



PARTE SPECIALE I

***PRINCIPI GENERALI DI COMPORTAMENTO APPLICABILI ALLE
ALTRE FATTISPECIE DI REATO RILEVANTI***



INDICE

I. PRINCIPI GENERALI DI COMPORTAMENTO APPLICABILI ALLE ALTRE FATTISPECIE DI REATO RILEVANTI	3
I. 1 Principi generali di comportamento applicabili ai reati di cui all'art. 24 <i>bis</i>	3
I. 2 Principi generali di comportamento applicabili ai reati di cui all'art. 25 <i>bis</i> 1.....	5
I. 3 Principi generali di comportamento applicabili ai reati di cui all'art. 25 <i>quater</i>	7
I. 4 Principi generali di comportamento applicabili ai reati di cui all'art. 25 <i>quinquies</i>	9
I. 5 Principi generali di comportamento applicabili ai reati di cui all'art. 25 <i>novies</i>	11
I. 6 Principi generali di comportamento applicabili ai reati di cui all'art. 25 <i>duodecies</i>	12
I. 7 Principi generali di comportamento applicabili ai reati di cui all'art. 25 <i>sexiesdecies</i>	13
I. 8 Principi generali di comportamento descritti dal Codice Etico di Gruppo	14



I. PRINCIPI GENERALI DI COMPORTAMENTO APPLICABILI ALLE ALTRE FATTISPECIE DI REATO RILEVANTI

Tutti i Destinatari del Modello, così come individuati nella Parte Generale del medesimo, sono chiamati all'osservanza dei principi generali di comportamento di seguito indicati, nonché ad adottare, ciascuno in relazione alla funzione in concreto esercitata, comportamenti conformi ad ogni altra norma interna aziendale che regoli in qualsiasi modo le attività rientranti nell'ambito di applicazione del Decreto.

I. 1 Principi generali di comportamento applicabili ai reati di cui all'art. 24 *bis*¹

Per quanto concerne i reati di cui all'art. 24 *bis* ("Delitti informatici e trattamento illecito di dati") del Decreto, l'esito delle attività di *risk assessment* svolte ha portato a ritenere concreta la possibilità di commissione degli stessi applicabile e rilevante in virtù dell'attività svolta dalla Società. Pertanto, per essi trovano applicazione i principi generali di comportamento di seguito descritti, nonché i principi generali di controllo descritti nella Parte Generale ed i principi generali di comportamento descritti nel Codice Etico di Gruppo.

A tutti coloro che operano per conto della Società è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di condotte:

- tali da integrare le fattispecie di reato sopra considerate (art. 24 *bis* del Decreto), ovvero tali da agevolarne la commissione;
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure aziendali o, comunque, non in linea con i principi espressi nel Modello e nel Codice Etico di Gruppo.

Nell'ambito dei suddetti comportamenti è fatto divieto, in particolare, di:

- utilizzare le risorse informatiche (es. *personal computer* fissi o portatili) assegnate dalla Società per finalità diverse da quelle lavorative;

¹ Si specifica che il decreto legge n. 105/2019, convertito con modificazioni in legge n. 133/2019, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, ha introdotto all'art. 24-bis, comma terzo, del D.Lgs. 231/2001, il reato di cui all'art. 1, comma undicesimo, del citato decreto-legge, rubricato "*Delitti in materia di perimetro di sicurezza cibernetica*". In prima istanza, ai sensi dell'art. 1, comma secondo, del decreto-legge n. 105/2019, la specifica individuazione dei soggetti rientranti nel perimetro di sicurezza nazionale cibernetica era stata demandata dal Legislatore ad un Decreto del Presidente del Consiglio dei Ministri (DPCM) (da emanarsi entro quattro mesi dalla data di entrata in vigore della legge di conversione). Successivamente, il c.d. Decreto "*Milleproroghe*" (Decreto Legge 30 dicembre 2019, n. 162, convertito con modificazioni in Legge n. 8, 28 febbraio 2020) ha, tra le altre disposizioni, modificato la precitata Legge n. 133/2019, introducendovi un nuovo comma 2 bis all'art. 1; con tale modifica, il Legislatore ha statuito che l'elencazione dei soggetti rientranti nel perimetro di sicurezza nazionale cibernetica, sarà invece contenuta in un atto amministrativo - adottato dal Presidente del Consiglio dei Ministri - entro trenta giorni dalla data di entrata in vigore del suddetto DPCM. Detto atto amministrativo, per il quale sarà escluso il diritto di accesso, non sarà soggetto a pubblicazione, fermo restando che a ciascun soggetto individuato sarà data, separatamente, comunicazione senza ritardo dell'avvenuta iscrizione nell'elenco. Inoltre, con il DPCM 30 luglio 2020, n. 131, è stato adottato il "*Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133*", pubblicato in Gazzetta Ufficiale Serie Generale n. 261 del 21.10.2020, che stabilisce i criteