2638 C.C.)

Si tratta di un'ipotesi di reato che può essere realizzata con due condotte distinte:

- la prima (i) attraverso l'esposizione nelle comunicazioni previste dalla legge alle autorità pubbliche di vigilanza, quali Consob o Banca d'Italia, (al fine di ostacolare l'esercizio delle funzioni di queste ultime) di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero (ii) mediante l'occultamento, con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati e concernenti la medesima situazione economica, patrimoniale o finanziaria.

La responsabilità sussiste anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;

- la seconda si realizza con il semplice ostacolo all'esercizio delle funzioni di vigilanza svolte da parte di pubbliche autorità, attuato consapevolmente ed in qualsiasi forma, anche omettendo le comunicazioni dovute alle autorità medesime.

Soggetti attivi del reato sono gli amministratori, i direttori generali, i sindaci ed i liquidatori.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione da uno a quattro anni, aumentata del doppio qualora si tratti di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 TUF.

CAPITOLO B.2

Attività Sensibili nell'ambito dei reati societari

Di seguito sono elencate le attività già esposte nella Parte Generale del presente Modello che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001:

- **comunicazioni esterne,** tra le quali rientrano:

  a) comunicazioni alle Autorità di vigilanza e gestione dei rapporti con le stesse: trattasi dei rapporti con le Autorità di vigilanza in merito agli adempimenti previsti in tema di comunicazioni dei dati societari;

  b) altre comunicazioni sociali previste dalla legge dirette ai soci o al pubblico: trattasi di informazioni relative ai bilanci e relazioni riguardanti la situazione economica, patrimoniale e finanziaria della Società al quale essa appartiene.

- **tenuta della contabilità, predisposizione di bilanci, relazioni, comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge e/o per disposizioni di Autorità di Vigilanza:** trattasi di contabilità in genere e bilanci, relazione semestrale, situazioni trimestrali, relazioni e prospetti allegati al bilancio e qualsiasi altro dato o prospetto richiesto da Autorità di vigilanza; ci si riferisce, altresì, ai rapporti con le Autorità di vigilanza in merito agli adempimenti previsti in tema di comunicazioni dei dati societari;

- **gestione dei rapporti con il Collegio Sindacale, società di revisione e altri organi Sociali, nonché redazione, tenuta e conservazione dei documenti su cui gli stessi potrebbero esercitare il controllo;**

- **gestione delle incombenze Societarie; operazioni sul capitale e operazioni sulle azioni:** trattasi degli adempimenti legislativi legati alla gestione delle attività in oggetto al fine di salvaguardare il patrimonio della società (operazioni su azioni; acconti su dividendi; conferimenti, fusioni e scissioni; distribuzione utili);

- **influenza sull'assemblea:** trattasi degli atti simulati o fraudolenti funzionali a procurare illecitamente una maggioranza assembleare; in questa Attività Sensibile viene in rilievo anche l'attività di preparazione delle riunioni assembleari.

CAPITOLO B.3

Regole e principi generali

B.3.1 Principi generali di comportamento

Obiettivo della presente Parte Speciale è che i Dipendenti, gli Organi Sociali, i Consulenti ed i soggetti dipendenti della Società CA Vita per i servizi prestati a CAA, si attengano – nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento delle attività nelle Attività Sensibili individuate in precedenza - a regole di condotta conformi a quanto prescritto in tale Parte Speciale e nelle policy e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire la commissione dei Reati Societari.

In particolare, gli Esponenti Aziendali, da un lato, e i Consulenti ed i soggetti dipendenti della Società CA Vita, dall'altro, nei limiti delle pattuizioni contrattuali, in relazione al tipo di rapporto in essere con la Società, dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati Societari;

2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

3. tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci ed al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della Società.

In ordine a tale punto, è fatto divieto di:

(i) predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società;

(ii) omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;

(iii) non attenersi ai principi e alle prescrizioni contenute nelle istruzioni predisposte o applicate dalla Società per la redazione dei bilanci;

4. osservare scrupolosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale ed agire sempre nel rispetto delle procedure interne aziendali che su tali norme si fondano, al fine di non ledere le garanzie dei creditori e dei terzi in genere al riguardo.

In ordine a tale punto, è fatto divieto di:

(i) restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;

(ii) ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;

(iii) acquistare o sottoscrivere azioni della Società o dell'eventuale società controllante fuori dai casi previsti dalla legge, con lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge;

(iv) effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;

(v) procedere in ogni modo a formazione o aumento fittizi del capitale sociale;

(vi) ripartire i beni sociali tra i soci – in fase di liquidazione – prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli;

5. assicurare il regolare funzionamento della Società e degli organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge, nonché la libera e corretta formazione della volontà assembleare.

In ordine a tale punto, è fatto divieto di:

(i) tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o della società di revisione o dei soci;

(ii) porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;

6. astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee 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.

In ordine a tale punto, è fatto divieto di pubblicare o divulgare notizie false, o porre in essere operazioni simulate o altri comportamenti di carattere fraudolento o ingannatorio suscettibili di determinare riflessi su strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato ed idonei ad alterarne sensibilmente il prezzo.

Per quanto riguarda gli strumenti finanziari quotati o per i quali è stata presentata una richiesta di ammissione alle negoziazioni o in un mercato regolamentato, si rinvia a quanto previsto nella Parte Speciale relativa ai reati ed illeciti amministrativi di abuso di mercato;

7. effettuare con tempestività, correttezza e completezza tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate.

In ordine a tale punto, è fatto divieto di:

(i) omettere di effettuare, con la dovuta chiarezza, completezza e tempestività, nei confronti delle Autorità in questione, (a) tutte le comunicazioni, periodiche e non, previste dalla legge e dalla ulteriore normativa di settore, nonché (b) la trasmissione dei dati e documenti previsti dalle norme in vigore e/o specificamente richiesti dalle predette Autorità;

(ii) esporre in tali comunicazioni e nella documentazione trasmessa fatti non rispondenti al vero oppure occultare fatti concernenti la situazione economica, patrimoniale o finanziaria della Società;

(iii) porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità pubbliche di Vigilanza, anche in sede di ispezione (espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

CAPITOLO B.4

Principi procedurali specifici

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente Capitolo B.3, devono rispettarsi, oltre ai principi generali contenuti nella Parte Generale del Modello, gli specifici principi procedurali qui di seguito descritti.

a) Predisposizione delle comunicazioni relative alla situazione economica, patrimoniale e finanziaria della società

Nella predisposizione dei suddetti documenti devono essere rispettati i seguenti principi:

- determinare con chiarezza e completezza i dati e le notizie che ciascuna funzione deve fornire, i criteri contabili per l'elaborazione dei dati e la tempistica per la loro consegna alle funzioni responsabili;
- prevedere la trasmissione di dati ed informazioni alla funzione responsabile attraverso un sistema (anche informatico) che consenta la tracciatura dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema.
- prevedere indispensabili controlli di merito indipendenti sulle poste di bilancio maggiormente critiche, anche con l'ausilio di controlli periodici e di scostamenti dei dati contabili con quelli di budget, lasciando evidenza documentale dei controlli effettuati..
- monitorare i rischi di alterazione delle scritture contabili da parte dei soggetti che partecipano al processo di alimentazione della contabilità generale/gestionale.

Prima della presentazione ed approvazione del progetto di bilancio occorre seguire alcune regole minime finalizzate alla diffusione del documento, che possono così riepilogarsi:

- tempestiva messa a disposizione di tutti i componenti del Consiglio di Amministrazione della bozza del bilancio/situazione infrannuale, prima della riunione del Consiglio di Amministrazione per l'approvazione dello stesso; il tutto con una documentata certificazione dell'avvenuta consegna della bozza in questione;

- adeguata giustificazione, documentazione ed archiviazione di eventuali modifiche apportate alla bozza di bilancio/situazioni infrannuali da parte degli Amministratori.

b) Gestione dei rapporti con la società di revisione contabile in ordine all'attività di comunicazione da parte di quest'ultima a terzi relativa alla situazione economica, patrimoniale o finanziaria della Società

Nei rapporti tra CAA e la società di revisione contabile sono adottati i seguenti presidi:

- gli incarichi di consulenza, aventi ad oggetto attività diversa dalla revisione contabile, vengono conferiti alla società di revisione, previo parere del Collegio Sindacale;
- è vietato il conferimento a soggetti che siano parte della "rete" o del "*network*" a cui appartiene la società di revisione, di incarichi diversi dalla revisione contabile che appaiono incompatibili con quest'ultima, in quanto suscettibili di pregiudicare l'indipendenza della società di revisione incaricata.

c) Operazioni relative al capitale sociale.

Tutte le operazioni sul capitale sociale di CAA, nonché la costituzione di società, l'acquisto e la cessione di partecipazioni, le fusioni e le scissioni devono essere effettuate nel rispetto delle regole di *Corporate Governance* e di legge.

d) Predisposizione delle comunicazioni alle Autorità di Vigilanza e gestione dei rapporti con le stesse.

Con riferimento alle attività soggette alla vigilanza di pubbliche autorità, in base alle specifiche normative applicabili, al fine di prevenire la commissione dei reati di false comunicazioni alle autorità e di ostacolo alle funzioni di vigilanza, le attività soggette a vigilanza devono essere svolte in base alle procedure aziendali esistenti, contenenti la disciplina delle modalità e l'attribuzione di specifiche responsabilità in relazione:

- alle segnalazioni periodiche alle autorità previste da leggi e regolamenti;
- alla trasmissione a queste ultime dei documenti previsti in leggi e regolamenti (ad es., bilanci e verbali delle riunioni degli Organi Sociali);

- alla trasmissione di dati e documenti specificamente richiesti dalle autorità di vigilanza;
- al comportamento da tenere nel corso degli accertamenti ispettivi.

I principi posti a fondamento di tali procedure sono:

- attuazione di tutti gli interventi di natura organizzativa necessari ad estrarre i dati e le informazioni per la corretta compilazione delle segnalazioni ed il loro puntuale invio all'autorità di vigilanza e/o alla pubblica amministrazione, nonché per una corretta formalizzazione e conservazione delle stesse, secondo le modalità ed i tempi stabiliti dalla normativa applicabile;
- nel corso dell'attività ispettiva, deve essere prestata da parte delle funzioni e delle articolazioni organizzative ispezionate la massima collaborazione all'espletamento degli accertamenti. In particolare, devono essere messi a disposizione con tempestività e completezza i documenti che gli incaricati ritengano necessario acquisire, previo il consenso del responsabile incaricato di volta in volta di interloquire con l'autorità;
- alle ispezioni devono partecipare i soggetti a ciò espressamente delegati. L'OdV dovrà essere prontamente informato sull'inizio di ogni attività ispettiva, mediante apposita comunicazione interna, inviata a cura della direzione aziendale di volta in volta interessata. Di tutto il procedimento relativo all'ispezione devono essere redatti gli appositi verbali, che verranno conservati dall'OdV.

e) Altre regole finalizzate alla prevenzione dei reati societari in genere.

Oltre alle regole di *Corporate Governance* e delle procedure esistenti, si dispone l'attuazione dei seguenti presidi integrativi:

- attivazione di un programma di formazione-informazione periodica del personale che presta attività nelle aree amministrazione, contabilità, finanza e controllo sui reati societari;
- previsione di riunioni periodiche, almeno con cadenza annuale, tra Collegio Sindacale e OdV per verificare l'osservanza della disciplina in tema di normativa societaria e di *Corporate Governance*;
- trasmissione al Collegio Sindacale, con congruo anticipo, di tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'assemblea o

del Consiglio di Amministrazione o sui quali esso debba esprimere un parere ai sensi di legge;

- trasmissione all'OdV dell'Ordine del Giorno delle riunioni assembleari da parte della funzione "Corporate governante e legale", successivamente alle stesse, del relativo verbale;
- aggiornamento di regolamenti interni e procedure nel rispetto della normativa societaria.

CAPITOLO B.5

I controlli dell'OdV

B. 5.1 Il controllo in generale

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza ed il suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (si rinvia a quanto esplicitato nella Parte Generale del presente Modello), l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di reati societari diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello commessi nell'interesse o a vantaggio della Società.

Principi procedurali da osservare nelle aree a rischio al fine di attivare le eventuali verifiche, l'Organismo di Vigilanza dovrà avere evidenza e mantenere traccia:

(i) di quanto posto in essere nella Società al fine di fornire opportune indicazioni per la corretta redazione del bilancio;

(ii) dei verbali degli incontri nei quali si dibattono i temi del bilancio tra le funzioni coinvolte (Direzione amministrazione fiscale, collegio sindacale, Comitato per il controllo interno). Per quanto attiene agli scambi di informazioni da e verso la società di revisione l'Organismo di Vigilanza dovrà mantenere agli atti evidenza;

(iii) delle riunioni del collegio sindacale, alle quali l'Organismo di Vigilanza è regolarmente invitato a partecipare.

Per quanto concerne il conferimento dell'incarico, l'Organismo di Vigilanza dovrà mantenere agli atti evidenza degli incarichi conferiti.

L'Organismo di Vigilanza dovrà, inoltre, esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni.

Inoltre, i compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i reati societari sono i seguenti:

(i) proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati di cui alla presente Parte Speciale;

(ii) monitoraggio sul rispetto delle procedure interne per la prevenzione dei reati societari. L'Organismo di Vigilanza è tenuto alla conservazione delle evidenze dei controlli e delle verifiche eseguiti;

(iii) esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

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

PARTE SPECIALE – C –

Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita

Reati di finanziamento del terrorismo

Reati con finalità di terrorismo o eversione dell'ordine democratico

DEFINIZIONI

Si rinvia alle definizioni di cui alla Parte Generale, fatte salve le ulteriori definizioni contenute nella presente Parte Speciale.

- **Black List:** le liste nazionali e internazionali nominative e di Paesi a rischio di riciclaggio pubblicate sul sito internet di Banca d'Italia e le liste di Paesi non cooperativi pubblicate sul sito internet del FAFT – GAFI.
- **Cliente:** il soggetto che instaura rapporti continuativi o compie Operazioni con la Società, secondo la definizione di cui al Decreto Antiriciclaggio.
- **Decreto Antiriciclaggio:** il Decreto legislativo 21 novembre 2007, n. 231 di recepimento 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 le misure di attuazione e successive modificazioni.
- **Operazione/i:** la trasmissione o movimentazione di mezzi di pagamento.
- **Operazioni Sospette:** ogni Operazione rispetto alla quale vi sia il sospetto che siano in corso o che siano state compiute o tentate operazioni in violazione della normativa in materia di riciclaggio (ad esempio sulla base delle sue caratteristiche, entità, natura, capacità economiche del soggetto cui è riferita, etc.).
- **Rapporto Continuativo:** un rapporto di durata, rientrante nell'attività sociale, che dia luogo a più operazioni di versamento, prelievo o trasferimento di mezzi di pagamento e che non si esaurisca in una sola Operazione.
- **Reati di Riciclaggio:** i reati di cui all'art. 25 *octies* del Decreto, ovvero i reati di ricettazione (art. 648 c.p.), riciclaggio (art. 648 *bis* c.p.) e impiego di denaro, beni e utilità di provenienza illecita (art. 648 *ter* c.p.).
- **Unità di Informazione Finanziaria o UIF:** la struttura nazionale incaricata di ricevere dai soggetti obbligati, di richiedere ai medesimi, di analizzare e comunicare alle autorità competenti le informazioni che riguardano ipotesi di riciclaggio o di finanziamento al terrorismo.

CAPITOLO C.1

La presente Parte Speciale si riferisce ai Reati di Riciclaggio di cui all'art. 25 octies del D.Lgs. 231/2001 (introdotti dal Decreto Antiriciclaggio), nonché ai Reati con finalità di terrorismo e di eversione dell'ordine democratico di cui all'art. 25 *quater* (introdotti dalla legge 14 gennaio 2003, n. 7) tra cui anche il Reato di Finanziamento del Terrorismo previsto dall'art. 2 della Convenzione internazionale "*per la repressione del finanziamento del terrorismo*" sottoscritta a New York il 9 dicembre 1999.

Le suddette fattispecie di reato, sebbene tutelino beni giuridici diversi, vengono tutte trattate nella presente Parte Speciale poiché:

- sono risultate a rischio nell'ambito delle medesime Attività Sensibili (ad esempio, selezione dei Fornitori e del personale dipendente);
- la commissione delle stesse può essere impedita attraverso l'implementazione dei medesimi presidi (ad esempio, le attività di verifica della clientela previste dal Decreto Antiriciclaggio possono essere estese anche nell'ambito delle Attività Sensibili alla commissione di Reati con Finalità di Terrorismo).

C.1.1. Le fattispecie dei reati di Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (Art. 25-*octies*, D.Lgs. 231/2001)

La presente Parte Speciale si riferisce ai Reati di Riciclaggio introdotti nel *corpus* del D.Lgs. 231 del 2001, all'art. 25-*octies*, attraverso il Decreto Antiriciclaggio.

Per Reati di Riciclaggio, considerati tali anche se le attività che hanno generato i beni da riciclare si sono svolte nel territorio di un altro Stato comunitario o di un Paese extracomunitario, si intendono:

RICETTAZIONE (ART. 648 C.P.)

Tale ipotesi di reato si configura nel caso in cui un soggetto, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta danaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farli acquistare, ricevere od occultare.

Per "acquisto" si intende l'effetto di un'attività negoziale, a titolo gratuito ed oneroso, mediante la quale l'agente consegua il possesso del bene.

Per "ricezione" si intende ogni forma di conseguimento del possesso de bene proveniente dal delitto, anche se solo temporaneamente.

Per "occultamento" si intende il nascondimento del bene proveniente da delitto dopo averlo ricevuto.

Perché sussista il reato non è necessario che il denaro o i beni debbano provenire direttamente o immediatamente da un qualsiasi delitto, ma è sufficiente anche una provenienza mediata, a condizione che l'agente sia consapevole di tale provenienza. Ricorre pertanto il delitto in esame non solo in relazione al prodotto o al profitto del reato, ma anche al denaro o alle cose che costituiscono il prezzo del reato, cioè alle cose acquistate col denaro di provenienza delittuosa oppure al denaro conseguito dall'alienazione di cose della medesima provenienza (si pensi al caso in cui la Società, al fine di ottenere un prezzo vantaggioso, acquisti beni da un soggetto che, parallelamente alla fornitura di tali beni, notoriamente svolga attività illecite quali lo spaccio di stupefacenti o faccia parte di un'associazione di tipo mafioso e utilizzi i profitti derivanti da tali attività illecite per investirli nell'attività lecita).

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione da due a otto anni e la multa da Euro 516 ad Euro 10.329.

RICICLAGGIO (ART. 648 BIS C.P.)

Tale ipotesi di reato si configura nel caso in cui un soggetto sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

Per "sostituzione" si intende la condotta consistente nel rimpiazzare il denaro, i beni o le altre utilità di provenienza illecita con valori diversi.

Per "trasferimento" si intende la condotta consistente nel ripulire il denaro, i beni o le altre utilità mediante il compimento di atti negoziali.

Per la realizzazione di tale reato, dunque, è richiesto un *quid pluris* rispetto al reato di ricettazione, ovvero il compimento di atti o fatti diretti alla sostituzione del denaro.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione da quattro a dodici anni e la multa da Euro 1.032 ad Euro 15.493.

La pena è aumentata quando il fatto è commesso nell'esercizio dell'attività professionale.

IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ART. 648 TER C. P.)

Tale ipotesi di reato si configura nel caso di impiego in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto.

La punibilità per tale reato è prevista solo per coloro i quali non siano già compartecipi del reato principale ovvero non siano imputabili a titolo di ricettazione o riciclaggio.

Il termine "impiegare" è normalmente sinonimo di "utilizzo per qualsiasi scopo": tuttavia, considerato che il fine ultimo perseguito dal legislatore consiste nell'impedire il turbamento del sistema economico e dell'equilibrio concorrenziale attraverso l'utilizzo di capitali illeciti reperibili a costi inferiori rispetto a quelli leciti, si ritiene che per "impiegare" debba intendersi in realtà "investire". Pertanto, dovrebbe ritenersi rilevante un utilizzo a fini di profitto.

Premesso che presupposto comune di tutte e tre le fattispecie incriminatrici di cui agli artt. 648, 648 *bis* e 648 *ter* c.p. è quello costituito dalla provenienza da delitto del denaro o di quasiasi altra utilità di cui l'agente sia venuto a disporre, si precisa che tali fattispecie si distinguono sotto il profilo soggettivo, per il fatto che la prima di esse richiede, oltre alla consapevolezza della su indicata provenienza, necessaria anche per le altre, solo una generica finalità di profitto, mentre la seconda o la terza richiedono la specifica finalità di far perdere le tracce dell'origine illecita, con l'ulteriore peculiarità, quanto alla terza, che detta finalità deve essere perseguita mediante l'impiego delle risorse in attività economiche o finanziarie.

La pena prevista per il soggetto che realizzi la fattispecie criminosa è la reclusione da quattro a dodici anni e la multa da Euro 1.032 ad Euro 15.493.

La pena è aumentata quando il fatto è commesso nell'esercizio dell'attività professionale.

C.1.2. Delitti con finalità di terrorismo o eversione dell'ordine democratico

I reati con finalità di terrorismo e di eversione dell'ordine democratico sono stati introdotti nel D.Lgs. 231/2001 (art. 25 – quater) dalla legge 14 gennaio 2003, n. 7 recante "*Ratifica ed esecuzione della Convenzione internazionale per la repressione del finanziamento del terrorismo, fatta a New York il 9 dicembre 1999, e norme di adeguamento dell'ordinamento interno*".

I reati con finalità di terrorismo e di eversione dell'ordine democratico previsti dall'art. 25 - *quater* del D.Lgs. 231/2001 ricomprendono, quindi, fattispecie di reato previste in:

A) il codice penale;

B) leggi speciali;

C) Convenzione di New York del 9 dicembre 1999.

Si riportano qui di seguito le fattispecie di reato che sono risultate - anche solo astrattamente - realizzabili nell'ambito delle attività aziendali

A) Reati con finalità di terrorismo e di eversione dell'ordine democratico previsti nel Codice Penale

ASSOCIAZIONI SOVVERSIVE (ART. 270 C.P.)

Tale ipotesi di reato si configura nei confronti di chiunque nel territorio dello Stato promuova, costituisca, organizzi o diriga associazioni dirette a stabilire violentemente la dittatura di una classe sociale sulle altre, ovvero a sopprimere violentemente una classe sociale o, comunque, a sovvertire violentemente gli ordinamenti economici o sociali costituiti nello Stato ovvero, infine, aventi come scopo la soppressione violenta di ogni ordinamento politico e giuridico della società.

ASSOCIAZIONE CON FINALITÀ DI TERRORISMO ANCHE INTERNAZIONALE O DI EVERSIONE DELL'ORDINAMENTO DEMOCRATICO (ART. 270-BIS C.P.)

Tale ipotesi di reato si configura nei confronti di chiunque promuova, costituisca, organizzi, diriga o finanzi associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico.

Ai fini della legge penale, la finalità di terrorismo ricorre anche quando gli atti di violenza siano rivolti contro una Stato estero, un'istituzione o un organismo internazionale.

A titolo esaustivo si riportano qui di seguito anche le fattispecie di reati previsti dall'art. 25-*octies* del Decreto 231 e ritenute, a seguito dell'analisi dei rischi e suggerimenti, non applicabili alla Società.

ASSISTENZA AGLI ASSOCIATI (ART. 270-TER C.P.)

ARRUOLAMENTO CON FINALITÀ DI TERRORISMO ANCHE INTERNAZIONALE (ART. 270-QUATER C.P.)

ADDESTRAMENTO AD ATTIVITÀ CON FINALITÀ DI TERRORISMO ANCHE INTERNAZIONALE (ART. 270-QUINQUIES C.P.)

CONDOTTE CON FINALITÀ DI TERRORISMO (ART. 270-SEXIES C.P.)

ATTENTATO PER FINALITÀ TERRORISTICHE O DI EVERSIONE (ART. 280 C.P.)

SEQUESTRO DI PERSONA A SCOPO DI TERRORISMO O DI EVERSIONE (ART. 289-BIS C.P.)

ISTIGAZIONE A COMMETTERE UNO DEI DELITTI CONTRO LA PERSONALITÀ DELLO STATO (ART. 302 C.P.)

COSPIRAZIONE POLITICA MEDIANTE ACCORDO E COSPIRAZIONE POLITICA MEDIANTE ASSOCIAZIONE (ARTT. 304 E 305 C.P.)

BANDA ARMATA, FORMAZIONE E PARTECIPAZIONE; ASSISTENZA AI PARTECIPI DI COSPIRAZIONE O DI BANDA ARMATA (ARTT. 306 E 307 C.P.)

B) Delitti con finalità di terrorismo o eversione dell'ordine democratico previsti da leggi penali speciali

Accanto alle fattispecie espressamente disciplinate dal codice penale, vengono in considerazione i reati previsti in materia da apposite leggi speciali. I reati di terrorismo previsti dalle leggi speciali consistono in tutta quella parte della legislazione italiana volta a combattere il terrorismo.

Tra le disposizioni di cui sopra va ricordato l'art. 1, Legge 6 febbraio 1980, n. 15 che prevede, come circostanza aggravante applicabile a qualsiasi reato il fatto che il reato stesso sia stato "*commesso per finalità di terrorismo o di eversione dell'ordine democratico*". Ne consegue che qualsiasi delitto previsto dal codice penale o dalle leggi speciali, anche diverso da quelli espressamente diretti a punire il terrorismo può diventare, purché commesso con dette finalità, uno di quelli suscettibili di costituire, a norma dell'art. 25-*quater*, presupposto per l'affermazione della responsabilità dell'ente.

Altre disposizioni specificamente dirette alla prevenzione dei reati commessi con finalità di terrorismo, sono contenute nella Legge 10 maggio 1976, n. 342, in materia di repressione di delitti contro la sicurezza della navigazione aerea, e nella Legge 28 dicembre 1989, n. 422, in materia di repressione dei reati diretti contro la sicurezza della

navigazione marittima e dei reati diretti contro la sicurezza delle installazioni fisse sulla piattaforma intercontinentale.

C) Delitto di finanziamento del terrorismo previsto dall'art. 2 della Convenzione di New York del 9 Dicembre 1999

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

Ai sensi del citato articolo, commette un reato chiunque con qualsiasi mezzo, direttamente o indirettamente, illegalmente e intenzionalmente, fornisca o raccolga fondi con l'intento di utilizzarli o sapendo che sono destinati ad essere utilizzati, integralmente o parzialmente, al fine di compiere qualsiasi altro atto diretto a causare la morte o gravi lesioni fisiche ad un civile, o a qualsiasi altra persona che non abbia parte attiva in situazioni di conflitto armato, quando la finalità di tale atto sia quella di intimidire una popolazione, o di obbligare un governo o un'organizzazione internazionale a compiere o ad astenersi dal compiere qualcosa.

Perché un atto possa comportare una delle suddette fattispecie non è necessario che i fondi siano effettivamente utilizzati per compiere quanto sopra descritto.

Commette ugualmente reato chiunque tenti di commettere i reati sopra previsti.

Commette altresì un reato chiunque:

- prenda parte in qualità di complice al compimento di un reato di cui sopra;
- organizzi o diriga altre persone al fine di commettere un reato di cui sopra;
- contribuisca al compimento di uno o più reati di cui sopra con un gruppo di persone che agiscono con una finalità comune. Tale contributo deve essere intenzionale e:
    - deve essere compiuto al fine di facilitare l'attività o la finalità criminale del gruppo, laddove tale attività o finalità implichino la commissione del reato; o
    - deve essere fornito con la piena consapevolezza che l'intento del gruppo è di compiere un reato.

Al fine di poter affermare se sia o meno ravvisabile il rischio di commissione di tale tipologia di reati, occorre esaminare il profilo soggettivo richiesto dalla norma ai fini della configurabilità del reato.

Dal punto di vista dell'elemento soggettivo, i reati di terrorismo si configurano come reati dolosi. Quindi, perché si realizzi la fattispecie dolosa è necessario, dal punto di vista della rappresentazione psicologica dell'agente, che il medesimo abbia coscienza dell'evento antigiuridico e lo voglia realizzare attraverso una condotta a lui attribuibile. Pertanto, affinché si possano configurare le fattispecie di reato in esame, è necessario che l'agente abbia coscienza del carattere terroristico dell'attività e abbia l'intento di favorirla.

Peraltro, sarebbe altresì configurabile il perfezionamento della fattispecie criminosa, qualora il soggetto agisca a titolo di dolo eventuale. In tal caso, l'agente dovrebbe prevedere ed accettare il rischio del verificarsi dell'evento, pur non volendolo direttamente. La previsione del rischio del verificarsi dell'evento e la determinazione volontaria nell'adottare la condotta criminosa devono comunque desumersi da elementi univoci e obiettivi.

C.1.3. La normativa di prevenzione del Reato di Finanziamento del Terrorismo

Il D.Lgs. 22 giugno 2007, n.109 ha introdotto nel nostro ordinamento "*Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE*", emanata dal Parlamento Europeo e dal Consiglio in data 26 ottobre 2005.

La nuova normativa in tema di Finanziamento del Terrorismo prevede che siano adottate le medesime misure di prevenzione già vigenti contro i Reati di Riciclaggio ed introdotte con il Decreto Antiriciclaggio. Tale normativa prevede inoltre altre norme idonee per attuare il "*congelamento dei fondi*" e delle "*risorse economiche*" disposto dalle numerose risoluzioni del Consiglio di sicurezza delle Nazioni Unite che si sono succedute dal 1999 ad oggi, dal Regolamento CE n. 2580/2001 emanato dal Consiglio in data 27 dicembre 2001 e relativo a misure restrittive specifiche destinate a combattere il terrorismo, nonché dai Regolamenti comunitari emanati ai sensi degli artt. 60 e 301 del Trattato istitutivo della Comunità Europea per il contrasto dell'attività dei Paesi che minacciano la pace e la sicurezza internazionale.

Ai sensi del D.Lgs. 109/2007, per "*congelamento di fondi*" si intende il divieto di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione del portafoglio. Per "*congelamento di risorse economiche*" si intende, invece, il divieto di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, utilizzo delle risorse economiche, compresi, a titolo meramente esemplificativo, la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia

Il congelamento dei fondi e delle risorse economiche è disposto, con decreto, su proposta del Comitato di Sicurezza Finanziaria, dal Ministro dell'Economia e delle Finanze, di concerto con il Ministro degli affari esteri.

CAPITOLO C.2

Attività Sensibili nell'ambito dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, dei reati con finalità di terrorismo o eversione dell'ordine democratico e del reato di finanziamento del terrorismo

I delitti in oggetto, come del resto indicato anche dalla Linee Guida ANIA, sono senz'altro astrattamente ipotizzabili per il settore assicurativo, specialmente quello di riciclaggio e di finanziamento del terrorismo.

Al riguardo, sebbene le imprese di assicurazione esercenti il ramo danni nel quadro della legislazione antiriciclaggio non siano destinatarie di specifici obblighi di identificazione e segnalazione ex D.Lgs. 231/2007, la Società:

- nel rispetto di quanto previsto dall'art. 32 Regolamento ISVAP 26 marzo 2008, n. 20, verifica la presenza dei requisiti minimi dei fornitori;
- ha ritenuto di predisporre la seguente parte speciale a presidio di un'area comunque a rischio di commissione reati il cui elemento determinante è costituito dai rapporti con la clientela nell'ambito dei quali si può rinvenire a carico di coloro che agiscono per l'ente una finalità illecita o la consapevolezza di una altrui finalità illecita.

Di seguito sono elencate le attività già indicate nella Parte Generale del presente Modello che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001:

- identificazione, registrazione e conservazione dati per ciascun cliente;
- esecuzione di operazioni disposte dalla clientela anche attraverso la Rete Distributiva;
- selezione e gestione dei rapporti con i fornitori e i consulenti;
- ricerca e selezione del personale e degli intermediari assicurativi;
- attività di investimento in Paesi a rischio terrorismo.

CAPITOLO C.3

Regole e principi procedurali specifici

C.3.1 Principi generali di comportamento

Obiettivo della presente Parte Speciale è che tutti i Dipendenti, Organi Sociali, i dipendenti di CA Vita per i servizi prestati a CAA, ed i soggetti che operano a livello periferico si attengano – nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento di attività nelle Aree a Rischio individuate in precedenza - a regole di condotta conformi a quanto prescritto in tale Parte Speciale e nelle *policy* e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire la commissione dei Reati di Riciclaggio e Reati con Finalità di Terrorismo.

In particolare, i soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai Reati di Riciclaggio, dai Reati con Finalità di Terrorismo o Eversione dell'Ordine Democratico e dai Reati di Finanziamento del Terrorismo;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione anagrafica di fornitori/clienti/partner anche stranieri;
4. non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità quali, a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura;
5. non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti;
6. effettuare un costante monitoraggio dei flussi finanziari aziendali.

La Società, a sua volta, al fine di prevenire il rischio di commissione dei Reati di Riciclaggio, dei Reati con Finalità di Terrorismo e del Reato di Finanziamento del Terrorismo:

1. adotta un sistema di individuazione e gestione del rischio di Riciclaggio e Finanziamento del Terrorismo conforme a quanto previsto dalle disposizioni normative tempo per tempo vigenti;
2. adotta sistemi, anche informatici, di identificazione, registrazione e conservazione dei dati per ciascun cliente che consentano la corretta imputazione di ogni operazione;
3. adotta specifiche procedure per la selezione e la gestione dei rapporti con i consulenti e con i fornitori;
4. adotta presidi idonei a prevenire il rischio di finanziamento del terrorismo in fase di liquidazione dei sinistri con controlli periodici in fase di apertura della procedura di liquidazione del sinistro;
5. adotta specifiche procedure per l'assunzione e la gestione del personale;
6. adotta una politica finanziaria che preveda l'assoluto divieto di investire in "*Paesi a rischio di terrorismo*";
7. gestisce la liquidità in modo tale che non siano trasferite somme di denaro contante o libretti di deposito, bancari o postali, al portatore o altri titoli al portatore in euro o valuta estera, per importi pari o superiori a 1.000 euro;
8. effettua un costante e regolare monitoraggio dei flussi finanziari aziendali, garantendone la tracciabilità e fornendo evidenza giustificativa di ciascuno di essi
9. inserisce nel Codice etico specifiche previsioni riguardanti il corretto comportamento da parte di tutti i Dipendenti delle aree che si reputano maggiormente esposte;

Per l'attuazione di tali principi si rinvia alle procedure, particolarmente dettagliate di cui al successivo paragrafo.

C.3.2 Principi procedurali specifici

C.3.2.1. In relazione all' identificazione della clientela, la Società:

a. effettua controlli periodici sia nella fase di assunzione di nuove polizze sia in quella di liquidazione finalizzati a verificare che la clientela non sia presente all'interno delle Black List.

C.3.2. In relazione all'esecuzione di operazioni disposte dalla clientela anche attraverso la Rete Distributiva, la Società:

a. adotta specifiche procedure per la liquidazione delle polizze assicurative che prevedano attività di identificazione dell'assicurato o del beneficiario a favore del quale deve essere disposto il pagamento;

b. addotta presidi volti ad impedire che le operazioni di liquidazione delle polizze assicurative non vengano disposte a favore di soggetti elencati nelle Black List nazionali e internazionali o su conti correnti di persone fisiche e giuridiche che si trovino in Paesi *"a rischio terrorismo*" o per le quali sono state disposte misure restrittive da parte delle autorità europee e internazionali;

c. circolarizza tra i responsabili delle funzioni addette all'esecuzione delle operazioni disposte dalla clientela (ad esempio, la funzione Gestione Sinistri o l'Assunzione) di un'informativa chiara e semplificata,che stabilisca quali sono le operazione anomale, al fine di contrastare i fenomeni delittuosi, nonché la tempistica con cui queste vengono segnalate (ad esempio: entro una determinata data). A tal fine si considerano anomale quelle operazioni che per caratteristiche, entità, natura o per qualsivoglia altra circostanza inducano a ritenere che il danaro, i beni e le utilità oggetto delle operazioni medesime possano provenire dalla commissione di reati in genere;

d. per i contratti di assicurazione contro i danni, vieta di ricevere denaro contante a titolo di pagamento di premi di importo superiore ad Euro 750 annui (Euro settecentocinquanta) per ciascun contratto. Per le coperture del ramo responsabilità civile auto e per le relative garanzie accessorie, se ed in quanto riferite allo stesso veicolo assicurato per la responsabilità civile auto, il divieto è per un importo superiore ad Euro 1.000 annui (Euro mille).

In presenza di un'operazione anomala, l'unità operativa interessata deve farne tempestiva segnalazione al Consiglio di Amministrazione e all'Organismo di Vigilanza.

C.3.2.2. In relazione alla selezione e gestione dei rapporti con i fornitori e i consulenti, la Società:

a. verifica l'attendibilità commerciale e professionale dei fornitori e dei Consulenti;

b. adotta procedure o policy aziendali volte a garantire che il processo di selezione dei Fornitori e del Consulenti avvenga nel rispetto dei criteri di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità, fermo restando la prevalenza dei requisiti di legalità rispetto a tutti gli altri. A tal fine le procedure prevedono:

   - la predisposizione di specifiche liste di consulenti, fornitori e altre controparti contrattuali con i quali siano già intercorsi rapporti contrattuali;
   - che, qualora si intenda intrattenere rapporti contrattuali con soggetti non inseriti nella lista sopra menzionata e salvo che si tratti di soggetti sottoposti a vigilanza pubblica, sia richiesta l'esibizione del certificato antimafia e del certificato penale relativo alla pendenza di procedimenti per l'accertamento di responsabilità amministrativa ex D.Lgs. 231/2001 o con particolare riferimento ai professionisti, la richiesta di documentazione comprovante l'iscrizione all'ordine professionale, all'albo e all'elenco appositamente formato e tenuto dalle autorità pubbliche;
   - che siano richieste informazioni sulle esperienze pregresse nello stesso ambito di attività o settore merceologico;
   - in relazione a ciascun acquisto o servizio, la comparazione di almeno tre offerte, da parte di tre Fornitori o Consulenti differenti, dalla quale emergano chiaramente i criteri adottati nella scelta del Fornitore o del Consulente;
   - i termini e le condizioni alle quali è possibile derogare alla procedura in oggetto;

c. nel caso di instaurazione di rapporti continuativi con Fornitori e Consulenti, si impegna ad attuare controlli periodici circa la persistenza in capo a questi ultimi dei requisiti che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto;

d. nei rapporti contrattuali con Fornitori e Consulenti, prevede apposite clausole che consentano di risolvere immediatamente il rapporto nel caso di condanna anche non definitiva per reati di riciclaggio, Finanziamento del Terrorismo o altri Reati con Finalità di Terrorismo.

e. effettua controlli sia formali che sostanziali dei flussi finanziari aziendali in entrata ed uscita; tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo ecc.), degli Istituti di credito utilizzati (sede delle banche coinvolte nelle operazioni) e di eventuali schermi societari e strutture fiduciarie utilizzate per eventuali operazioni straordinarie;

f. per altre tipologie di incassi, diniego di accettazione di denaro e titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) per importi complessivamente superiori a Euro 1.000, se non tramite intermediari a ciò abilitati, quali banche, istituti di moneta elettronica e Poste Italiane S.p.A. da parte di Clienti;

g. previsione di modalità formalizzate per la modifica delle coordinate bancarie di pagamento del fornitore rispetto a quelle inizialmente concordate in sede contrattuale ovvero rispetto a quelle dallo stesso utilizzate in precedenti rapporti contrattuali.

C.3.2.3. In relazione alla ricerca e selezione del personale e degli intermediari assicurativi, la Società:

a. adotta specifiche procedure di selezione e assunzione del personale dipendente di qualsiasi livello e di collaboratori a progetto che garantiscano un criterio di trasparenza sulla base dei seguenti parametri:

- professionalità adeguata rispetto all'incarico o alle mansioni da assegnare;
- uguaglianza di trattamento tra i diversi candidati;
- affidabilità rispetto al rischio di infiltrazione criminale: a tal riguardo, la Società assicura che vengano prodotti da ciascun Dipendente prima dell'assunzione i seguenti documenti:
  - casellario giudiziario, o
  - certificato dei carichi pendenti, non anteriore a tre mesi;
  - in alternativa ai suddetti certificati penali può essere richiesto il rilascio dell'autocertificazione con la quale il candidato selezionato dichiara di non aver subito condanna e di non avere procedimenti penali in corso per reati di Riciclaggio, Finanziamento del Terrorismo o altro Reato con Finalità di Terrorismo o eversione dell'Ordine Democratico.

b. conserva la documentazione esibita in sede di assunzione da parte del dipendente anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo.

C.3.2.4. In relazione all'attività di investimento in Paesi a rischio terrorismo, la Società:

a. adotta una politica finanziaria che preveda il divieto a carico della Compagnia, e degli eventuali terzi cui la stessa ha conferito incarico o mandato:

   - di effettuare acquisti di strumenti o prodotti finanziari, partecipativi o non partecipativi, quotati o non quotati, titoli, investimenti in genere che abbiano a oggetto – diretto o indiretto – società o enti inseriti nelle Black List per il riciclaggio e per il finanziamento al terrorismo emanate e aggiornate dalle autorità italiane competenti;

   - di avvalersi di servizi finanziari effettuati da società, enti o persone fisiche inseriti nelle Black List sopra richiamate.

CAPITOLO C.4

I controlli dell'OdV

L'OdV effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei Destinatari , nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo.

In particolare, è compito dell'Organismo di Vigilanza:

a) monitorare l'efficacia delle procedure interne per la prevenzione dei Reati di Riciclaggio Finanziamento del Terrorismo e Reati con Finalità di Terrorismo;

b) proporre eventuali modifiche nelle Attività a Rischio in ragione di eventuali mutamenti nell' operatività della Società;

b) esaminare eventuali segnalazioni specifiche provenienti dagli organi di controllo, da terzi o da qualsiasi esponente della Società ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute;

c) effettuare tutte le segnalazioni di cui all'art. 52 del Decreto Antiriciclaggio.

L'Organismo di Vigilanza svolge altresì un ruolo attivo e propositivo nella formulazione di adeguati programmi e procedure di accertamento per verificare l'osservanza dell'intera normativa antiriciclaggio e antiterrorismo e, in particolare, degli obblighi di segnalazione di Operazioni Sospette.

PARTE SPECIALE – D –

Delitti contro la personalità individuale

Capitolo D.1

Le fattispecie dei delitti contro la personalità individuale (art. 25-*quinquies*, D.Lgs. 231/2001).

La presente Parte Speciale si riferisce ai reati contro la personalità individuale introdotti ai sensi dell'art. 5, Legge 11 agosto 2003, n. 228, in tema di misure contro la tratta delle persone che ha aggiunto nel *corpus* del Decreto l'art. 25-*quinquies* (di seguito "Reati contro la personalità individuale").

La Legge 9 gennaio 2006, n. 7 in materia di "Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedo-pornografia anche a mezzo internet" ha, altresì, introdotto l'art. 25-*quater*, il quale modifica l'ambito di applicazione dei delitti di pornografia minorile e detenzione di materiale pornografico (artt. 600-*ter* e 600-*quater* c.p.), includendo anche le ipotesi in cui tali illeciti siano commessi mediante l'utilizzo di materiale pornografico raffigurante immagini virtuali di minori degli anni diciotto o parti di esse (c.d. "pedo-pornografia virtuale" ai sensi del rinvio del nuovo art. 600-*quater1*, c.p.). Inoltre, si dispone anche la punibilità dell'ente nel caso di commissione del reato di cui all'art. 583-*bis* c.p. ("Pratiche di mutilazione degli organi genitali femminili") anch'esso introdotto nel codice penale dalla citata Legge 9 gennaio 2006, n. 7.

Si provvede qui di seguito a fornire una breve descrizione dei reati contemplati nella presente Parte Speciale "D", così come indicati all'art. 25-*quinquies* del Decreto e ritenuti applicabili alla Società.

RIDUZIONE O MANTENIMENTO IN SCHIAVITÙ O IN SERVITÙ (ART. 600 C.P.)

Chiunque esercita su una persona poteri corrispondenti a quelli del diritto di proprietà ovvero chiunque riduce o mantiene una persona in uno stato di soggezione continuativa, costringendola a prestazioni lavorative o sessuali ovvero all'accattonaggio o comunque a prestazioni che ne comportino lo sfruttamento, è punito con la reclusione da otto a venti anni.

La riduzione o il mantenimento nello stato di soggezione ha luogo quando la condotta è attuata mediante violenza, minaccia, inganno, abuso di autorità o approfittamento di una situazione di inferiorità fisica o psichica o di una situazione di necessità, o mediante la promessa o la dazione di somme di denaro o di altri vantaggi a chi ha autorità sulla persona.

La pena è aumentata da un terzo alla metà se i fatti di cui al primo comma sono commessi in danno di minore degli anni diciotto o sono diretti allo sfruttamento della prostituzione o al fine di sottoporre la persona offesa al prelievo di organi.

INIZIATIVE TURISTICHE VOLTE ALLO SFRUTTAMENTO DELLA PROSTITUZIONE MINORILE (ART. 600-QUINQUIES C. P.)

Chiunque organizza o propaganda viaggi finalizzati alla fruizione di attività di prostituzione a danno di minori o comunque comprendenti tale attività è punito con la reclusione da sei a dodici anni e con la multa da lire trenta milioni a lire trecento milioni.

***

Per quanto attiene ai reati connessi alla schiavitù, tali ipotesi di reato si estendono non solo al soggetto che direttamente realizza la fattispecie illecita, ma anche a chi consapevolmente agevola anche solo finanziariamente la medesima condotta.

La condotta rilevante in questi casi può essere costituita dal procacciamento illegale della forza lavoro attraverso il traffico di migranti e la tratta degli schiavi.

Un esempio potrebbe essere rappresentato dal procacciamento di servizi (ad es. attività di pulizia della sede della società) tramite una ditta appaltatrice che si serva di persone ridotte quasi in schiavitù e che, per tale ragione, prestano la propria attività a prezzo sensibilmente inferiore rispetto alla concorrenza.

***

A titolo esaustivo si riportano qui di seguito le altre fattispecie di reati previsti dall'art. 25-*quinquies* del Decreto 231 e ritenute, a seguito dell'analisi dei rischi e suggerimenti, non applicabili alla Società.

PROSTITUZIONE MINORILE (ART. 600-BIS C.P.)

MINORILE (ART. 600-TER C.P.)

DETENZIONE DI MATERIALE PORNOGRAFICO (ART. 600-QUATER C.P.)

TRATTA DI PERSONE (ART. 601 C.P.)

ACQUISTO E ALIENAZIONE DI SCHIAVI (ART. 602 C.P.)

PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI (ART. 583-BIS C.P.)

Capitolo D.2

Attività Sensibili nell'ambito dei reati societari

I delitti in oggetto non sono né facilmente né tutti ipotizzabili per il settore assicurativo, ma la Società ha preferito comunque tenerne conto e considerare i relativi rischi sia per l'attività aziendale sia per la prestazione assicurativa. Pertanto, pur escludendo coinvolgimenti tali da far pensare ad una impresa di assicurazione diretta a perseguire, in tutto o in parte, finalità identificabili o connesse con il compimento di attività criminose configuranti i reati predetti, sono state contemplate solo le fattispecie di concorso o di fiancheggiamento nei reati stessi.

Di seguito sono elencate le attività già esposte nella Parte Generale del presente Modello che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001:

- organizzazione di iniziative turistiche per viaggi all'estero al fine di motivare/gratificare i Dipendenti e la Rete Distributiva;
- contratti di consulenza finanziaria prestata a favore di Clienti o affidamento di contratti di fornitura di servizi e appalto a soggetti che - direttamente o indirettamente – gestiscano attività illecite come il traffico di minori o impongano condizioni lavorative ai propri dipendenti tali da configurare vere e proprie forme di schiavitù.

Capitolo D.3

Regole e principi procedurali specifici

D.3.1 Principi di comportamento

Obiettivo della presente Parte Speciale è che i Dipendenti, gli Organi Sociali, i soggetti che operano a livello periferico (agenti, sub-agenti, personale d'agenzia, promotori, *broker*) ed i Partner della Società, come meglio individuati nella Parte Generale del Modello, si attengano a regole di condotta conformi a quanto infra prescritto nonché alle *policy* e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire ed impedire il verificarsi di condotte rilevanti o un coinvolgimento nella commissione dei Reati contro la personalità individuale.

A tal proposito, la Società:

(i) provvede a richiedere le necessarie informazioni ai fornitori al fine di valutare la trasparenza degli stessi nell'ambito del rispetto dei diritti del lavoratore e della normativa in materia di salute e sicurezza;

(ii) valuta e disciplina con particolare dovizia sia l'organizzazione di viaggi o di soggiorni in località estere con specifico riguardo a località note per il fenomeno del c.d. "turismo sessuale" sia la stipula di contratti di locazione degli immobili aziendali (i.e. procedendo ad una accurata valutazione della controparte al fine di escludere che negli immobili locati vengano realizzate le condotte illecite di cui al Capitolo D.1).

D.3.2 Divieti

Ai Destinatari individuati al paragrafo precedente è vietato:

a) porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-*quinquies* del Decreto);

b) porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo o favorirne la commissione.

D.3.3 Obblighi

I Destinatari, come meglio individuati al Paragrafo D.3.1, sono obbligati:

a) nei rapporti con i fornitori, a rispettare tutti i principi procedurali indicati dalle *policy* aziendali con riguardo all'instaurazione dei suddetti rapporti;

b) ad instaurare e mantenere rapporti con i fornitori improntati alla massima correttezza e trasparenza richiedendo, in sede contrattuale, garanzie sul rispetto da parte di questi ultimi della normativa di settore in materia giurislavoristica, di salute e sicurezza sul luogo di lavoro nonché dei principi etici a tutela della persona;

c) utilizzare in modo adeguato gli strumenti informatici in proprio possesso non accedendo a siti Internet contenenti materiale pedo-pornografico.

D.3.4 Policy e Procedure Specifici

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui alla presente Parte Speciale, i Destinatari, come meglio individuati al paragrafo D.3.1, sono tenuti, in generale, a conoscere e rispettare tutte le regole e i principi contenuti nei documenti, codici di comportamento, *policy* e procedure aziendali.

Tali *policy* e procedure e loro eventuali successive integrazioni o modiche si considerano parte integrante del Modello di Organizzazione e Controllo di CA Vita e, pertanto, si devono intendere come recepite nella loro attuale configurazione:

- Codice Etico;
- *Policy IT* che disciplina alcune delle tematiche dei reati considerati nella presente parte speciale.

Capitolo D.4

I controlli dell'OdV

D.4.1 Il controllo in generale

Fermo restando quanto previsto nella Parte Generale relativamente ai poteri e doveri dell'Organismo di Vigilanza e al suo potere discrezionale di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli sulle attività potenzialmente a rischio di commissione dei reati di cui alla presente Parte Speciale, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. Tali verifiche potranno riguardare, a titolo esemplificativo, l'idoneità delle procedure interne adottate, il rispetto delle stesse da parte di tutti i Destinatari e l'adeguatezza del sistema dei controlli interni nel suo complesso.

Inoltre, i compiti di vigilanza dell'Organismo di Vigilanza in relazione all'osservanza del Modello per quanto concerne i Reati contro la personalità individuale sono i seguenti:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei Reati di contro la personalità individuale di cui alla presente Parte Speciale;
- monitoraggio sul rispetto delle procedure per la prevenzione dei Reati contro la personalità individuale in costante coordinamento con le funzioni *Compliance* ed *Internal Audit*;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Sociali, da terzi o da qualsiasi esponente aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

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

PARTE SPECIALE – E –

Reati ed illeciti amministrativi di abuso di mercato

Capitolo E.1
Le fattispecie dei reati e di illeciti amministrativi di abuso di mercato (Art. 25-*sexies*, D.Lgs. 231/2001 e Art. 187-*quinquies* TUF)

Si descrivono di seguito le singole fattispecie di reato e di illecito amministrativo per le quali l'art. 25-*sexies*, D.Lgs. 231/2001 e l'art. 187-*quinquies* D.Lgs. n. 58/98 (di seguito, "TUF") prevedono la responsabilità della Società nei casi in cui tali reati ed illeciti amministrativi siano stati compiuti nell'interesse o a vantaggio della società stessa. I reati e gli illeciti amministrativi di cui alla presente Parte Speciale si riferiscono a strumenti finanziari ammessi alla negoziazione o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato italiano o di altro Paese dell'Unione Europea.

E.1.1 La definizione di "informazione privilegiata"

Attorno al concetto di informazione privilegiata ruota l'intera disciplina sull'*insider trading* e quella concernente l'informazione societaria disciplinata nel Titolo III, Capo I, artt. 114 e seguenti del TUF e nel Regolamento Emittenti n. 11971/1999.

Secondo quanto previsto dall'art. 181 TUF, si intendono di carattere privilegiato le informazioni che presentano le seguenti caratteristiche (qui di seguito le "Informazioni Privilegiate"):

a) sono di carattere preciso e pertanto:

   (i) devono essere inerenti a un complesso di circostanze o eventi esistenti o verificatisi o a circostanze o eventi che ragionevolmente possa prevedersi che verranno ad esistenza o che si verificheranno (il riferimento è ai casi in cui la notizia è in via di formazione e riguarda eventi non ancora verificatisi, si pensi al caso caratterizzato dalla notizia che una società quotata stia per lanciare un'OPA, oppure il caso riguardante un piano strategico di riposizionamento produttivo della società emittente i titoli) e

   (ii) devono essere sufficientemente specifiche (ossia esplicite e dettagliate), in modo che chi le impiega sia posto in condizione di ritenere che dall'uso delle stesse potranno effettivamente realizzarsi quegli effetti sul prezzo degli strumenti finanziari;

b) non sono ancora state rese pubbliche;

c) riguardano, direttamente o indirettamente, uno o più emittenti strumenti finanziari o uno o più strumenti finanziari, e sono relative alla situazione economica patrimoniale ("*corporate information*") ovvero a vicende organizzative dell'emittente ("*market information*");

d) sono *"price sensitive"*, ossia sono tali che, se rese pubbliche, sarebbero presumibilmente utilizzate da un investitore ragionevole come uno degli elementi su cui fondare le proprie decisioni di investimento.

E.1.2 I reati di abuso di mercato

ABUSO DI INFORMAZIONI PRIVILEGIATE (ART. 184 TUF)

La fattispecie punisce chiunque, essendo in possesso di informazioni privilegiate per essere membro di organi amministrativi, di direzione o di controllo di una società emittente, oppure per essere socio, ovvero per averle apprese nell'esercizio di un'attività lavorativa, di una professione o di una funzione privata o pubblica, o di un ufficio:

a) acquista, vende o compie altre operazioni, direttamente o indirettamente, per conto proprio o per conto di terzi, su strumenti finanziari utilizzando le informazioni privilegiate acquisite nelle modalità sopra descritte (c.d. "*insider trading*");

b) comunica tali informazioni ad altri, al di fuori del normale esercizio del lavoro, della professione, della funzione o dell'ufficio cui si è preposti (a prescindere dalla circostanza che i terzi destinatari utilizzino effettivamente l'informazione comunicata per compiere operazioni) (c.d. "*tipping*");

c) raccomanda o induce altri, sulla base delle informazioni privilegiate delle quali è in possesso, a compiere taluna delle operazioni indicate nella lettera a) (c.d. "*tuyautage*").

La fattispecie punisce, inoltre, i soggetti che, entrando in possesso di informazioni privilegiate a causa della preparazione o della realizzazione di attività delittuose, compiono taluna delle azioni di cui sopra (è l'ipotesi, ad esempio, del pirata informatico che a seguito dell'accesso abusivo al sistema informatizzato di una società riesce ad entrare in possesso di informazioni riservate *"price sensitive"*).

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da due a dodici anni e la multa da Euro 40.000 ad Euro 6.000.000.

MANIPOLAZIONE DI MERCATO (ART. 185 TUF)

La fattispecie punisce chiunque diffonde notizie false (c.d. manipolazione informativa) o pone in essere operazioni simulate o altri artifizi (c.d. manipolazione operativa) concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari.

Si ha manipolazione informativa anche allorquando la creazione di un'indicazione fuorviante derivi dall'inosservanza degli obblighi di comunicazione da parte dell'emittente o di altri soggetti obbligati.

La pena prevista per il soggetto che realizzi la suddetta fattispecie criminosa è la reclusione da due a dodici anni e la multa da Euro 40.000 ad Euro 10.000.000.

E.1.3 Gli illeciti amministrativi richiamati dall'art. 187-*quinquies* del TUF

ABUSO DI INFORMAZIONI PRIVILEGIATE (ART. 187 bis TUF)

La fattispecie di cui all'art. 187-*bis* TUF punisce con una sanzione amministrativa sia le condotte realizzabili dagli *insider* primari già punite come reato dall'art. 184 TUF ("chiunque essendo in possesso di informazioni privilegiate in ragione della sua qualità di membro di organi di amministrazione, direzione o controllo dell'emittente, della partecipazione al capitale dell'emittente, ovvero dell'esercizio di un'attività lavorativa, di una professione o di una funzione, anche pubblica, o di un ufficio"), sia quelle realizzate dagli *insider* secondari (o "*tippees*", cioè coloro che, direttamente o indirettamente, abbiano ottenuto dagli *insider* primari – "*tippers*" accesso all'informazione privilegiata), laddove la corrispondente fattispecie delittuosa attribuisce rilevanza esclusivamente alle condotte poste in essere dagli insider primari.

I comportamenti degli *insider* secondari sono puniti sia se sono commessi a titolo di dolo sia se sono commessi con colpa ("la sanzione prevista al comma 1" dell'art. 187-*bis* "si applica a chiunque, in possesso di informazioni privilegiate, conoscendo o potendo conoscere in base ad ordinaria diligenza il carattere privilegiato delle stesse, compie taluno dei fatti ivi descritti").

Si sottolinea, inoltre, che anche il semplice tentativo può rilevare ai fini dell'applicabilità della disciplina in oggetto.

La pena prevista per tale illecito amministrativo è la sanzione amministrativa pecuniaria da Euro 100.000 ad Euro 15.000.000.

MANIPOLAZIONE DI MERCATO (ART. 187-ter TUF)

La fattispecie di cui all'art. 187-*ter* TUF amplia le condotte rilevanti ai fini dell'applicabilità delle sanzioni amministrative rispetto a quelle penalmente sanzionate dalla corrispondente fattispecie delittuosa e punisce chiunque, tramite qualsiasi mezzo di informazione, compreso internet, diffonde informazioni, voci o notizie false o fuorvianti che forniscano o siano suscettibili di fornire indicazioni false ovvero fuorvianti in merito agli strumenti finanziari. A differenza di quanto previsto dalla corrispondente fattispecie di reato, pertanto, l'art. 187-*ter* TUF non richiede, ai fini della sanzionabilità delle condotte, che le notizie false, le operazioni simulate o gli altri artifizi siano "concretamente idonee" ad alterare i prezzi.

Il comma 3 del medesimo articolo 187-*ter* TUF prevede la sanzionabilità delle seguenti condotte:

a) operazioni od ordini di compravendita che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;

b) operazioni od ordini di compravendita che consentono, tramite l'azione di una o più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più strumenti finanziari ad un livello anomalo o artificiale;

c) operazioni od ordini di compravendita che utilizzano artifizi od ogni altro tipo di inganno o di espediente;

d) altri artifizi idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

La pena prevista per tale illecito amministrativo è la sanzione amministrativa pecuniaria da Euro 100.000 ad Euro 25.000.000.

Capitolo E.2

Attività Sensibili nell'ambito dei reati di abuso di mercato

È opportuno ricordare che le imprese di assicurazione non rientrano nella categoria degli intermediari finanziari (c.d. soggetti abilitati) come individuati dall'art. 1 TUF e vengono parificate a questi esclusivamente in casi specifici, che prevedono per alcuni operatori economici l'adempimento di vari oneri per il contrasto, a livello finanziario, di determinate fattispecie criminose, quali il riciclaggio di denaro e il terrorismo internazionale.

Tuttavia, sebbene debba esser sempre verificata l'esistenza dell'interesse o vantaggio dell'ente, i Reati in questione sono ipotizzabili, almeno astrattamente, per il settore assicurativo, in quanto l'impresa di assicurazione riveste il ruolo di investitore istituzionale o, comunque, di investitore molto attivo, nonché elabora e diffonde studi, ricerche o raccomandazioni di tipo economico-finanziario.

Inoltre, anche in riferimento al tipo di reati *de quibus* vanno anzitutto ricordati i vincoli e gli oneri che, in base alla disciplina di vigilanza, gravano sulle imprese di assicurazione per quanto concerne, tra l'altro, le informazioni contabili, le relazioni sull'andamento, le partecipazioni, la separazione di patrimoni o di classi di attivi, nonché per il rispetto del segreto professionale da parte dei dipendenti dell'impresa.

Il corretto e continuativo adempimento delle suddette disposizioni è senz'altro importante strumento di salvaguardia, ma non può considerarsi sufficiente ancorché se ne aumenti la specifica attenzione.

Di seguito sono elencate le attività già esposte nella Parte Generale del presente Modello che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001:

- comunicazioni all'esterno (ISVAP, banche d'investimento, azionisti, giornalisti, etc.);
- gestione dei rapporti con i giornalisti e con altri rappresentanti dei mezzi di comunicazione di massa;
- impartire ordini di acquisto e/o di vendita direttamente o alla società di *asset management*.

Capitolo E.3

Regole e principi procedurali specifici

E.3.1 Principi di comportamento

Obiettivo della presente Parte Speciale è che i Dipendenti e gli Organi Sociali – nei limiti delle rispettive competenze e nella misura in cui siano coinvolti nello svolgimento delle attività nelle Aree a Rischio individuate in precedenza – a regole di condotta conformi a quanto prescritto in tale Parte Speciale e nelle *policy* e procedure cui la stessa fa riferimento diretto o indiretto, al fine di prevenire la commissione dei Reati ed Illeciti Amministrativi di abuso di mercato.

In particolare, i soggetti sopra meglio individuati dovranno attenersi ai seguenti principi di condotta:

1. astenersi dal tenere comportamenti tali da integrare le fattispecie previste dai suddetti Reati ed Illeciti Amministrativi di abuso di mercato;
2. astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato o di illecito amministrativo rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
3. astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari quotati o per i quali è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato.

E.3.2 Regole comportamentali

Ai fini dell'attuazione delle regole elencate, devono altresì rispettarsi i seguenti principi riferibili alla Aree a Rischio di cui al precedente paragrafo E.3.1.

• Gestione delle Informazioni Privilegiate relative a tutte le società quotate in genere.

Con riferimento a tale Attività a Rischio si elencano qui di seguito, a mero titolo esemplificativo e non esaustivo, alcune circostanze in cui la Società potrebbe trovarsi a dover gestire Informazioni Privilegiate appartenenti ad altre società:

- distribuzione di prodotti assicurativi vita a prevalente contenuto finanziario;

- dati revisionali e obiettivi quantitativi concernenti l'andamento della gestione;

- comunicazioni relative a operazioni di fusione/scissione e a nuove iniziative di particolare rilievo ovvero a trattative e/o accordi in merito all'acquisizione e/o cessione di *asset* significativi;

- attività di finanza straordinaria, quali, a titolo esemplificativo, fusioni, scissioni, incorporazioni, scorpori;

- mutamento nel controllo o nei patti parasociali di controllo;

- cambiamenti nell'organo di amministrazione e controllo;

- modifica del revisore o qualsiasi informazione collegata alla sua attività;

- operazioni sul capitale o emissione di obbligazioni o warrant per acquistare/sottoscrivere azioni;

- aumento o diminuzione del capitale sociale;

- acquisto o cessione di partecipazioni o altri asset o attività rilevanti;

- ristrutturazione o riorganizzazione che abbiano un effetto sul bilancio;

- decisioni relative ai programmi di acquisto di azioni proprie o operazioni aventi ad oggetto altri strumenti finanziari quotati;

- modifiche dei diritti relativi a determinate categorie di azioni quotate;

- istanze di fallimento ovvero ordinanze del tribunale relative a procedure concorsuali;

- significative controversie legali;

- revoca o cancellazione di linee di credito;

- liquidazione volontaria o altre cause di liquidazione;

- rilevante cambiamento nel valore degli *asset*;

- insolvenza dei principali debitori;

- riduzione del valore delle proprietà immobiliari;

- introduzione di processi o prodotti innovativi;

- decremento o incremento nel valore degli strumenti finanziari in portafoglio;

- aggiudicazione di gare per l'acquisto di *asset* rilevanti;

- ordini rilevanti ricevuti da clienti, loro cancellazione o rilevanti modifiche;

- ritiro o ingresso in rilevanti settori di business;

- rilevanti modifiche nella politica degli investimenti;

- informazioni relative al pagamento dei dividendi;

- analisi relative a strumenti finanziari o emittenti in particolare se contenenti raccomandazioni di investimento;

- rapporti delle agenzie di *rating*, ricerche da parte di banche d'affari, raccomandazioni o suggerimenti concernenti gli strumenti finanziari;

- decisioni riguardanti le modifiche delle regole di *governance* degli indici di mercato, con particolare riguardo alla loro composizione;

- decisioni delle autorità della concorrenza e del mercato relative alle società quotate non ancora pubblicate.

Con riferimento a tale Attività a Rischio è espressamente vietato ai Destinatari, come meglio individuati al paragrafo precedente, di:

1) utilizzare o comunicare informazioni privilegiate relative a strumenti finanziari o emittenti strumenti finanziari, quotati, comunque ottenute, anche al di fuori della propria attività lavorativa;

2) partecipare a gruppi di discussione o *chat-room* su internet aventi ad oggetto strumenti finanziari o emittenti strumenti finanziari, quotati e nei quali vi sia uno scambio di informazioni concernenti strumenti finanziari quotati, o società quotate in genere o strumenti finanziari emessi da tali soggetti, a meno che si tratti di incontri istituzionali per i quali è già stata compiuta una verifica di legittimità da parte delle funzioni competenti e/o non vi sia scambio di informazioni il cui carattere non privilegiato sia evidente;

3) sollecitare l'ottenimento di informazioni privilegiate su strumenti finanziari o emittenti strumenti finanziari quotati;

4) comunicare qualsiasi informazione all'interno della Società, dei comitati, degli organi sociali di tipo collegiale senza il puntuale e metodico rispetto della normativa vigente in materia di informazioni privilegiate;

5) lasciare documentazione contenente informazioni privilegiate in luoghi in cui potrebbe facilmente essere letta da persone che non sono autorizzate a conoscere tali informazioni secondo quanto previsto dalla normativa vigente.

• Attività di comunicazione e diffusione all'esterno di informazioni price sensitive.

Con riferimento a tale Attività a Rischio è espressamente vietato ai Destinatari, come meglio individuati al paragrafo precedente, di:

1) effettuare comunicazioni all'esterno nel mancato rispetto delle procedure interne in materia e senza il preventivo coordinamento con le funzioni preposte a tale compito;

2) rivelare a terzi informazioni privilegiate relative a strumenti finanziari o emittenti strumenti finanziari, quotati o non quotati, se non nei casi in cui tale rivelazione sia richiesta da leggi, da altre disposizioni regolamentari o da specifici accordi contrattuali con cui le controparti si siano impegnate a utilizzare dette informazioni privilegiate esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenere la riservatezza sulle stesse;

3) comunicare o diffondere all'esterno analisi o valutazioni su uno strumento finanziario quotato (o indirettamente sul suo emittente) che possano influenzare i terzi, dopo aver preso precedentemente posizione su tale strumento finanziario, beneficiando di conseguenza dell'impatto della valutazione diffusa sul prezzo di detto strumento, senza avere allo stesso tempo comunicato al pubblico, in modo corretto ed efficace, l'esistenza di tale conflitto di interesse;

4) diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso internet, o tramite qualsiasi altro mezzo;

5) diffondere al pubblico valutazioni o una notizia su uno strumento finanziario od un emittente senza prima aver verificato l'attendibilità e il carattere non privilegiato dell'informazione;

6) consigliare ai terzi operazioni di investimento sulla base delle informazioni privilegiate in loro possesso;

7) discutere di informazioni privilegiate in presenza di estranei o, comunque, soggetti non autorizzati a conoscere tali informazioni sulla base della normativa vigente;

8) discutere di informazioni privilegiate al telefono in luoghi pubblici ovvero in ufficio con la modalità "viva voce", onde evitare che informazioni privilegiate possano essere ascoltate da estranei o comunque da soggetti non autorizzati a conoscere tali informazioni secondo quanto previsto dalla normativa vigente.

• Operazioni sui mercati regolamentati relative a titoli quotati nei medesimi mercati.

Con riferimento a tale Attività a Rischio è espressamente vietato ai Destinatari, come meglio individuati al paragrafo precedente, direttamente o indirettamente, di:

1) acquistare, o impartire ordini per l'acquisto di, uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere informazioni fuorvianti sullo strumento finanziario in modo da aumentarne il prezzo;

3) concludere operazioni o impartire ordini in modo tale da evitare che i prezzi di mercato degli strumenti finanziari di interesse per la Società scendano al di sotto di un certo livello, principalmente per sottrarsi alle conseguenze negative derivanti dal connesso peggioramento del rating degli strumenti finanziari stessi;

4) agire consultandosi con altri soggetti per acquisire una posizione dominante sull'offerta o sulla domanda di uno strumento finanziario che abbia l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita o determinare altre condizioni commerciali non corrette;

5) effettuare operazioni di compravendita di uno strumento finanziario nella consapevolezza di un conflitto di interessi (a meno che esso non venga esplicitato nelle forme previste dalla normativa), allorquando tale operazione non sarebbe stata ragionevolmente effettuata in caso di assenza di conflitto di interessi;

6) operare creando inusuali concentrazioni di operazioni in accordo con altri soggetti su un particolare strumento finanziario;

7) realizzare un'inusuale operatività sulle azioni di una società prima dell'annuncio di informazioni privilegiate relative alla società utilizzando le stesse informazioni privilegiate;

8) effettuare operazioni che hanno la finalità di aggirare gli accorgimenti previsti dai meccanismi di negoziazione (ad esempio, con riferimento ai limiti quantitativi, ai parametri relativi al differenziale tra le proposte di acquisto e di vendita, ecc.);

9) impartire ordini di compravendita o eseguire operazioni prima o dopo che la stessa società o soggetti ad essa collegati abbiano diffuso studi, ricerche o raccomandazioni di investimento errate o tendenziose o manifestamente influenzate da interessi rilevanti;

10) acquistare partecipazioni di un emittente appartenente al c.d. "mercato sottile" realizzando poi operazioni volte a farne aumentare i prezzi così da consentire di ottenere performance superiori al *benchmark* di riferimento;

11) aprire una posizione lunga su uno strumento finanziario ed effettuare ulteriori acquisti e/o diffondere fuorvianti informazioni positive sullo strumento finanziario in modo da aumentarne il prezzo;

12) prendere una posizione ribassata su uno strumento finanziario ed effettuare un'ulteriore attività di vendita e/o diffondere fuorvianti informazioni negative sullo strumento finanziario in modo da ridurne il prezzo;

13) aprire una posizione su un determinato strumento finanziario e chiuderla immediatamente dopo che la posizione stessa è stata resa nota al pubblico;

14) realizzare un'inusuale operatività sugli strumenti finanziari di una società emittente prima dell'annuncio di informazioni privilegiate relative alla società, a meno che tale operatività non sia basata solo su analisi di mercato, su informazioni non privilegiate ovvero su altre notizie pubblicamente disponibili;

15) realizzare operazioni che hanno la finalità di aumentare il prezzo di uno strumento finanziario nei giorni precedenti all'emissione di uno strumento finanziario derivato collegato o di uno strumento finanziario convertibile;

16) omettere di comunicare le operazioni sospette individuate secondo le specifiche procedure predisposte in materia dalla Società. Tale divieto è operativo anche con riferimento alla prestazione dei servizi di negoziazione in conto terzi e di ricezione e trasmissione di ordini.

Capitolo E.4

I controlli dell'OdV

E. 4.1 Il controllo in generale

L'OdV effettua dei periodici controlli diretti a verificare il corretto adempimento da parte dei destinatari, come meglio individuati al Paragrafo E.3.1, nei limiti dei rispettivi compiti e attribuzioni, delle regole e principi contenuti nella presente Parte Speciale e nelle procedure aziendali cui la stessa fa esplicito o implicito richiamo.

A tal riguardo, è compito dell'Organismo di Vigilanza:

- proporre che vengano costantemente aggiornate le procedure aziendali relative alla prevenzione dei reati e degli illeciti amministrativi di cui alla presente Parte Speciale;
- monitorare il rispetto delle procedure interne per la prevenzione dei reati ed illeciti amministrativi di abuso di informazioni privilegiate e di manipolazione di mercato;
- esaminare eventuali segnalazioni specifiche provenienti dagli Organi Societari, da terzi o da qualsiasi Esponente Aziendale ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

PARTE SPECIALE – F –

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

Definizioni

Si rinvia alle definizioni di cui alla Parte Generale, fatte salve le ulteriori definizioni contenute nella presente Parte Speciale.

- **BS–OHSAS 18001 o British Standard:** British Standard OHSAS 18001, edizione 2007.
- **Datore di Lavoro**: il soggetto titolare del rapporto di lavoro con il Lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il Lavoratore presta la propria attività, ha la responsabilità, in virtù di apposita delega, dell'organizzazione stessa o del singolo settore in quanto esercita i poteri decisionali e di spesa.
- **Decreto Sicurezza**: il decreto legislativo 9 aprile 2008, n. 81 "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro".
- **DUVRI o Documento Unico di Valutazione dei Rischi per le Interferenze**: il documento redatto dal Datore di Lavoro committente contenente una valutazione dei rischi che indichi le misure per eliminare o, ove ciò non risulti possibile, ridurre al minimo i rischi da interferenze.
- **DVR o Documento di Valutazione dei Rischi**: il documento redatto dal Datore di Lavoro contenente una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante l'attività lavorativa ed i criteri per la suddetta valutazione, l'indicazione delle misure di prevenzione e protezione attuate e dei dispositivi di protezione individuali adottati a seguito di tale valutazione, il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere, l'indicazione del nominativo del RSPP, del RLS e del Medico Competente che ha partecipato alla valutazione del rischio, nonché l'individuazione delle mansioni che eventualmente espongono i lavoratori a rischi specifici che richiedono una riconosciuta capacità professionale, specifica esperienza, adeguata formazione ed addestramento.

- **Lavoratori**: persone che, indipendentemente dalla tipologia contrattuale, svolgono un'attività lavorativa nell'ambito dell'organizzazione della Società.
- **Linee guida UNI-INAIL**: le linee guida elaborate dall'UNI e dall'INAIL per la costituzione volontaria da parte delle imprese di un sistema di gestione della salute e sicurezza sul lavoro del 28 settembre 2001.
- **Medico Competente**: il medico in possesso di uno dei titoli e dei requisiti formali e professionali indicati nel Decreto Sicurezza che collabora con il Datore di Lavoro ai fini della valutazione dei rischi e al fine di effettuare la Sorveglianza Sanitaria ed adempiere tutti gli altri compiti di cui al Decreto Sicurezza.
- **Reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro:** i reati di cui all'art. 25-*septies* del D.Lgs. 231/2001, ovvero l'omicidio colposo (art. 589 c.p) e le lesioni personali gravi o gravissime (art. 590 terzo comma c.p.) commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.
- **RLS o Rappresentante dei Lavoratori per la Sicurezza**: il soggetto eletto o designato per rappresentare i Lavoratori in relazione agli aspetti della salute e sicurezza durante il lavoro.
- **RSPP o Responsabile del Servizio di Prevenzione e Protezione**: il soggetto in possesso delle capacità e dei requisiti professionali indicati nel Decreto Sicurezza, designato dal Datore di Lavoro, a cui risponde, per coordinare il Servizio di Prevenzione e Protezione.
- **Sorveglianza Sanitaria**: l'insieme degli atti medici finalizzati alla tutela dello stato di salute e sicurezza dei Lavoratori in relazione all'ambiente di lavoro, ai fattori di rischio professionali, ed alle modalità di svolgimento dell'attività lavorativa.
- **SPP o Servizio di Prevenzione e Protezione**: l'insieme delle persone, sistemi e mezzi esterni o interni alla Società finalizzati all'attività di prevenzione e protezione dei rischi professionali per i Lavoratori.
- **SSL**: Salute e Sicurezza dei Lavoratori.

Capitolo F.1

Le fattispecie dei reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (Art. 25-*septies*, D.Lgs. 231/2001)

Si provvede qui di seguito a fornire una breve descrizione dei reati commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro indicati all'art. 25-*septies* del Decreto.

Tale articolo, originariamente introdotto dalla legge 3 agosto 2007, n. 123, e successivamente sostituito ai sensi dell'art. 300 del Decreto Sicurezza, prevede l'applicazione di sanzioni pecuniarie ed interdittive agli Enti i cui esponenti commettano i reati di cui agli artt. 589 (omicidio colposo) e 590 terzo comma (lesioni personali colpose gravi o gravissime) del codice penale, in violazione delle norme sulla tutela della salute e sicurezza sul lavoro. Le fattispecie delittuose inserite all'art. 25-*septies* riguardano unicamente le ipotesi in cui l'evento sia stato determinato non già da colpa di tipo generico (e dunque per imperizia, imprudenza o negligenza) bensì da "colpa specifica" che richiede che l'evento si verifichi a causa della inosservanza delle norme sulla salute e sicurezza sul lavoro.

OMICIDIO COLPOSO (ART. 589 C. P.)

Il reato si configura ogni qualvolta un soggetto cagioni per colpa la morte di altro soggetto.

LESIONI PERSONALI COLPOSE GRAVI O GRAVISSIME (ART. 590 COMMA 3 C. P.)

Il reato si configura ogni qualvolta un soggetto, in violazione delle norme per la prevenzione degli infortuni sul lavoro, cagioni per colpa ad altro soggetto lesioni gravi o gravissime.

Ai sensi del comma 1 dell'art. 583 c. p., la lesione è considerata grave nei seguenti casi:

"1) se dal fatto deriva 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 ai quaranta giorni;

2) se il fatto produce l'indebolimento permanente di un senso o di un organo".

Ai sensi del comma 2 dell'art. 583 c.p., la lesione è considerata invece gravissima se dal fatto deriva:

"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 della favella;

la deformazione, ovvero lo sfregio permanente del viso".

Al fine di garantire l'adozione di un valido presidio avverso la potenziale commissione dei Reati di cui all'art. 25-*septies* del Decreto, la Società ha deciso di dotarsi anche della presente Parte Speciale, in conformità a quanto disposto dall'art. 30 del Decreto Sicurezza.

Ai sensi del suddetto articolo "*in sede di prima applicazione i modelli di organizzazione aziendale definiti conformemente alle Linee Guida Uni-Inail per un sistema di gestione della salute e sicurezza sul lavoro del 28 settembre 2001, o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti".*

A tal proposito appare opportuno sottolineare come la Società abbia deciso di ispirarsi ai principio previsti nelle suddette Linee Guida Uni-Inail.

Si fa tuttavia presente come, nonostante quanto appena precisato, nella predisposizione di tale Parte Speciale si sia comunque tenuto conto dei principi cardine di entrambi i sistemi di gestione, al fine di garantire il rispetto da parte dei Destinatari di regole minime di comportamento tenute dalla Società nell'affrontare il tema della sicurezza.

Capitolo F.2

Attività Sensibili nell'ambito dei reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Partendo dall'assunto che tutte le aree e tutti gli ambienti fisici nei quali si svolge attività lavorativa per l'impresa in rapporto di dipendenza o di collaborazione, nonché le attività lavorative esterne svolte per conto dell'impresa, sono esposti al rischio infortunistico, si pone l'accento sulle attività di verifica degli adempimenti richiesti dalle normative in materia di salute e sicurezza nei luoghi di lavoro, nonché sulla predisposizione delle procedure informative relative alla gestione delle strutture (locali, arredi, macchinari ecc.) e sulla valutazione sanitaria degli ambienti di lavoro.

Di seguito sono elencate le attività già esposte nella Parte Generale del presente Modello che, per il loro contenuto intrinseco, sono considerate maggiormente esposte alla commissione dei Reati di cui al D.Lgs. 231/2001:

- attività svolte dal personale dipendente presso la sede della Società alla quale sono connessi i tipici rischi d'ufficio (ad es. postura, videoterminale);
- attività svolte da personale esterno presso la sede della Società, quali ad esempio i fornitori di servizi in base a contratti di appalto, d'opera o di somministrazione (art. 26 del Decreto Sicurezza).

Eventuali modifiche o integrazioni delle suddette Aree a Rischio sono rimesse alla competenza dell'Amministratore Delegato e sottoposte annualmente al Consiglio di Amministrazione che potrà procedere con la successiva attività di ratifica secondo quanto indicato nella Parte Generale del Modello.

Capitolo F.3

Regole e principi procedurali specifici

F.3.1 Principi di comportamento

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

La Società si pone come obiettivo quello di enunciare i principi cui si ispira ogni azione aziendale e a cui tutti devono attenersi in rapporto al proprio ruolo ed alle responsabilità assunte all'interno della Società, nell'ottica della salute e sicurezza di tutti i Lavoratori.

In particolare tali obiettivi consistono in:

- una chiara affermazione della responsabilità dell'intera organizzazione aziendale, dal Datore di Lavoro al singolo Lavoratore, nella gestione delle tematiche relative alla salute e sicurezza sul lavoro, ciascuno per le proprie attribuzioni e competenze;
- l'impegno a considerare tali tematiche come parte integrante della gestione aziendale;
- l'impegno al miglioramento continuo ed alla prevenzione;
- l'impegno a fornire le risorse umane e strumentali necessarie;
- l'impegno a garantire che i Destinatari, nei limiti delle rispettive attribuzioni, siano sensibilizzati a svolgere la propria attività nel rispetto delle norme sulla tutela della salute e sicurezza;
- l'impegno al coinvolgimento ed alla consultazione dei Lavoratori, anche attraverso il RLS;
- l'impegno ad un'analisi e ad una revisione periodica degli obiettivi al fine di renderli idonei a migliorare il sistema della salute e sicurezza dei lavoratori presente nella Società.

F.3.2 Il processo di pianificazione

La Società, con cadenza periodica:

- definisce gli obiettivi finalizzati al mantenimento e/o miglioramento delle misure di prevenzione e protezione così come l'adeguamento della struttura alla normativa applicabile;
- individua le figure/strutture coinvolte nel raggiungimento dei suddetti obbiettivi e l'attribuzione dei relativi compiti e responsabilità;
- definisce le risorse, anche economiche, necessarie;
- prevede le modalità di verifica dell'effettivo ed efficace raggiungimento degli obiettivi.

F.3.3 L'organizzazione del sistema

F.3.3.1 Compiti e responsabilità

Nella definizione dei compiti organizzativi ed operativi dei Lavoratori, devono essere esplicitati e resi noti anche quelli relativi alle attività di sicurezza di loro competenza, nonché le responsabilità connesse all'esercizio delle stesse ed i compiti di ispezione, verifica e sorveglianza in materia di SSL.

Si riportano qui di seguito gli adempimenti che, in attuazione dei principi sopra descritti e della normativa applicabile, sono posti a carico delle figure rilevanti.

Il Datore di Lavoro

Al Datore di Lavoro della Società sono attribuiti tutti gli obblighi in materia di salute e sicurezza sul lavoro, tra cui i seguenti compiti non delegabili:

1) valutare tutti i rischi per la sicurezza e per la salute dei lavoratori;

2) elaborare, all'esito di tale valutazione, un Documento di Valutazione dei Rischi (da custodirsi presso l'azienda) contenente tra l'altro:

- una relazione sulla valutazione di tutti i rischi per la sicurezza e la salute durante il lavoro, nella quale siano specificati i criteri adottati per la valutazione stessa;

- l'indicazione delle eventuali misure di prevenzione e di protezione attuate e degli eventuali dispositivi di protezione individuale adottati a seguito della suddetta valutazione dei rischi (artt. 74 – 79 Decreto Sicurezza);
- il programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza;
- l'individuazione delle procedure per l'attuazione delle misure da realizzare nonché dei ruoli dell'organizzazione aziendale che vi debbono provvedere;
- l'indicazione del nominativo del RSPP, del RLS e del Medico Competente che abbiano partecipato alla valutazione del rischio.

L'attività di valutazione e di redazione del documento deve essere compiuta in collaborazione con il RSPP e con il Medico Competente. La valutazione dei rischi è oggetto di consultazione preventiva con il Rappresentante dei Lavoratori per la Sicurezza;

3) designare il Responsabile del Servizio di Prevenzione.

Al Datore di Lavoro sono attribuiti numerosi altri compiti dallo stesso delegabili a soggetti qualificati. Tali compiti, sono previsti dall'art. 18 del Decreto Sicurezza e riguardano, tra l'altro: a) la nomina del Medico Competente per l'effettuazione della Sorveglianza Sanitaria; b) la designazione preventivamente dei Lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave ed immediato, di salvataggio, di primo soccorso e, comunque, di gestione delle emergenze; c) l'adempimento degli obblighi di informazione, formazione ed addestramento; d) la convocazione della riunione periodica di cui all'art. 35 Decreto Sicurezza; e) l'aggiornamento delle misure di prevenzione in relazione ai mutamenti organizzativi che hanno rilevanza ai fini della salute e sicurezza del lavoro, etc.

In relazione a tali compiti, ed a ogni altro compito affidato al Datore di Lavoro che possa essere da questi delegato ai sensi del Decreto Sicurezza, la suddetta delega è ammessa con i seguenti limiti e condizioni:

- che esso risulti da atto scritto recante data certa;
- che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;

- che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;
- che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate.

Al fine di garantire l'attuazione di un modello di sicurezza aziendale sinergico e compartecipativo, il Datore di Lavoro fornisce al Servizio di Prevenzione e Protezione ed al Medico Competente informazioni in merito a:

a) la natura dei rischi;

b) l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;

c) la descrizione dei luoghi di lavoro e degli eventuali processi produttivi;

d) i dati relativi agli infortuni e quelli relativi alle malattie professionali.

Il Servizio di Prevenzione e Protezione (SPP)

Nell'adempimento degli obblighi in materia di salute e sicurezza sul lavoro, il Datore di Lavoro si avvale, ricorrendo anche a soggetti esterni alla Società, del Servizio di Prevenzione e Protezione dei rischi professionali che provvede:

- all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- ad elaborare, per quanto di competenza, le misure preventive e protettive a seguito della valutazione dei rischi e i sistemi di controllo di tali misure;
- ad elaborare le linee guida, *alert* e indicazioni operative relative alle varie attività aziendali;
- a proporre attività di informazione e formazione dei Lavoratori;
- a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro nonché alla riunione periodica di cui all'art. 35 Decreto Sicurezza;
- a fornire ai Lavoratori ogni informazione in tema di tutela della salute e sicurezza sul lavoro che si renda necessaria.

Qualora nell'espletamento dei relativi compiti, il RSPP della Società verificasse la sussistenza di eventuali criticità nell'attuazione delle azioni di recupero prescritte dal Datore di Lavoro, il RSPP coinvolto dovrà darne immediata comunicazione all'OdV.

L'eventuale sostituzione del RSPP dovrà altresì essere comunicata all'OdV con l'espressa indicazione delle motivazioni a supporto di tale decisione.

Il RSPP deve avere le capacità e i requisiti professionali in materia di prevenzione e sicurezza che sono specificamente indicati dall'art. 32 del Decreto Sicurezza e che sono accertati dal Datore di Lavoro prima della nomina attraverso documentazione che ne comprovi il possesso :

Il RSPP è coinvolto regolarmente ed è invitato alle riunioni dell' OdV relativamente alle materie di sua competenza.

Il Medico Competente

Il Medico Competente provvede tra l'altro a:

- collaborare con il Datore di Lavoro e con il Servizio di Prevenzione e Protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della Sorveglianza Sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e dell'integrità psicofisica dei lavoratori e all'attività di formazione ed informazione nei loro confronti, per la parte di competenza considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro;
- programmare ed effettuare la Sorveglianza Sanitaria;
- istituire, aggiornare e custodire sotto la propria responsabilità una cartella sanitaria e di rischio per ogni Lavoratore sottoposto a Sorveglianza Sanitaria;
- fornire informazioni ai lavoratori sul significato degli accertamenti sanitari a cui sono sottoposti ed informandoli sui relativi risultati;
- comunicare per iscritto in occasione della riunione periodica di cui all'art. 35 Decreto Sicurezza i risultati anonimi collettivi della Sorveglianza Sanitaria effettuata, fornendo indicazioni sul significato di detti risultati ai fini dell'attuazione delle misure per la tutela della salute e della integrità psicofisica dei lavoratori;

- visitare gli ambienti di lavoro almeno una volta l'anno o a cadenza diversa in base alla valutazione di rischi.

Il Medico Competente deve essere in possesso di uno dei titoli *ex* art. 38, D.Lgs. 81/2008, che vengono accertati dal Datore di Lavoro prima di provvedere alla relativa nomina.

Il Rappresentante dei Lavoratori per la Sicurezza (RLS)

È il soggetto eletto o designato, in conformità a quanto previsto dagli accordi sindacali in materia, per rappresentare i lavoratori per gli aspetti di salute e sicurezza sui luoghi di lavoro.

Il RLS riceve, a cura del Datore di Lavoro o di un suo delegato, la prevista formazione specifica in materia di salute e sicurezza.

Il RLS:

- accede ai luoghi di lavoro;
- è consultato preventivamente e tempestivamente in merito alla valutazione dei rischi e all'individuazione, programmazione, realizzazione e verifica delle misure preventive;
- è consultato sulla designazione del RSPP e degli incaricati dell'attuazione delle misure di emergenza e di pronto soccorso e del Medico Competente;
- è consultato in merito all'organizzazione delle attività formative;
- promuove l'elaborazione, l'individuazione a l'attuazione di misure di prevenzione idonee a tutelare la salute e l'integrità psicofisica dei lavoratori;
- partecipa alla "riunione periodica di prevenzione e protezione dai rischi";
- riceve informazioni inerenti la valutazione dei rischi e le misure di prevenzione relative e, ove ne faccia richiesta e per l'espletamento della sua funzione, copia del Documento di Valutazione dei Rischi e del DUVRI.

Il RLS dispone del tempo necessario allo svolgimento dell'incarico, senza perdita di retribuzione, nonché dei mezzi necessari per l'esercizio delle funzioni e delle facoltà riconosciutegli; non può subire pregiudizio alcuno a causa dello svolgimento della propria attività e nei suoi confronti si applicano le stesse tutele previste dalla legge per le rappresentanze sindacali.

I Lavoratori

È cura di ciascun Lavoratore porre attenzione alla propria sicurezza e salute e a quella delle altre persone presenti sul luogo di lavoro su cui possono ricadere gli effetti delle sue azioni ed omissioni, in relazione alla formazione e alle istruzioni ricevute e alle dotazioni fornite.

I Lavoratori devono in particolare:

- osservare le disposizioni e le istruzioni impartite dal Datore di Lavoro o dal suo delegato ai fini della protezione collettiva ed individuale;
- utilizzare correttamente le apparecchiature da lavoro nonché gli eventuali dispositivi di sicurezza, ove presenti;
- segnalare immediatamente al Datore di Lavoro o ai soggetti incaricati le deficienze dei mezzi e dispositivi dei punti precedenti, nonché le altre eventuali condizioni di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle loro competenze e possibilità, per eliminare o ridurre tali deficienze o pericoli;
- non rimuovere né modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- partecipare ai programmi di formazione e di addestramento organizzati dal Datore di Lavoro;
- sottoporsi ai controlli sanitari previsti nei loro confronti;
- contribuire, insieme al Datore di Lavoro o al suo delegato all'adempimento di tutti gli obblighi imposti dall'autorità competente o comunque necessari per tutelare la sicurezza e la salute dei lavoratori durante il lavoro.

I lavoratori di aziende che svolgono per la Società attività in regime di appalto e subappalto devono esporre apposita tessera di riconoscimento.

F.3.3.2 Informazione e formazione

Informazione

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

a) le conseguenze derivanti dallo svolgimento della propria attività non conformemente alle regole adottate dalla Società in tema di SSL;

b) il ruolo e le responsabilità che ricadono su ciascuno di essi e l'importanza di agire in conformità con la politica aziendale e le procedure in materia di sicurezza e ogni altra prescrizione relativa al sistema di SSL adottato dalla Società, nonché ai principi indicati nella presente Parte Speciale.

Ciò premesso, la Società, in considerazione dei diversi ruoli, responsabilità e capacità e dei rischi cui è esposto ciascun Dipendente, è tenuta ai seguenti oneri informativi:

- la Società deve fornire adeguata informazione ai dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) circa i rischi specifici dell'impresa, per quanto limitati, sulle conseguenze di questi e sulle misure di prevenzione e protezione adottate;
- deve essere data evidenza dell'informativa erogata per la gestione del pronto soccorso, emergenza, evacuazione e prevenzione incendi e devono essere verbalizzati gli eventuali incontri;
- i dipendenti e nuovi assunti (compresi lavoratori interinali, stagisti e co.co.pro.) devono ricevere informazione sulla nomina del RSPP, sul Medico Competente e sugli addetti ai compiti specifici per il pronto soccorso, salvataggio, evacuazione e prevenzione incendi;
- deve essere formalmente documentata l'informazione e l'istruzione per l'uso delle attrezzature di lavoro messe a disposizione dei Lavoratori;
- il RSPP e/o il Medico Competente devono essere coinvolti nella definizione delle informazioni;

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

Formazione

- La Società deve fornire adeguata formazione a tutti i dipendenti in materia di sicurezza sul lavoro;
- il RSPP e/o il Medico Competente devono partecipare alla stesura del piano di formazione;

- la formazione erogata deve prevedere questionari di valutazione;
- la formazione deve essere adeguata ai rischi della mansione cui il Lavoratore è in concreto assegnato;
- gli addetti a specifici compiti in materia di prevenzione e protezione (addetti prevenzione incendi, addetti all'evacuazione, addetti al pronto soccorso) devono ricevere specifica formazione;
- la società deve effettuare periodiche esercitazioni di evacuazione di cui deve essere data evidenza (verbalizzazione dell'avvenuta esercitazione con riferimento a partecipanti, svolgimento e risultanze).

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

F.3.4.3 Comunicazione, flusso informativo e cooperazione

Al fine di dare maggior efficacia al sistema organizzativo adottato per la gestione della sicurezza e quindi alla prevenzione degli infortuni sul luogo di lavoro, la Società si organizza per garantire un adeguato livello di circolazione e condivisione delle informazioni tra tutti i Lavoratori.

A tal proposito la Società adotta un sistema di comunicazione interna che prevede due differenti tipologie di flussi informativi:

a) dal basso verso l'alto

Il flusso dal basso verso l'alto è garantito dalla Società ricevendo da parte dei Lavoratori segnalazioni, osservazioni, proposte ed esigenze di miglioria inerenti alla gestione della sicurezza in ambito aziendale; Tali segnalazioni vengo portate a conoscenza da parte dei Lavoratori ai propri superiori in linea gerarchica affinchè siano trasmesse al Datore di Lavoro o al suo Delegato

b) dall'alto verso il basso

Il flusso dall'alto verso il basso ha lo scopo di diffondere a tutti i Lavoratori la conoscenza del sistema adottato dalla Società per la gestione della sicurezza nel luogo di lavoro.

A tale scopo la Società garantisce ai Destinatari un'adeguata e costante informativa attraverso la predisposizione di comunicati da diffondere internamente e l'organizzazione di incontri periodici che abbiano ad oggetto:

- eventuali nuovi rischi in materia di salute e sicurezza dei Lavoratori;
- modifiche nella struttura organizzativa adottata dalla Società per la gestione della salute e sicurezza dei Lavoratori;
- contenuti delle procedure aziendali adottate per la gestione della sicurezza e salute dei Lavoratori;
- ogni altro aspetto inerente alla salute e alla sicurezza dei Lavoratori.

Documentazione

La Società dovrà provvedere alla conservazione, sia su supporto cartaceo che informatico, i seguenti documenti:

- la cartella sanitaria, la quale deve essere istituita e aggiornata dal Medico Competente e custodita dal Datore di Lavoro;
- il Documento di Valutazione dei Rischi che indica la metodologia con la quale si è proceduto alla valutazione dei rischi e contiene il programma delle misure di mantenimento e di miglioramento.

La Società è altresì chiamata a garantire che:

- il RSPP, il Medico Competente, gli incaricati dell'attuazione delle misure di emergenza e pronto soccorso, vengano nominati formalmente;
- venga data evidenza documentale delle avvenute visite dei luoghi di lavoro effettuate dal RSPP e dal Medico Competente;
- venga adottato e mantenuto aggiornato il registro delle pratiche delle malattie professionali riportante data, malattia, data emissione certificato medico e data inoltro della pratica;
- venga conservata la documentazione inerente a leggi, regolamenti, norme antinfortunistiche attinenti all'attività aziendale;

- vengano conservati, ove previsti, i manuali e le istruzioni per l'uso di macchine, attrezzature ed eventuali dispositivi di protezione individuale forniti dai costruttori;
- venga conservata ogni procedura adottata dalla Società per la gestione della salute e sicurezza sui luoghi di lavoro;
- tutta la documentazione relativa alle attività di Informazione e Formazione venga conservata a cura del RSPP e messa a disposizione dell' OdV.

F.3.4 L'attività di controllo

La Società deve assicurare un controllo periodico delle misure di prevenzione e protezione adottate sui luoghi di lavoro.

A tale scopo la Società:

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

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

La Società garantisce che gli eventuali interventi correttivi necessari, vengano predisposti nel più breve tempo possibile.

F.3.5 Gli interventi successivi alle attività di controllo

Al termine dell'attività di controllo di cui alla precedente paragrafo, la Società pianifica gli interventi necessari per eliminare le criticità rilevate, al fine di accertare che il sistema di salute e sicurezza sia adeguatamente attuato e siano raggiunti gli obiettivi prefissati.

Della suddetta attività di controllo e degli esiti della stessa deve essere data evidenza su base documentale.

Capitolo F.4

I contratti di appalto

La Società deve predisporre e mantenere aggiornato l'elenco delle aziende che operano all'interno dei propri siti con contratto d'appalto.

Le modalità di gestione e di coordinamento dei lavori in appalto devono essere formalizzate in contratti scritti nei quali siano presenti espressi riferimenti agli adempimenti di cui all'art. 26, D.Lgs. 81/2008. Al riguardo, il Datore di Lavoro deve:

- verificare l'idoneità tecnico-professionale delle imprese appaltatrici in relazione ai lavori da affidare in appalto attraverso i) acquisizione del certificato di iscrizione alla camera di commercio, industria e artigianato ii) acquisizione dell'autocertificazione dell'impresa appaltatrice o dei lavoratori autonomi del possesso dei requisiti di idoneità tecnico professionale ai sensi dell'art. 4, D.P.R. 28 dicembre 2000, n. 445;
- fornire informazioni dettagliate agli appaltatori circa gli eventuali rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e in merito alle misure di prevenzione e di emergenza adottate in relazione alla propria attività;
- cooperare all'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto dell'appalto;
- coordinare gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori;
- predisporre un unico Documento di Valutazione di Rischi che indichi le misure adottate al fine di eliminare, o quanto meno ridurre al minimo, i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva; tale documento deve allegarsi al contratto di appalto o d'opera. Tale adempimento non è necessario in caso di appalto di servizi di natura intellettuale, di mere forniture di materiali o attrezzature nonché di lavori o servizi la cui durata non sia superiore ai due giorni

Nei contratti di somministrazione, di appalto e di subappalto, devono essere specificamente indicati i costi relativi alla sicurezza del lavoro. A tali dati può accedere, su richiesta, il Rappresentante per la Sicurezza dei Lavoratori.

Nei contratti di appalto deve essere chiaramente definita la gestione degli adempimenti in materia di sicurezza sul lavoro nel caso di subappalto.

L'imprenditore committente risponde in solido con l'appaltatore, nonché con ciascuno degli eventuali ulteriori subappaltatori, per tutti i danni per i quali il lavoratore, dipendente dall'appaltatore o dal subappaltatore, non risulti indennizzato ad opera dell'Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro.

Capitolo F.5

I controlli dell'OdV

Fermo restando il potere discrezionale dell' OdV di attivarsi con specifiche verifiche a seguito delle segnalazioni ricevute (per le quali si rinvia a quanto esplicitato nella Parte Generale del presente Modello Organizzativo), l'OdV può:

(a) partecipare agli eventuali incontri organizzati dalla Società tra le funzioni preposte alla sicurezza valutando quali tra essi rivestano rilevanza per il corretto svolgimento dei propri compiti;

(b) accedere a tutta la documentazione aziendale disponibile in materia.

La Società istituisce altresì a favore dell'Organismo di Vigilanza flussi informativi idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio degli infortuni, delle criticità nonché notizie di eventuali malattie professionali accertate o presunte.

L'Organismo di Vigilanza, nell'espletamento delle attività di cui sopra, può avvalersi di tutte le risorse competenti in azienda (ad esempio: il Responsabile del Servizio di Prevenzione e Protezione; il Rappresentante dei Lavoratori per la Sicurezza; il Medico Competente; gli incaricati dell'attuazione delle misure di emergenza e primo soccorso nonché gli incaricati del Servizio Tecnico ed immobili).

L'Organismo di Vigilanza si incontra regolarmente ed almeno semestralmente con il RSPP per una disamina complessiva degli aspetti relativi alle tematiche sulla sicurezza sul lavoro.

PARTE SPECIALE – G –

Delitti informatici e trattamento illecito di dati e delitti in materia di violazione del diritto d'autore

Capitolo G.1

G.1.1. Le fattispecie dei delitti informatici e trattamento illecito di dati (art. 24-*bis* del Decreto 231) e dei delitti in materia di violazione del diritto d'autore (art. 25-*novies* del Decreto 231)

La presente Parte Speciale si riferisce ai delitti informatici e trattamento illecito di dati (art. 24-*bis,* di seguito, per brevità, i "Delitti Informatici"), nonché ai delitti in materia di violazione del diritto d'autore introdotti dalla Legge 99/2009 tra i Reati presupposto sanzionabili ai sensi del Decreto 231 (art. 25-*novies*).

Si descrivono qui di seguito le singole fattispecie di reato per le quali gli artt. 24-*bis* e 25 *novies* del D.Lgs. n. 231/2001 prevedono una responsabilità degli enti nei casi in cui tali reati siano stati compiuti nell'interesse o a vantaggio degli stessi. A tal riguardo si sottolinea che, nonostante le due tipologie di reati tutelino interessi giuridici differenti, si è ritenuto opportuno trattarli un'unica Parte Speciale in quanto:

- entrambe le fattispecie presuppongono un corretto utilizzo delle risorse informatiche;
- le Attività Sensibili risultano, in virtù di tale circostanza, in parte sovrapponibili;
- i principi procedurali mirano, in entrambi i casi, a garantire la sensibilizzazione dei Destinatari in merito alle molteplici conseguenze derivanti da un non corretto utilizzo delle risorse informatiche.

G.1.2. Delitti informatici e trattamento illecito di dati

FALSITÀ IN DOCUMENTI INFORMATICI (ART. 491-BIS C.P.)

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, co. 1, lett. p), D.Lgs. 82/2005, salvo modifiche ed integrazioni).

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di inserimento fraudolento di dati falsi nelle banche dati pubbliche oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli.

Inoltre, il delitto potrebbe essere integrato tramite la cancellazione o l'alterazione di informazioni a valenza probatoria presenti sui sistemi dell'ente, allo scopo di eliminare le prove di un altro reato.

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-TER C.P.)

Tale reato si realizza quando un soggetto "abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo". Tale delitto è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora il delitto in oggetto riguardi sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Il delitto di accesso abusivo al sistema informatico rientra tra i delitti contro la libertà individuale. Il bene che viene protetto dalla norma è il domicilio informatico seppur vi sia chi sostiene che il bene tutelato è, invece, l'integrità dei dati e dei programmi contenuti nel sistema informatico. L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema.

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Il delitto di accesso abusivo a sistema informatico si integra, ad esempio, nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file, ma limitandosi ad eseguire una copia (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

Il delitto potrebbe essere astrattamente commesso da parte di qualunque dipendente della Società accedendo abusivamente ai sistemi informatici di proprietà di terzi (*outsider hacking*), ad esempio, per prendere cognizione di dati riservati di un'impresa concorrente, ovvero tramite la manipolazione di dati presenti sui propri sistemi come risultato dei processi di business allo scopo di produrre un bilancio falso o, infine, mediante l'accesso abusivo a sistemi aziendali protetti da misure di sicurezza, da parte di utenti dei sistemi stessi, per attivare servizi non richiesti dalla clientela.

DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615-QUATER C.P.)

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

La pena è della reclusione da uno a due anni e della multa da 5.164 Euro a 10.329 Euro se il danno è commesso:

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

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

Il legislatore ha introdotto questo reato al fine di prevenire le ipotesi di accessi abusivi a sistemi informatici. Per mezzo dell'art. 615-*quater* c.p., pertanto, sono punite le condotte preliminari all'accesso abusivo poiché consistenti nel procurare a sé o ad altri la disponibilità di mezzi di accesso necessari per superare le barriere protettive di un sistema informatico.

I dispositivi che consentono l'accesso abusivo ad un sistema informatico sono costituiti, ad esempio, da codici, password o schede informatiche (ad esempio, badge, carte di credito, bancomat e smart card).

Questo delitto si integra sia nel caso in cui il soggetto che sia in possesso legittimamente dei dispositivi di cui sopra (operatore di sistema) li comunichi senza autorizzazione a terzi soggetti, sia nel caso in cui tale soggetto si procuri illecitamente uno di tali dispositivi. La condotta è abusiva nel caso in cui i codici di accesso siano ottenuti a seguito della violazione di una norma, ovvero di una clausola contrattuale, che vieti detta condotta (ad esempio, policy Internet).

L'art. 615-*quater*, inoltre, punisce chi rilascia istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente della Società autorizzato ad un certo livello di accesso al sistema informatico che ottenga illecitamente il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno della Società oppure carpisca in altro modo fraudolento o ingannevole il codice di accesso.

DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-QUINQIES C.P.)

Tale reato si realizza qualora qualcuno, "allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del

suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici". Tale reato è punito con la reclusione fino a due anni e con la multa sino a Euro 10.329.

Questo delitto è integrato, ad esempio, nel caso in cui il soggetto si procuri un virus, idoneo a danneggiare un sistema informatico o qualora si producano o si utilizzino delle smart card che consentono il danneggiamento di apparecchiature o di dispositivi elettronici.

Questi fatti sono punibili solo nel caso in cui un soggetto persegua lo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o, ancora, al fine di favorire l'interruzione parziale o totale o l'alterazione del funzionamento. Ciò si verifica, ad esempio, qualora un dipendente introduca un virus idoneo a danneggiare o ad interrompere il funzionamento del sistema informatico di un concorrente.

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUATER C.P.)

Tale ipotesi di reato si integra qualora un soggetto fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero impedisce o interrompe tali comunicazioni, nonché nel caso in cui un soggetto riveli, parzialmente o integralmente, il contenuto delle comunicazioni al pubblico mediante qualsiasi mezzo di informazione al pubblico. Tale reato è punito con la reclusione da sei mesi a quattro anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o sulle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

La norma tutela la libertà e la riservatezza delle comunicazioni informatiche o telematiche durante la fase di trasmissione al fine di garantire l'autenticità dei contenuti e la riservatezza degli stessi.

La fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Perché possa realizzarsi questo delitto è necessario che la comunicazione sia attuale, vale a dire in corso, nonché personale ossia diretta ad un numero di soggetti determinati o determinabili (siano essi persone fisiche o giuridiche). Nel caso in cui la comunicazione sia rivolta ad un numero indeterminato di soggetti la stessa sarà considerata come rivolta al pubblico.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione di dati, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, ovvero comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato si integra, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente.

INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUINQUIES C.P.)

Questa fattispecie di reato si realizza quando qualcuno, "fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi". Tale reato è punito con la reclusione da uno a quattro anni.

La condotta vietata dall'art. 617-*quinquies* è, pertanto, costituita dalla mera installazione delle apparecchiature, a prescindere dalla circostanza che le stesse siano o meno utilizzate. Si tratta di un reato che mira a prevenire quello precedente di intercettazione, impedimento o interruzione di comunicazioni informatiche o telematiche.

Anche la semplice installazione di apparecchiature idonee all'intercettazione viene punita dato che tale condotta rende probabile la commissione del reato di intercettazione. Ai fini della condanna il giudice dovrà, però, limitarsi ad accertare se l'apparecchiatura installata abbia, obbiettivamente, una potenzialità lesiva.

Qualora all'installazione faccia seguito anche l'utilizzo delle apparecchiature per l'intercettazione, interruzione, impedimento o rivelazione delle comunicazioni, si applicheranno nei confronti del soggetto agente, qualora ricorrano i presupposti, più fattispecie criminose.

Il reato si integra, ad esempio, a vantaggio dell'ente, nel caso in cui un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato (se privo delle necessarie autorizzazioni) si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635-BIS C.P.)

Tale fattispecie reato si realizza quando un soggetto "distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui". Tale reato è punito con la reclusione da sei mesi a tre anni.

La pena è della reclusione da uno a quattro anni se il fatto è commesso con violenza alla persona o con minaccia o se è commesso abusando della qualità di operatore del sistema.

Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

Il danneggiamento potrebbe essere commesso a vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento delle obbligazioni da parte del fornitore.

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.)

Tale reato si realizza quando un soggetto "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". Tale reato è punito con la reclusione da uno a quattro anni.

La sanzione è da tre a otto anni se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, ovvero la pena è aumentata se il fatto è commesso abusando della qualità di operatore del sistema.

La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Questo delitto si distingue dal precedente poiché, in questo caso, il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica.

Perché il reato si integri è sufficiente che si tenga una condotta finalizzata al deterioramento o alla soppressione del dato.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635-QUATER C.P.)

Questo reato di realizza quando un soggetto "mediante le condotte di cui all'art. 635-bis (danneggiamento di dati, informazioni e programmi informatici), 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". Tale reato è punito con la reclusione da uno a cinque anni.

La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Si tenga conto che qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635-*bis*.

Il reato si integra in caso di danneggiamento o cancellazione dei dati o dei programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio, attraverso l'inserimento nel sistema di un virus).

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (ART. 635-QUINQUIES C.P.)

Questo reato si configura quando "il fatto di cui all'art. 635-*quater* (Danneggiamento di sistemi informatici o telematici) è diretto a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento". Tale reato è punito con la pena della reclusione da uno a quattro anni.

La sanzione è della reclusione da tre a otto anni se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se lo stesso è reso, in tutto o in parte, inservibile nonché nelle ipotesi in cui il fatto sia stato commesso con abuso della qualità di operatore del sistema.

La pena è aumentata se il fatto è commesso con violenza alla persona o con minaccia ovvero abusando della qualità di operatore di sistema.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità, differentemente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (art. 635-*ter*), quel che rileva è che il sistema sia utilizzato per il perseguimento di pubblica utilità indipendentemente dalla proprietà privata o pubblica del sistema stesso.

Il reato si può configurare nel caso in cui un Dipendente cancelli file o dati, relativi ad un'area per cui sia stato abilitato ad operare, per conseguire vantaggi interni (ad esempio, far venire meno la prova del credito da parte di un ente o di un fornitore) ovvero che l'amministratore di sistema, abusando della sua qualità, ponga in essere i comportamenti illeciti in oggetto per le medesime finalità già descritte.

FRODE INFORMATICA DEL SOGGETTO CHE PRESTA SERVIZI DI CERTIFICAZIONE DI FIRMA ELETTRONICA (ART. 640-QUINQUIES C.P.)

Questo reato si configura quando "il soggetto che presta servizi di certificazione di firma elettronica , 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". Tale reato è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 Euro.

Questo reato può essere integrato da parte dei certificatori qualificati o meglio i soggetti che prestano servizi di certificazione di firma elettronica qualificata. La Società, tuttavia, non effettua attività di certificazione di firma elettronica.

G.1.3. Delitti in materia di violazione del diritto d'autore

La Legge 23 luglio 2009, n. 99, introducendo nell'ambito del Decreto 231 l'art 25-*novies* concernente i "*delitti in materia di violazione del diritto d'autore",* ha esteso la responsabilità amministrativa degli enti anche ai reati di cui alla Legge 22 aprile 1941, n. 633 relativa alla protezione del diritto d'autore e di altri diritti connessi al suo esercizio (di seguito "*Legge sul Diritto d'Autore*").

Si provvede a descrivere qui di seguito le fattispecie di reato punibili ai sensi dell'art. 25-*novies* del Decreto 231 e ritenute, a seguito dell'analisi dei rischi e suggerimenti, *prima facie* applicabili alla Società.

DIVULGAZIONE TRAMITE RETI TELEMATICHE DI UN'OPERA DELL'INGEGNO PROTETTA (art. 171 comma 1 lett. a-bis e comma 3. legge sul diritto d'autore)

In relazione alla fattispecie delittuosa di cui all'art. 171 della Legge sul Diritto d'Autore, il Decreto ha preso in considerazione esclusivamente due fattispecie, ovvero:

(i) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno protetta o di parte di essa;

(ii) la messa a disposizione del pubblico, attraverso l'immissione in un sistema di reti telematiche e con connessioni di qualsiasi genere, di un'opera dell'ingegno non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore o alla reputazione dell'autore.

Se dunque nella prima ipotesi ad essere tutelato è l'interesse patrimoniale dell'autore dell'opera, che potrebbe vedere lese le proprie aspettative di guadagno in caso di libera circolazione della propria opera in rete, nella seconda ipotesi il bene giuridico protetto

non è, evidentemente, l'aspettativa di guadagno del titolare dell'opera, ma il suo onore e la sua reputazione.

Tale reato potrebbe ad esempio essere commesso nell'interesse della Società qualora venissero caricati sulla rete aziendale dei contenuti coperti dal diritto d'autore affinché gli stessi potessero essere utilizzati nell'ambito dell'attività lavorativa.

DUPLICAZIONE, A FINI DI LUCRO, DI PROGRAMMI INFORMATICI O IMPORTAZIONE, DISTRIBUZIONE, VENDITA, DETENZIONE PER FINI COMMERCIALI DI PROGRAMMI CONTENUTI IN SUPPORTI NON CONTRASSEGNATI DALLA SIAE (art. 171-bis legge sul diritto d'autore.)

La norma in esame è volta a tutelare il corretto utilizzo dei *software* e delle banche dati.

Per ciò che concerne i *software*, è prevista la rilevanza penale dell'abusiva duplicazione nonché dell'importazione, distribuzione, vendita e detenzione a scopo commerciale o imprenditoriale e locazione di programmi "pirata".

Il reato in ipotesi si configura nel caso in cui chiunque 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 SIAE.

Il fatto è punito anche se la condotta ha ad oggetto qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori.

Il secondo comma della stessa norma punisce inoltre chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui alla Legge sul Diritto d'Autore.

Sul piano soggettivo, per la configurabilità del reato è sufficiente lo scopo di lucro, sicchè assumono rilevanza penale anche tutti quei comportamenti che non sono sorretti dallo specifico scopo di conseguire un guadagno di tipo prettamente economico (come nell'ipotesi dello scopo di profitto).

Tale reato potrebbe ad esempio essere commesso nell'interesse della società qualora venissero utilizzati, per scopi lavorativi, programmi non originali ai fine di risparmiare il costo derivante dalla licenza per l'utilizzo di un *software* originale.

DUPLICAZIONE, RIPRODUZIONE, TRASMISSIONE – PER USO NON PERSONALE E A SCOPO DI LUCRO – DI UN'OPERA DELL'INGEGNO DESTINATA AL CIRCUITO TELEVISIVO, CINEMATOGRAFICO, DELLA VENDITA O DEL NOLEGGIO (art. 171-ter Legge sul diritto d'autore)

La lunga disposizione tende alla tutela di una serie numerosa di opere dell'ingegno: opere destinate al circuito radiotelevisivo e cinematografico, incorporate in supporti di qualsiasi tipo contenenti fonogrammi e videogrammi di opere musicali, ma anche opere letterarie, scientifiche o didattiche.

A restringere l'ambito di applicabilità della disposizione, però, vi sono due requisiti.

Il primo è che le condotte siano poste in essere per fare un uso non personale dell'opera dell'ingegno, e il secondo è il dolo specifico di lucro, necessario per integrare il fatto tipico.

A titolo esaustivo si riportano qui di seguito anche le fattispecie di reati previsti dall'art. 25-*novies* del Decreto 231 e ritenute, a seguito dell'analisi dei rischi e suggerimenti, non applicabili alla Società.

MANCATA COMUNICAZIONE ALLA SIAE DEI DATI IDENTIFICATIVI DEI SUPPORTI NON SOGGETTI AL CONTRASSEGNO DA PARTE DEI PRODUTTORI O IMPORTATORI DEGLI STESSI (art. 171-septies Legge sul diritto d'autore)

PRODUZIONE, IMPORTAZIONE, VENDITA, ISTALLAZIONE E UTILIZZO PER USO PUBBLICO E PRIVATO, A FINI FRAUDOLENTI, DI APPARATI ATTI ALLA DECODIFICAZIONE DI TRASMISSIONI AUDIOVISIVE AD ACCESSO CONDIZIONATO (art. 171-octies Legge sul diritto d'autore).

Capitolo G.2

G.2.1 Attività Sensibili nell'ambito dei delitti informatici

A seguito di una approfondita analisi della realtà aziendale, le principali Attività Sensibili che la Società ha individuato al proprio interno riguardano il corretto utilizzo e l'idonea protezione dei sistemi informatici, come di seguito indicate:

a) utilizzo della rete aziendale, del servizio di posta elettronica e accesso ad internet;

b) gestione della rete informatica aziendale, evoluzione della piattaforma tecnologica e applicativa IT nonché sicurezza informatica;

c) erogazione di servizi di installazione e servizi professionali di supporto al personale della Società (ad esempio, assistenza, manutenzione, gestione della rete, manutenzione e *security*).

G.2.2. Attività Sensibili nell'ambito dei delitti in violazione del diritto d'autore

In relazione ai delitti in violazione del diritto d'autore, sono state individuate le seguenti Attività Sensibili:

a) utilizzo degli applicativi informatici aziendali, in considerazione del potenziale utilizzo senza licenza di *software* coperti da altrui diritto d'autore;

b) gestione dei contenuti multimediali sulla rete aziendale e in particolare sul sito internet aziendale, in considerazione, tra l'altro, del possibile illegittimo utilizzo all'interno di quest'ultimo di composizioni musicali, immagini o altre opere dell'ingegno coperte da altrui diritto d'autore;

c) riproduzione di opere dell'ingegno coperte dal diritto d'autore.

Capitolo G.3

Regole e principi generali

Obiettivo della presente Parte Speciale è che i Dipendenti, gli Organi Sociali e i soggetti che operano a livello periferico (agenti, sub-agenti, personale d'agenzia, promotori, *broker*) nella misura in cui gli stessi possano essere coinvolti nelle Attività Sensibili, si attengano a regole di condotta conformi a quanto prescritto dalla stessa al fine di prevenire e impedire il verificarsi dei Delitti Informatici e di Delitti in violazione del Diritto d'Autore.

Nell'espletamento delle attività aziendali e, in particolare, nelle Attività Sensibili, è espressamente vietato ai soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, di porre in essere, collaborare o dare causa alla realizzazione di comportamenti, anche omissivi, tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale (art. 24-*bis* e 25 *novies* del Decreto).

In particolare non è ammesso:

- porre in essere quei comportamenti che (i) integrano le fattispecie di reato o, sebbene non costituiscano di per sé un'ipotesi di reato, (ii) possano esserne il presupposto (ad esempio, mancato controllo);
- divulgare informazioni relative ai sistemi informatici aziendali;
- utilizzare i sistemi informatici della Società per finalità non connesse alla mansione svolta o comunque contrarie al Codice Etico/Codice di Comportamento;
- installare autonomamente nel PC in dotazione per uso aziendale *software* non autorizzati dalla Società;
- utilizzare illecitamente materiale tutelato da altrui diritto d'autore.

Nell'espletamento delle rispettive attività/funzioni oltre alle regole di cui al Modello ed alla presente Parte Speciale, i Destinatari sono tenuti a conoscere ed osservare tutte le regole e i principi contenuti nei seguenti documenti:

- la politica aziendale relativa alla gestione degli accessi logici a reti, sistemi, dati e applicazioni;

- la politica aziendale relativa alla gestione delle credenziali personali (*username* e *password*);
- l'impegno alla corretta gestione delle informazioni di cui si viene a conoscenza per ragioni operative.

Al fine di mitigare il rischio di commissione dei Delitti Informatici dei Delitti in violazione del Diritto d'Autore e, di conseguenza, anche di assicurare il corretto adempimento degli obblighi connessi alla normativa di riferimento, la Società, in relazione alle operazioni inerenti lo svolgimento della propria attività, assolve i seguenti adempimenti:

1. fornisce, ai Destinatari, un'adeguata informazione circa il corretto utilizzo degli *user-id* e delle *password* per accedere ai principali sottosistemi informatici utilizzati presso la Società;

2. limita, attraverso abilitazioni di accesso differenti, l'utilizzo dei sistemi informatici e l'accesso agli stessi, da parte dei Destinatari, esclusivamente per le finalità connesse agli impieghi da questi ultimi svolti;

3. effettua, per quanto possibile, nel rispetto della normativa sulla privacy, degli accordi sindacali in essere e dello Statuto dei Lavoratori, controlli periodici sulla rete informatica aziendale al fine di individuare comportamenti anomali;

4. predispone e mantiene adeguate difese fisiche a protezione dei server della Società;

5. predispone e mantiene adeguate difese a protezione degli ulteriori sistemi informatici aziendali;

6. effettua periodici inventari dei *software* e delle banche dati in uso presso l'azienda e verifica che l'utilizzo degli stessi sia legittimato da apposita licenza;

7. effettua, per quanto possibile, controlli periodici sui contenuti del sito internet aziendale.

Capitolo G.4

Principi procedurali specifici

Ai fini dell'attuazione delle regole e del rispetto dei divieti elencati nel precedente Capitolo, devono essere ottemperati i principi procedurali qui di seguito descritti, oltre alle Regole e ai Principi Generali già contenuti nella Parte Generale del presente Modello.

In particolare, si elencano qui di seguito le regole che devono essere rispettate dai destinatari della presente Parte Speciale, meglio individuati nel Capitolo precedente, nell'ambito delle Attività Sensibili:

1. i dati e le informazioni non pubbliche, relative anche a clienti e terze parti (commerciali, organizzative, tecniche), incluse le modalità di connessione da remoto, devono essere gestiti come riservati;

;

2. è vietato in qualunque modo modificare la configurazione di postazioni di lavoro fisse o mobili, senza l'autorizzazione di amministratori di sistema o della funzione IT;

3. è vietato utilizzare strumenti software e/o hardware che potrebbero essere adoperati per valutare o compromettere la sicurezza di sistemi informatici o telematici (sistemi per individuare le password, identificare le vulnerabilità, decifrare i file criptati, intercettare il traffico in transito, ecc.);

4. è vietato ottenere credenziali di accesso a sistemi informatici o telematici aziendali, dei clienti o di terze parti, con metodi o procedure differenti da quelle per tali scopi autorizzate dalla Società;

5. è vietato divulgare, cedere o condividere con personale interno o esterno alla Società le proprie credenziali di accesso ai sistemi e alla rete aziendale, di clienti o terze parti;

6. è vietato accedere ad un sistema informatico altrui (anche di un collega) e manomettere ed alterarne i dati ivi contenuti;

7. è vietato manomettere, sottrarre o distruggere il patrimonio informatico aziendale, di clienti o di terze parti, comprensivo di archivi, dati e programmi;

8. è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici, a meno che non sia esplicitamente previsto nei propri compiti lavorativi;

9. è vietato effettuare prove o tentare di compromettere i controlli di sicurezza di sistemi informatici o telematici di clienti o terze parti a meno che non sia esplicitamente richiesto e autorizzato da specifici contratti o previsto nei propri compiti lavorativi;

10. è vietato sfruttare eventuali vulnerabilità o inadeguatezze nelle misure di sicurezza dei sistemi informatici o telematici, di clienti o di terze parti, per ottenere l'accesso a risorse o informazioni diverse da quelle cui si è autorizzati ad accedere, anche nel caso in cui tale intrusione non provochi un danneggiamento a dati, programmi o sistemi;

11. è vietato comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi e le modalità con cui sono utilizzati;

12. è proibito distorcere, oscurare sostituire la propria identità e inviare e-mail riportanti false generalità o contenenti virus o altri programmi in grado di danneggiare o intercettare dati;

13. è vietato utilizzare immagini, video, composizioni musicali, banche dati ovvero qualsiasi opera dell'ingegno protetta dal diritto d'autore senza aver ottenuto le necessarie licenze e permessi;

14. è vietato utilizzare immagini, video o composizioni musicali senza preventiva autorizzazione da parte del Servizio Marketing al fine di pubblicizzare o promuovere prodotti assicurativi;

15. è vietato riprodurre opere dell'ingegno (quali ad esempio libri o manuali) se non nei limiti del 15% per sola finalità di agevolare la lettura e l'esame delle tematiche ivi trattate.

La Società si impegna, a sua volta, a porre in essere i seguenti adempimenti:

1. informare adeguatamente i Dipendenti e gli altri soggetti eventualmente autorizzati dell'importanza di mantenere i propri codici di accesso (*username* e *password*) confidenziali e di non divulgare gli stessi a soggetti terzi;

2. far sottoscrivere ai Dipendenti e agli altri soggetti eventualmente autorizzati uno specifico documento con il quale gli stessi si impegnino al corretto utilizzo delle risorse informatiche aziendali;

3. informare i Dipendenti e gli altri soggetti eventualmente autorizzati della necessità di non lasciare incustoditi i propri sistemi informatici e della convenienza di

bloccarli, qualora si dovessero allontanare dalla postazione di lavoro, con i propri codici di accesso;

4. impostare i sistemi informatici in modo tale che, qualora non vengano utilizzati per un determinato periodo di tempo, si blocchino automaticamente;

5. fornire un accesso da e verso l'esterno (connessione alla rete Internet) esclusivamente ai sistemi informatici dei Dipendenti o di eventuali soggetti terzi che ne abbiano la necessità ai fini lavorativi o connessi all'amministrazione societaria;

6. limitare gli accessi alla stanza server unicamente al personale autorizzato;

7. proteggere, per quanto possibile, ogni sistema informatico societario al fine di prevenire l'illecita installazione di dispositivi *hardware* in grado di intercettare le comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero capace di impedirle o interromperle;

8. fornire ogni sistema informatico di adeguato software e *antivirus* nonché di un firewall di sistema e far sì che, ove possibile, questi non possano venir disattivati;

9. impedire l'installazione e l'utilizzo di software non approvati dalla Società e non correlati con l'attività professionale espletata per la stessa;

10. limitare l'accesso alle aree ed ai siti Internet particolarmente sensibili poiché veicolo per la distribuzione e diffusione di programmi infetti (c.d. "*virus*") capaci di danneggiare o distruggere sistemi informatici o dati in questi contenuti;

11. impedire l'installazione e l'utilizzo, sui sistemi informatici della Società, di software (c.d. "P2P", di *files sharing* o di *istant messaging*) mediante i quali è possibile scambiare con altri soggetti all'interno della rete Internet ogni tipologia di file (quali filmati, documenti, canzoni, virus, ecc.) senza alcuna possibilità di controllo da parte della Società;

12. qualora per la connessione alla rete Internet si utilizzino collegamenti *wireless* (ossia senza fili, mediante *routers* dotati di antenna *WiFi*), proteggere gli stessi impostando una chiave d'accesso, onde impedire che soggetti terzi, esterni alla Società, possano illecitamente collegarsi alla rete Internet tramite i *routers* della stessa e compiere illeciti ascrivibili ai Dipendenti;

13. prevedere un procedimento di autenticazione mediante *username* e *password* al quale corrisponda un profilo limitato della gestione di risorse di sistema, specifico per ognuno dei Dipendenti e degli altri soggetti eventualmente autorizzati;

14. limitare l'accesso alla rete informatica aziendale dall'esterno, adottando e mantenendo sistemi di autenticazione diversi o ulteriori rispetto a quelli predisposti per l'accesso interno dei Dipendenti e degli altri soggetti eventualmente autorizzati;

15. effettuare qualora le esigenze lo richiedano, in presenza di accordi sindacali che autorizzino in tale senso e ove possibile ai sensi di legge, controlli *ex ante* ed *ex post* sulle attività effettuate dal personale sulle reti;

16. verificare periodicamente la corrispondenza tra i *software* installati nei singoli sistemi informatici aziendali ed il numero di licenze ottenute per il relativo utilizzo;

17. verificare periodicamente la corrispondenza tra le banche dati in uso e il numero delle licenze ottenute per il relativo utilizzo;

18. richiamare periodicamente in modo inequivocabile i propri Dipendenti, anche attraverso apposita attività di formazione, ad un corretto utilizzo degli strumenti informatici in proprio possesso;

19. disciplinare attraverso procedure o *policy* aziendali le modalità attraverso le quali modificare il sito internet aziendale;

20. indicare specificatamente quali figure interne partecipino al processo decisionale di modifica del sito internet aziendale e quali figure siano invece demandate ad attuare effettivamente le modifiche;

21. prevedere che l'accesso al sito internet aziendale a fini di modifica sia attuabile solo in possesso di specifiche *password* a tale scopo generate;

22. verificare periodicamente l'eventuale pubblicazione sul proprio sito internet aziendale di materiale non autorizzato;

23. fornire alle figure aziendali interessate adeguata informazione circa le potenziali rischiosità in materia di responsabilità amministrativa degli enti connesse all'attività di configurazione del sito internet aziendale.

Capitolo G.5

I controlli dell'OdV

G.5.1 Il controllo in generale

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'art. 24-*bis* e all'art. 25-*novies,* D.Lgs. 231/2001 sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'art. 24-*bis* e all'art. 25-*novies* del Decreto 231; con riferimento a tale punto, l'OdV conduce controlli a campione sulle attività potenzialmente a rischio di Delitti Informatici e Delitti in violazione del Diritto d'Autore, diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello e, in particolare, alle procedure interne in essere;

- proporre che vengano aggiornate le procedure aziendali relative alla prevenzione dei Delitti Informatici e dei Delitti in violazione del Diritto d'Autore di cui alla presente Parte Speciale, anche in considerazione del progresso e dell'evoluzione delle tecnologie informatiche;

- proporre e collaborare alla predisposizione delle procedure di controllo relative ai comportamenti da seguire nell'ambito delle Attività Sensibili individuate nella presente Parte Speciale;

- monitorare il rispetto delle procedure e la documentazione interna per la prevenzione dei Delitti Informatici e dei Delitti in violazione del Diritto d'Autore in costante coordinamento con le funzioni IT, *Marketing*, *Compliance* ed *Internal Audit*;

- consultarsi con il responsabile della funzione IT ed invitare periodicamente lo stesso a relazionare alle riunioni dell'OdV;

- consultarsi con il responsabile della funzione *Marketing* ed invitare periodicamente lo stesso a relazionare alle riunioni dell'OdV;

- esaminare le segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari o opportuni;

- conservare traccia dei flussi informativi ricevuti, e delle evidenze dei controlli e delle verifiche eseguiti.

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

PARTE SPECIALE – H –

Delitti di criminalità organizzata

CAPITOLO H.1

Delitti di criminalità organizzata (art. 24-*ter* Decreto 231)

La legge 15 luglio 2009 n. 94, recante disposizioni in materia di sicurezza pubblica ha introdotto nel Decreto 231 l'art. 24 ter (di seguito i "Delitti di Criminalità Organizzata") ampliando la lista dei Reati presupposto alle seguenti fattispecie criminose:

- *"associazione per delinquere"* di cui all'art 416 c.p.;
- *"associazione per delinquere finalizzata alla riduzione o mantenimento in schiavitù o in servitù (ex art. 600 c.p.) alla tratta di persone (ex art. 601 c.p.) o all'acquisto e alienazione di schiavi (ex art. 602 c.p.)"* di cui all'art. 416 comma 6 c.p.;
- "*associazione di stampo mafioso anche straniere"* di cui all'art. 416 bis c.p.;
- *"scambio elettorale politico-mafioso"* di cui all'art. 416 ter c.p.;
- *"sequestro di persona a scopo di rapina o di estorsione"* di cui all'art. 630 c.p.;
- *"associazione a delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope"* di cui all'art. 74 del D.P.R. n. 309/1990;
- *"delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra, di esplosivi e di armi clandestine"* di cui all'art. 407 comma 2, lett. a) n. 5 c.p.p..

Da un'analisi preliminare "dei rischi e dei suggerimenti" concernente le attività svolte dalla Società è emerso che il rischio di commissione dei reati di cui agli articoli 416 comma 6 c.p., 416 bis, 416 ter c.p., 630 c.p. nonché all'art. 74 del D.P.R. n. 309/1990 e all'art. 407 comma 2, lett. a) n. 5 c.p.p. è remoto e solo astrattamente ipotizzabile.

Si fornisce qui di seguito una breve descrizione della fattispecie di cui all'art. 24 ter del Decreto ritenuta prima facie rilevante per la Società e prevista dall'art. 416 c.p..

ASSOCIAZIONE PER DELINQUERE (ART. 416 C.P.)

La condotta sanzionata dall'art. 416 c.p. è integrata mediante la costituzione e la conservazione di un vincolo associativo continuativo con fine criminoso tra tre o più persone, allo scopo di commettere una serie indeterminata di delitti, con la predisposizione di mezzi necessari per la realizzazione del programma criminoso e con la permanente consapevolezza di ciascun associato di far parte di un sodalizio e di essere disponibile ad operare per l'attuazione del programma delinquenziale.

Il reato associativo è caratterizzato, pertanto, dai seguenti elementi fondamentali:

1) *stabilità e permanenza*: il vincolo associativo deve essere tendenzialmente stabile e destinato a durare anche oltre la realizzazione dei delitti concretamente programmati;

2) *indeterminatezza del programma criminoso*: l'associazione a delinquere non si configura se i partecipanti si associano al fine di compiere un solo reato; lo scopo dell'associazione deve essere quello di commettere più delitti, anche della stessa specie (in tal caso l'indeterminatezza del programma criminoso ha riguardo solo all'entità numerica);

3) *esistenza di una struttura organizzativa*: l'associazione deve prevedere un'organizzazione di mezzi e di persone che, seppure in forma rudimentale, siano adeguati a realizzare il programma criminoso e a mettere in pericolo l'ordine pubblico.

In particolare, sono puniti coloro che promuovono, costituiscono o organizzano l'associazione, oltre a coloro che regolano l'attività collettiva da una posizione di superiorità o supremazia gerarchica, definiti dal testo legislativo come "capi".

Sono puniti altresì con una pena inferiore tutti coloro che partecipano all'associazione.

Il reato in questione assume rilevanza ai fini della responsabilità amministrativa degli enti anche se commesso a livello "*transnazionale*" ai sensi dell'art. 10 della Legge 16 marzo 2006, n. 146 (legge di ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale).

A tal riguardo giova sottolineare che ai sensi dell'art. 3 della suddetta legge si considera "transnazionale" il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

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

* * *

Come emerge dalla descrizione del reato in esame, attraverso lo strumento del reato associativo potrebbero essere commessi altri reati, siano essi espressamente previsti dal Decreto 231 oppure non rientranti tra le fattispecie delittuose che autonomamente comportano la responsabilità amministrativa dell'ente. Le tipologie di reati previsti espressamente dal Decreto 231 sono state analizzate ed approfondite nelle relative Parti Speciali (cui occorre rinviare), indipendentemente dalla circostanza che la loro esecuzione avvenga in forma associativa o meno. Quanto invece ai reati non previsti espressamente

dal Decreto 231, da un'analisi preventiva dei rischi e suggerimenti è emersa l'opportunità di dare rilevanza ed autonoma dignità ad alcune tipologie di reati che, in virtù delle condotte sanzionate, risultano *prima facie* a rischio in relazione all'attività assicurativa, ossia i reati tributari e di truffa, soprattutto nella forma della c.d. truffa contrattuale.

A) I reati tributari

I reati tributari, previsti dal D.Lgs. 74/2000 recante la "*nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'art. 9 della legge 25 giugno 1999, n. 205*", sono:

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
- Dichiarazione fraudolenta mediante artifici;
- Dichiarazione infedele;
- Omessa dichiarazione;
- Emissione di fatture o di altri documenti per operazioni inesistenti;
- Occultamento o distruzione di documenti contabili;
- Omesso versamento di ritenute certificate;
- Omesso versamento di IVA;
- Indebita compensazione;
- Sottrazione fraudolenta al pagamento di imposte.

B) Reati di truffa (ex art. 640 c.p.)

Il reato di truffa si configura ai sensi dell'art. 640 c.p. ogni volta che un qualsiasi soggetto, inducendo qualcuno in errore con artifizi o raggiri, procuri per sé o per altri un ingiusto profitto in danno di altri.

Il suddetto reato punisce le condotte aggressive contro il patrimonio personale altrui realizzate attraverso:

- *artifizi*, ossia attraverso una manipolazione o una trasfigurazione della realtà esterna, provocata mediante la simulazione di fatti o circostanze in realtà inesistenti;

- *raggiri*, ossia attraverso un'attività simulatrice posta in essere con parole e argomentazioni che fanno scambiare il falso per il vero.

Si tenga conto che le suddette condotte devono essere idonee ad indurre in errore la vittima e pertanto non rilevano ai fini della configurazione del reato in esame artifizi o raggiri grossolani e palesemente non credibili.

In considerazione dell'attività svolta dalla Società, il suddetto reato assume particolare rilevanza nella forma della c.d. "*truffa contrattuale*", ossia di quella elaborazione giurisprudenziale del reato di truffa ex art. 640 c.p. che è configurabile tutte le volte in cui, nell'ambito di un rapporto contrattuale, uno dei contraenti ponga in essere artifizi o raggiri diretti a tacere o a dissimulare fatti o circostanze tali che, ove conosciuti, avrebbero indotto l'altro contraente ad astenersi dal concludere il contratto.

In tali casi gli artifizi o i raggiri richiesti per la sussistenza del reato possono consistere anche nel silenzio maliziosamente serbato su alcune circostanze da parte di chi abbia il dovere di farle conoscere, indipendentemente dal fatto che dette circostanze potessero essere conoscibili dalla controparte con ordinaria diligenza. Tali fattispecie, pertanto, sono particolarmente diffuse nelle relazioni contrattuali che, essendo connotate da un alto grado di asimmetria informativa, trovano specifica e dettagliata regolamentazione da parte delle Autorità di Vigilanza. Le disposizioni regolamentari, infatti, prevedono in capo ai soggetti vigilati l'obbligo di comportarsi con diligenza e correttezza nell'interesse dei clienti operando in modo che essi siano adeguatamente informati e impongono agli stessi specifici obblighi giuridici di agire in modo tale da assicurare trasparenza ed equo apprezzamento delle condizioni contrattuali.

CAPITOLO H.2

Attività Sensibili

In relazione ai reati e alle condotte criminose sopra esplicitate, le attività ritenute più specificamente a rischio risultano essere, ai fini della presente Parte Speciale, le seguenti:

1. *Selezione del personale*: si tratta di attività finalizzate all'assunzione di personale dipendente e consistenti nell'accertamento dei requisiti di onorabilità e affidabilità in capo ai candidati. Tali attività si svolgono attraverso l'attribuzione di specifico incarico a società di *head hunting* o attraverso la selezione diretta da parte dei responsabili di funzione interessati all'integrazione della risorsa.

   L'Attività Sensibile in esame è legata ai profili di rischiosità connessi – nell'ottica di possibile commissione dei reati associativi – all'impiego in azienda di personale con pendenze penali.

2. *Selezione delle controparti contrattuali*: si tratta di attività finalizzate all'accertamento della sussistenza dei requisiti di onorabilità e affidabilità in capo a:

   - *Intermediari*, ossia ai soggetti operanti nella rete distributiva con i quali la Società stipula accordi di distribuzione dei propri prodotti assicurativi;
   - *Partner commerciali*, ossia fornitori, consulenti e altri enti con i quali la Società potrebbe intraprendere forme di collaborazione contrattualmente regolate (es. associazioni temporanee di impresa – ATI, *joint venture*, consorzi ecc.).

   La selezione delle controparti contrattuali rileva in quanto l'instaurazione di rapporti con le stesse potrebbe rappresentare un fondamentale presupposto fattuale per la successiva commissione dei reati associativi.

3. *Formazione delle scritture contabili, gestione della contabilità e degli adempimenti fiscali*, ossia le attività connesse alla registrazione delle fatture e alla compilazione, tenuta e conservazione delle scritture contabili rilevanti ai fini tributari nonché tutte le attività relative alla predisposizione delle dichiarazioni fiscali ed attività collaterali.

   L'Attività Sensibile in esame si fonda sulla rilevanza dell'attività di formazione delle scritture contabili e di gestione della contabilità in relazione alla potenziale commissione di un reato di natura tributaria.

   Tali attività risultano sensibili su due fronti: nei rapporti commerciali con soggetti

terzi e nei rapporti contrattuali con società del Gruppo ("*Operazioni Infragruppo*").

4. *Attività connesse allo sviluppo di prodotti assicurativi*: si tratta di attività connesse alla predisposizione dei contratti con la clientela, la distribuzione e la commercializzazione degli stessi.

   L'Attività Sensibile in esame si fonda sulla rilevanza dell'attività di predisposizione dei contratti con la clientela in relazione alla potenziale commissione di un reato di truffa contrattuale.

CAPITOLO H.3

Regole e principi generali

H.3.1 Il sistema in linea generale

Obiettivo della presente Parte Speciale è che i Destinatari del Modello si attengano – nella misura in cui gli stessi siano coinvolti nello svolgimento delle Attività Sensibili o di attività alle stesse connesse nonchè in considerazione della diversa posizione e dei diversi obblighi che ciascuno di essi assume nei confronti della Società – a regole di condotta conformi a quanto prescritto nella stessa al fine di prevenire e impedire il verificarsi dei Delitti di Criminalità Organizzata.

In particolare, la presente Parte Speciale ha la funzione di fornire:

- un elenco dei principi generali nonché dei principi procedurali specifici cui i Destinatari sono tenuti ad attenersi per una corretta applicazione del Modello;
- all'OdV ed ai responsabili delle funzioni aziendali chiamati a cooperare con lo stesso, i principi e gli strumenti operativi necessari al fine di poter esercitare le attività di controllo, monitoraggio e verifica agli stessi demandati.

Nell'espletamento delle rispettive attività/funzioni, oltre alle regole di cui al presente Modello, i Destinatari sono tenuti, in generale, a rispettare tutte le regole e i principi disposti dalla Società e dal Gruppo alla quale la stessa appartiene.

H.3.2 Principi generali di comportamento

I seguenti principi di carattere generale si applicano a tutti i Destinatari.

In via generale, è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate; sono altresì proibite le violazioni ai principi ed alle procedure aziendali richiamate nella presente Parte Speciale.

In generale, in relazione ai reati di associazione per delinquere:

a) è fatto divieto di procedere all'assunzione di personale dipendente senza aver rispettato le procedure di assunzione adottate dalla Società e senza aver prima constatato

la sussistenza di requisiti di onorabilità e affidabilità; è inoltre fatto divieto di favorire candidati per il solo fatto che gli stessi siano legati da rapporti di parentela, affinità o amicizia con soggetti operanti all'interno della Società;

b) è fatto divieto di instaurare rapporti con soggetti terzi - persone fisiche o giuridiche, italiane o straniere - senza aver rispettato i criteri e le metodologie di selezione previsti dalle procedure aziendali.

In particolare, in relazione ai reati di associazione per delinquere finalizzati alla realizzazione di reati tributari:

3. è fatto divieto di emettere fatture per operazioni non esistenti o altri documenti falsi attestanti costi spese o altre passività al fine di abbattere il reddito imponibile, l'IVA o altre imposte (es. contratti di locazione o compravendita, false ricevute fiscali, falsi certificati di sostituti di imposta, contratti simulati di cessione del credito ecc.);

4. è fatto divieto di intestare conti correnti a prestanomi, aprire e gestire fondi extracontabili e intestare beni fittiziamente;

5. è fatto divieto di *i)* emettere fatture o altri documenti per operazioni in tutto o in parte inesistenti *ii)* emettere fatture o altri documenti recanti l'indicazione di corrispettivi o IVA in misura superiore a quella reale o nomi diversi da quelli veri affinché, pur risultando veritiera la cessione o la prestazione, il relativo costo possa essere realizzato da soggetti diversi da coloro che hanno fruito della prestazione o cessione;

6. è fatto divieto di occultare o distruggere tutti o parte dei documenti la cui tenuta è obbligatoria, in misura totale o anche solo tale da rendere impossibile la ricostruzione di tutta la gestione economica del contribuente per quell'anno.

In relazione ai reati di associazione per delinquere finalizzati alla realizzazione di truffe contrattuali:

7. è fatto divieto di commercializzare polizze assicurative attraverso canali distributivi non autorizzati dalla Società;

8. è fatto divieto di commercializzare polizze assicurative attraverso soggetti non autorizzati all'intermediazione dei prodotti assicurativi;

9. è fatto divieto indurre con frode, con raggiri o con artifizi un consumatore a stipulare una polizza o ad acquistare un prodotto assicurativo.

CAPITOLO H.4

Principi procedurali specifici

H.4.1 Principi procedurali specifici generalmente applicabili

Ai fini dell'attuazione dei principi e regole generali e dei divieti elencati al precedente cap. H.3, devono rispettarsi gli specifici principi procedurali qui di seguito descritti, oltre alle regole e principi generali già contenuti nella Parte Generale del Modello. Le regole qui di seguito descritte, devono essere rispettate sia nell'esplicazione dell'attività della Società in territorio italiano, sia eventualmente all'estero.

Al fine di prevenire eventuali infiltrazioni criminali nell'esercizio dell'attività aziendale sono previsti a carico degli Esponenti Aziendali e dei Dipendenti, ciascuno per le attività di propria competenza, i seguenti obblighi:

- non sottostare a richieste di qualsiasi tipo contrarie alla legge e darne, comunque, informativa al proprio diretto superiore il quale, a sua volta, dovrà darne comunicazione all'Amministratore Delegato e all'Organismo di Vigilanza;
- consentire l'accesso alle aree aziendali soltanto a persone autorizzate.

E' in ogni caso fatto obbligo a ciascun Esponente Aziendale, anche per il tramite di propri superiori gerarchici, segnalare all'OdV qualsiasi elemento da cui possa desumersi il pericolo di interferenze criminali in relazione all'attività aziendale e la Società si impegna a tal riguardo a garantire la riservatezza a coloro che adempiano ai suddetti obblighi di segnalazione o denuncia con un pieno supporto, anche in termini di eventuale assistenza legale.

La Società nell'ambito della propria organizzazione si dota dei seguenti presidi:

1. procedure di selezione e assunzione del personale dipendente di qualsiasi livello e di collaboratori a progetto che garantiscano un criterio di trasparenza sulla base dei seguenti parametri:

- professionalità adeguata rispetto all'incarico o alle mansioni da assegnare;
- uguaglianza di trattamento tra i diversi candidati;
- affidabilità rispetto al rischio di infiltrazione criminale: a tal riguardo, la Società assicura che vengano prodotti da ciascun Dipendente prima dell'assunzione i seguenti documenti:
    - casellario giudiziario, o

- certificato dei carichi pendenti, non anteriore a tre mesi.
- in alternativa ai suddetti certificati penali può essere richiesto il rilascio dell'autocertificazione con la quale il candidato selezionato dichiara di non aver subito condanna e di non avere procedimenti penali in corso per reati di associazione a delinquere, per reati di stampo mafioso e altri reati rilevanti ai fini della responsabilità amministrativa degli enti (es. riciclaggio, reati societari etc.) o specificamente connessi all'attività svolta dalla Società (es. tributari e fiscali, frodi etc.).

La Società conserva la documentazione esibita in sede di assunzione da parte del dipendente anche al fine di consentirne la consultazione da parte dell'OdV nell'espletamento della consueta attività di vigilanza e controllo.

2. nella selezione e successiva gestione del rapporto contrattuale con Consulenti e Partner commerciali, la Società adotta procedure o *policy* aziendali volte a garantire che il processo di selezione avvenga nel rispetto dei criteri di trasparenza, pari opportunità di accesso, professionalità, affidabilità ed economicità, fermo restando la prevalenza dei requisiti di legalità rispetto a tutti gli altri. A tal fine le procedure prevedono:

- la predisposizione di specifiche liste di consulenti, fornitori e altre controparti contrattuali con i quali siano già intercorsi rapporti contrattuali;
- qualora si intenda intrattenere rapporti contrattuali con soggetti non inseriti nella lista sopra menzionata e salvo che si tratti di soggetti sottoposti a vigilanza pubblica, la richiesta di esibizione del certificato antimafia;
- con particolare riferimento ai professionisti, la richiesta di documentazione comprovante l'iscrizione all'ordine professionale, all'albo e all'elenco appositamente formato e tenuto dalle autorità pubbliche;
- la richiesta di informazioni sulle esperienze pregresse nello stesso ambito di attività o settore merceologico.

Ad integrazione dei principi sopra esposti, nel caso di instaurazione di rapporti continuativi con controparti contrattuali, la Società si impegna ad attuare efficacemente controlli periodici circa la persistenza in capo a questi ultimi dei requisiti che in fase di selezione iniziale hanno permesso l'instaurazione del rapporto;

3. nei rapporti contrattuali con Partner Commerciali, Consulenti o altri soggetti terzi, la Società prevede apposite clausole che consentano di risolvere immediatamente il

rapporto nel caso di condanna anche non definitiva per reati di associazione a delinquere, per reati di stampo mafioso e altri reati rilevanti ai fini della responsabilità amministrativa degli enti (es. riciclaggio, reati societari etc.) o specificamente connessi all'attività svolta dalla Società (es. tributari e fiscali, frodi etc.);

H.4.2 Principi procedurali specifici relativi ai reati tributari

1. Nella predisposizione e successiva tenuta delle scritture contabili rilevanti ai fini tributari, anche in relazione alle attività svolte per le altre società del Gruppo, la Società pone in essere una serie di misure idonee ad assicurare che gli Esponenti Aziendali e i Destinatari – nell'ambito delle rispettive competenze:

- custodiscano in modo corretto ed ordinato le scritture contabili e gli altri documenti di cui sia obbligatoria la conservazione ai fini fiscali, approntando difese fisiche e/o informatiche che impediscano eventuali atti di distruzione e/o occultamento;
- siano rispettate le disposizioni dell'Autorità di Vigilanza in materia contabile e fiscale.

I presidi adottati dalla Società, devono altresì:

- disciplinare l'interazione tra tutte le figure aziendali coinvolte nella compilazione delle dichiarazioni di natura contabile, attraverso una precisa specificazione dei singoli ruoli;
- disciplinare il coordinamento delle funzioni interne della Società con eventuali *outscourcer* (o consulenti) coinvolti nella redazione delle suddette scritture;
- attuare un attento monitoraggio del rispetto dei principi che regolano la compilazione, tenuta e conservazione delle dichiarazioni di natura contabile;
- prevedere un controllo finale di tipo "operativo" che consenta di accertare la veridicità e la completezza dei dati riflessi nelle dichiarazioni di natura contabile.

2. Nella predisposizione delle dichiarazioni annuali relative alle imposte sui redditi e sul valore aggiunto, anche in relazione alle attività svolte per le altre società del Gruppo, la Società si dota di presidi tali che gli Esponenti Aziendali - nell'ambito delle rispettive competenze:

- non indichino elementi passivi fittizi avvalendosi di fatture o altri documenti aventi rilievo probatorio analogo alle fatture, per operazioni inesistenti;
- non indichino elementi attivi per un ammontare inferiore a quello effettivo o elementi passivi fittizi (es. costi fittiziamente sostenuti e/o ricavi indicati in misura inferiore a quella reale) facendo leva su una falsa rappresentazione nelle scritture contabili obbligatorie e avvalendosi di mezzi idonei ad ostacolarne l'accertamento;
- non indichino una base imponibile in misura inferiore a quella effettiva attraverso l'esposizione di elementi attivi per un ammontare inferiore a quello reale o di elementi passivi fittizi;
- non facciano decorrere inutilmente i termini previsti dalla normativa applicabile per la presentazione delle medesime così come per il successivo versamento delle imposte da esse risultanti.

3. La Società assicura una prevenzione delle rischiosità potenzialmente connesse all'attività di fatturazione infragruppo, attraverso:

- proceduralizzazione delle singole fasi di emissione delle fatture infragruppo e dell'interazione tra le diverse figure aziendali che prendono parte a tale attività;
- controllo sistematico dell'effettivo espletamento da parte della Società dell'attività per cui viene emessa relativa fattura;
- previsione di periodiche verifiche circa il rispetto dei principi sopra esposti.

4. La Società, anche attraverso la predisposizione di specifiche procedure, si impegna a garantire l'attuazione del principio di segregazione dei ruoli in relazione alle attività di gestione delle contabilità aziendale e nella successiva trasposizione nelle dichiarazioni tributarie con riferimento, a titolo esemplificativo, a:

- controllo sull'effettività delle prestazioni rispetto alle fatture emesse;
- verifica della veridicità delle dichiarazioni rispetto alle scritture contabili;
- verifica della corrispondenza tra i certificati rilasciati in qualità di sostituto d'imposta e l'effettivo versamento delle ritenute.

Si rinvia in ogni caso ai principi procedurali contenuti nella Parte Speciale B del presente Modello.

H.4.3. Principi procedurali specifici relativi alla frode contrattuale

1. Nei confronti della clientela la Società si impegna a svolgere la propria attività con trasparenza, diligenza e professionalità, sin dalla prima fase di informazione precontrattuale e durante tutto il rapporto di fornitura dei servizi assicurativi, compresa l'assistenza durante l'esecuzione del rapporto contrattuale, la liquidazione dei sinistri, nonché in caso di reclamo.

2. la Società, anche nell'osserva delle disposizioni emanate dall'Autorità di Vigilanza, si dota di procedure o *policy* aziendali volte a specificare le diverse fasi di progettazione, commercializzazione, pubblicizzazione e gestione dei rapporti contrattuali che prevedano, in particolare:

- la definizione degli obiettivi, delle metodologie e delle funzioni coinvolte nelle diverse fasi di analisi, studio, controllo di conformità, realizzazione, promozione e pubblicità dei prodotti assicurativi;
- la definizione dei processi autorizzativi alla commercializzazione e pubblicizzazione dei nuovi prodotti;
- l'istituzione di un comitato interfunzionale (Comitato Nuove Attività e Prodotti) il quale, composto dai responsabili delle funzioni interessate allo sviluppo e alla promozione di nuovi prodotti assicurativi nonchè alla redazione delle disposizioni contrattuali, definisca gli obiettivi, le modalità e i contenuti principali dei prodotti di nuova erogazione o le modifiche da apportare ai prodotti già erogati dalla Società;
- la verbalizzazione degli incontri del suddetto comitato, nonché appositi flussi informativi con l'organo amministrativo.

3. La Società affida la distribuzione dei propri prodotti esclusivamente a soggetti autorizzati dall'Autorità di Vigilanza all'attività di intermediazione assicurativa e selezionati sulla base dei criteri di cui al capitolo H.4.1;

4. la Società, in conformità alle disposizioni di Vigilanza, effettua controlli sulla vendita dei prodotti assicurativi volti specificamente a verificare la corretta esposizione ai clienti da parte degli intermediari delle condizioni generali di polizza in fase precontrattuale, nonché la raccolta e conservazione di tutta la documentazione e delle informazioni necessarie per la profilazione del cliente;

5. la Società si impegna a fornire ai propri intermediari tutte le informazioni, istruzioni e documenti necessari alla commercializzazione delle polizze assicurative, nonché ad organizzare adeguati corsi di formazione;

6. la Società si dota di risorse e strumenti conformi alla normativa di Vigilanza volti a garantire al cliente l'ottenimento di informazioni o chiarimenti esaustivi sui rapporti contrattuali in essere nonché la gestione di eventuali reclami,

7. la Società individua i criteri e le modalità per la gestione del contenzioso e la definizione di accordi transattivi con la clientela.

Capitolo H.5

I controlli dell'OdV

H.5.1 Il controllo in generale

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i Reati di cui alla presente Parte Speciale sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare periodicamente l'efficacia della stessa a prevenire la commissione dei Reati quivi previsti. Con riferimento a tale punto l'OdV - avvalendosi eventualmente della collaborazione di consulenti tecnici competenti in materia - condurrà una periodica attività di analisi sulla funzionalità del sistema preventivo adottato con la presente Parte Speciale e proporrà alle funzioni competenti eventuali azioni migliorative o modifiche qualora vengano rilevate violazioni significative delle previsioni contenute nella presente Parte Speciale;;
- proporre e collaborare nella predisposizione delle istruzioni standardizzate relative ai comportamenti da seguire nell'ambito delle Attività Sensibili

individuate nella presente Parte Speciale; tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico;

- esaminare eventuali segnalazioni di presunte violazioni del Modello ed effettuare gli accertamenti ritenuti necessari od opportuni in relazione alle segnalazioni ricevute.

Allo scopo di adempiere adeguatamente ai propri compiti, l'OdV può organizzare specifici incontri con:

a) i Responsabili delle funzioni Legale/Risorse Umane in merito ad eventuali segnalazioni di procedimenti penali in corso che vedano coinvolti Esponenti Aziendali o altri Destinatari per reati associativi o per altri reati rilevanti ai fini della responsabilità amministrativa degli enti (es. riciclaggio, reati societari etc.) o specificamente connessi all'attività svolta dalla Società (es. reati tributari e fiscali, frodi etc.)

b) L'Amministratore Delegato in merito ad eventuali anomalie riscontrate nella gestione degli adempimenti fiscali che, *prima facie*, potrebbero assumere rilevanza penale.

E' altresì attribuito all'OdV il potere di accedere o di richiedere ai propri delegati di accedere a tutta la documentazione e a tutti i siti rilevanti per lo svolgimento dei propri compiti.

Al fine di dare attuazione ai principi di cui alle lett. a) e b) che precedono, la Società prevede l'istituzione di flussi informativi proceduralizzati nei confronti dell'OdV. Tali flussi informativi dovranno essere idonei a consentire a quest'ultimo di acquisire le informazioni utili per il monitoraggio delle anomalie rilevanti ai sensi della presente Parte Speciale e delle criticità rilevate in tale ambito.

Fermo restando quanto appena indicato, l'informativa all'OdV dovrà essere data senza indugio nel caso in cui si verifichino violazioni ai principi procedurali specifici contenuti nel capitolo H.4 della presente Parte Speciale ovvero alle procedure, *policy* e normative aziendali attinenti alle Attività Sensibili sopra individuate.

PARTE SPECIALE – I –

Delitti contro l'industria e il commercio e delitti di contraffazione

CAPITOLO I.1

A) Delitti contro l'industria e il commercio

La Legge 23 luglio 2009, n. 99 ha esteso la responsabilità amministrativa degli enti prevista dal Decreto 231 ai "*delitti contro l'industria e il commercio*" (art. 25 *bis* 1.) configurabili ogni qualvolta venga commesso nell'interesse o a vantaggio dell'ente una delle seguenti fattispecie di reati:

- *turbata libertà dell'industria o del commercio* (art. 513 c.p.);
- *illecita concorrenza con minaccia o violenza* (art. 513 bis c.p.);
- *frodi contro le industrie nazionali* (art. 514 c.p.);
- *frode nell'esercizio del commercio* (art. 515 c.p.);
- *vendita di sostanze alimentari non genuine come genuine* (art. 516 c.p.);
- *vendita di prodotti industriali con segni mendaci* (art. 517 c.p.);
- *fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale* (art. 517 ter c.p.);
- *contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari* (art. 517 quater c.p.).

Si provvede a fornire qui di seguito una breve descrizione dei reati che sono risultati astrattamente configurabili in relazione all'attività aziendale svolta dalla Società.

TURBATA LIBERTA' DELL'INDUSTRIA E DEL COMMERCIO (ART. 513 C.P.)

Risponde del delitto di turbata libertà dell'industria e del commercio ai sensi dell'art. 513 c.p. chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di una industria o di un commercio.

Tale norma ha ad oggetto la tutela del libero esercizio dell'industria, ossia di qualsiasi forma di organizzazione che tenda a concentrare l'attività produttiva, e del commercio, inteso come esercizio abituale dell'acquisto e della rivendita dei beni a scopo di guadagno: rientrano, pertanto, nell'ambito di protezione della norma tutti i tipi di attività economica che rispettino i requisiti di organizzazione, economicità e professionalità stabiliti dall'art. 2082 c.c. per l'esercizio dell'attività imprenditoriale.

In particolare la condotta dell'intermediario deve essere concretamente idonea a:

- *impedire*, ossia a contrastare anche temporaneamente o parzialmente l'esercizio dell'attività industriale o commerciale;
- *turbare*, ossia alterare il regolare e libero svolgimento dell'attività industriale o commerciale.

La fattispecie in oggetto prevede alternativamente l'uso della violenza sulle cose o di mezzi fraudolenti. In relazione alla prima, deve farsi riferimento all'art. 392 co.2 c.p. il quale prevede in generale che "*agli effetti della legge penale si ha «violenza sulle cose» allorché la cosa venga danneggiata o trasformata o ne è mutata la destinazione*".

Con riferimento alla definizione di mezzi fraudolenti, invece, non essendo previsto alcunché dalle norme del codice penale, devono intendersi tali tutti i mezzi che sono in concreto idonei a trarre in inganno la vittima (es. artifizi, raggiri e menzogne).

La condotta tipica nella prassi si manifesta attraverso atti di concorrenza sleale, intendendosi per tali quelli commessi da colui che ai sensi dell'art. 2598 c.c.:

a. usa nomi o segni distintivi idonei a produrre confusione con nomi o segni distintivi legittimamente usati da altri o imita servilmente i prodotti di un concorrente, o compie con qualsiasi altro mezzo atti idonei a creare confusione con i prodotti o con altre attività di un concorrente;
b. diffonde notizie e apprezzamenti sui prodotti e sull'attività di un concorrente, idonei a determinarne il discredito, o si appropria di pregi dei prodotti o dell'impresa di un concorrente;
c. si avvale direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale e idoneo a danneggiare l'altrui azienda.

Ai fini della rilevanza penale e, quindi, delle configurabilità del reato è comunque necessario che i suddetti comportamenti siano idonei concretamente a impedire o turbare l'esercizio dell'attività industriale o commerciale e che siano posti in essere con violenza o quantomeno con mezzi fraudolenti. In caso contrario rimangono sanzionabili solo ai sensi dell'art. 2599 c.c. e 2600 c.c. attraverso un provvedimento giudiziario volto ad inibire il comportamento sleale, ad eliminarne gli effetti e a liquidare il risarcimento dei danni provocati (con possibile pubblicazione della sentenza).

Il suddetto reato potrebbe configurarsi in astratto qualora la Società adotti politiche di commercializzazione o pubblicizzazione particolarmente aggressive e condotte attraverso raggiri o simulazioni al fine di sviare la clientela di un determinato *competitor* oppure nel

caso in cui utilizzi mezzi fraudolenti diretti nei confronti di un intermediario assicurativo che collabora con un *competitor* al fine di indurlo a cessare la propria attività di promozione dei prodotti assicurativi concorrenti e, quindi, di conquistare la quota di mercato.

ILLECITA CONCORRENZA CON MINACCIA O CON VIOLENZA (ART. 513 BIS C.P.)

L'art. 513 *bis* punisce chiunque nell'esercizio di una attività commerciale, industriale o comunque produttiva, compie atti di concorrenza con violenza o minaccia.

Gli atti di concorrenza previsti dalla norma non sono di per sé illeciti e consistono in un insieme di attività compiute al fine di produrre o vendere di più rispetto agli altri esercenti la stessa attività o attività simile. Tali atti diventano illeciti e integrano, quindi, il suddetto reato solo nel caso in cui vengano compiuti con violenza, ossia impiegando energia fisica sulla persona o sulle cose, o con minaccia ossia prospettando ad una persona un male ingiusto e futuro il cui verificarsi dipenderà dalla volontà del minacciante.

L'intermediario tende attraverso le suddette condotte ad eliminare i concorrenti, reprimendo la loro capacità di autodeterminarsi.

B) I reati di contraffazione

La Legge 23 luglio 2009, n. 99 ha introdotto, altresì, all'interno dei reati di "*falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento*" di cui all'art. 25 bis del Decreto 231 le fattispecie di "*contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni*" (di seguito, i "**delitti di contraffazione**") e di "*introduzione nello Stato e commercio di prodotti con segni falsi*", previste rispettivamente dagli art. 473 c.p. e art. 474 c.p..

Si provvede a fornire qui di seguito una breve descrizione del reato di cui all'art. 473 c.p., in quanto ritenuto *prima facie* rilevante in relazione all'attività svolta dalla Società.

CONTRAFFAZIONE, ALTERAZIONE O USO DI MARCHI O SEGNI DISTINTIVI OVVERO DI BREVETTI, MODELLI E DISEGNI (ART. 473 C.P.)

L'art. 473 c.p. sanziona penalmente:

a) chiunque, potendo conoscere dell'esistenza del titolo di proprietà industriale,

contraffà o altera marchi o segni distintivi, nazionali o esteri, di prodotti industriali;

b) chiunque, senza essere incorso nella contraffazione o alterazione, fa uso di tali marchi o segni contraffatti o alterati.

La norma ha ad oggetto la tutela di segni distintivi o di prodotti industriali, ossia di:

- *marchi*: segni (emblema, figura, denominazione etc.) destinati a distinguere merci o prodotti di una determinata impresa;
- *brevetti*: attestati con i quali è concesso il diritto all'uso esclusivo di una invenzione o di una scoperta;
- *disegni industriali*: rappresentazione figurativa di qualsiasi bene o prodotto industriale;
- *modello industriale*: archetipo di una scoperta o di una nuova applicazione industriale (es. modelli ornamentali e modelli di utilità).

La condotta criminosa consiste nella falsificazione del segno distintivo in modo tale da ingenerare confusione nella distinzione dei segni e può quindi consistere nella:

- *contraffazione*, ossia nella creazione di cosa del tutto simile ad un'altra in modo da trarre in inganno sulla sua essenza;
- *alterazione*, ossia nella modificazione dell'aspetto, della sostanza o della natura di una cosa.

La condotta viene penalmente sanzionata anche nel caso di utilizzo commerciale o industriale dei marchi o dei segni distintivi già falsificati e, quindi, anche non di contraffazione o alterazione *strictu sensu*.

Il reato potrebbe configurarsi in relazione all'utilizzo da parte della Società di segni distintivi già registrati da altre società operanti nello stesso ambito di attività e per commercializzare un prodotto assicurativo avente peculiari caratteristiche. Tale condotta, creando confusione nei prodotti assicurativi, potrebbe avvantaggiare la Società inducendo gli assicurati a sottoscrivere polizze assicurative che già ritengono di conoscere.

CAPITOLO I.2

Attività Sensibili nell'ambito dei delitti contro l'industria e il commercio e dei reati di contraffazione

Dall'analisi dei rischi e suggerimenti è emerso che i delitti contro l'industria e il commercio sono difficilmente configurabili da parte della Società ma, tuttavia, non possono essere sottovalutati. A tal proposito, la Società ha individuato nel proprio ambito di operatività le seguenti Attività Sensibili che risultano maggiormente esposte al rischio di commissione dei Reati in oggetto:

a. rapporti commerciali con gli intermediari assicurativi di altre compagnie non appartenenti al Gruppo Crédit Agricole;
b. commercializzazione e pubblicizzazione dei prodotti assicurativi (nuovi ovvero già esistenti) e relativa informativa ai consumatori;
c. partecipazione a gare d'appalto o a procedure di *beauty contest*.

CAPITOLO I.3

Regole e principi generali

Sebbene la commissione di delitti contro l'industria e il commercio sia solo astrattamente ipotizzabile, con la presente Parte Speciale la Società intende disporre regole di condotta uniformi destinate a tutti i Dipendenti e agli Organi Sociali della Società al fine di prevenire e impedire il verificarsi di condotte criminose che possano integrare i reati di turbata libertà dell'industria e del commercio o illecita concorrenza con minaccia o con violenza nonché i delitti di contraffazione.

Nell'espletamento delle attività aziendali e, in particolare, nelle Attività Sensibili, è espressamente vietato ai soggetti sopra indicati, anche in relazione al tipo di rapporto posto in essere con la Società, porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate nella presente Parte Speciale (artt. 25 *bis* e 25-*bis* 1. del Decreto).

In particolare non è ammesso:

1. intrattenere rapporti d'affari con intermediari assicurativi di altre compagnie assicurative concorrenti, se non nelle forme e con le modalità stabilite dalle procedure aziendali;
2. usare nomi o segni distintivi per la commercializzazione dei prodotti assicurativi che siano idonei a produrre confusione con nomi o segni distintivi legittimamente usati da altre compagnie assicurative;
3. imitare servilmente i prodotti di un concorrente che abbiano caratteristiche peculiari e specifiche tali da poter essere considerate proteggibili dalla normativa oggetto della presente Parte Speciale;
4. compiere qualsiasi atto idoneo a creare confusione tra i prodotti assicurativi della Società e i prodotti di un concorrente;
5. diffondere notizie e/o apprezzamenti sui prodotti e sull'attività di un concorrente che siano anche solo potenzialmente idonei a determinarne il dis o;
6. partecipare a gare d'appalto o *beauty contest* qualora tale attività non rientri nella propria *job description* ovvero, in tale ultima ipotesi, senza preventiva autorizzazione da parte delle funzioni competenti;

7. utilizzare marchi diversi da quelli espressamente autorizzati dalla Società per la commercializzazione e pubblicizzazione dei prodotti assicurativi;

8. utilizzare segni distintivi già registrati da altre società per commercializzare e pubblicizzare i prodotti assicurativi.

Al fine di mitigare il rischio di commissione dei Delitti di contraffazione e, di conseguenza, anche di assicurare il corretto adempimento degli obblighi connessi alla normativa di riferimento, la Società, in relazione alle operazioni inerenti lo svolgimento della propria attività, assolve i seguenti adempimenti:

1. predispone un registro di tutti i marchi e i segni distintivi concessi in uso alla Società da parte di altre società (anche del Gruppo di appartenenza) o da altri soggetti che ne sono titolari;
2. predispone presidi volti ad accertare l'inconfondibilità dei segni distintivi utilizzati per commercializzare e pubblicizzare i prodotti assicurativi;
3. a tal fine prevede la necessaria consultazione delle banche dati messe a disposizione dall'Ufficio Italiano Brevetti – anche tramite consulenti esterni – prima dell'utilizzo a scopi commerciali di segni o simboli grafici che possano costituire marchi già registrati

CAPITOLO I.4

Principi procedurali specifici

Ai fini dell'attuazione delle regole e del rispetto dei divieti elencati nel precedente Capitolo, devono essere ottemperati i principi procedurali qui di seguito descritti, oltre alle Regole e ai Principi Generali già contenuti nella Parte Generale del presente Modello.

In particolare, si elencano qui di seguito le regole che devono essere rispettate dai destinatari della presente Parte Speciale, meglio individuati nel Capitolo precedente, nell'ambito delle Attività Sensibili:

1. è fatto divieto di utilizzare minaccia, violenza o mezzi fraudolenti al fine di indurre un intermediario assicurativo a cessare o ridurre o modificare a proprio vantaggio l'attività di promozione dei prodotti assicurativi di un *competitor*;
2. è fatto divieto di utilizzare nomi o segni distintivi per la commercializzazione dei prodotti assicurativi che non siano stati previamente oggetto di valutazione da parte delle funzioni competenti a svolgere indagini relative alla potenziale idoneità degli stessi a confondere la clientela;
3. diffondere notizie su compagnie assicurative concorrenti, attraverso la stampa, internet ovvero qualsiasi altro mezzo di comunicazione senza preventiva autorizzazione e senza seguire le procedure aziendali che disciplinano tale processo;
4. denigrare un concorrente o, comunque, convincere fraudolentemente un appaltatore a scegliere la Società preferendola ad altre nell'ambito di una gara d'appalto o di un *beauty contest*.
5. è fatto divieto di inserire nella carta intestata, nei documenti contenenti le polizze assicurative, nelle *brochure* pubblicitarie, nel sito internet e in qualsiasi altro supporto cartaceo o informatico simboli o segni grafici prima che non sia stata verificata la non registrazione dei medesimi nonché l'inconfondibilità degli stessi attraverso indagini e consultazioni di banche dati messe a disposizione dall'Ufficio Italiano Marchi e Brevetti;
6. è fatto divieto di inserire nella carta intestata, nei documenti contenenti le polizze assicurative, nelle *brochure* pubblicitarie, nel sito internet e in qualsiasi altro supporto cartaceo o informatico simboli o segni grafici prima che non sia stata ottenuta espressa autorizzazione dalle funzioni competenti.

La Società:

1. prevede linee guida di comportamento nei rapporti d'affari con gli intermediari assicurativi;
2. predispone presidi volti ad accertare l'inconfondibilità dei segni distintivi utilizzati per commercializzare e pubblicizzare i prodotti assicurativi;
3. predispone presidi volti ad evitare la diffusione di informazioni o di apprezzamenti che possano essere lesivi delle attività commerciali dei competitors;
4. dispone procedure che individuino le funzioni competenti, i criteri e le modalità di partecipazione alle gare d'appalto o di beauty contest;
5. prevede all'interno delle procedure relative allo sviluppo e alla commercializzazione dei prodotti assicurativi un processo di consultazione delle banche dati messe a disposizione dall'Ufficio Italiano Marchi e Brevetti da attuarsi ogni volta che si intendano utilizzare nuovi segni o simboli grafici;
6. dispone un elenco di tutti i marchi e i segni distintivi utilizzati (e, pertanto, utilizzabili) dalla Società per la commercializzazione e pubblicizzazione dei prodotti assicurativi, prevedendo apposita procedura aziendale per l'utilizzo di nuovi marchi o segni distintivi;
7. predispone controlli sui contenuti del sito internet, delle brochure pubblicitarie e su altri eventuali supporti informatici o cartacei attraverso i quali sono commercializzati e/o pubblicizzati i prodotti assicurativi.

Capitolo I.5

I controlli dell'OdV

I compiti di vigilanza dell'OdV in relazione all'osservanza del Modello per quanto concerne i delitti di cui all'art. 25-*bis* 1 D.Lgs. 231/2001 sono i seguenti:

- svolgere verifiche periodiche sul rispetto della presente Parte Speciale e valutare regolarmente la sua efficacia a prevenire la commissione dei delitti di cui all'artt. 25 *bis* e 25-*bis* 1 del Decreto 231;
- consultarsi con il responsabile delle funzioni Marketing e Commerciale ogni qualvolta sorga il sospetto di violazione dei principi comportamentali previsti dalla presente Parte Speciale.

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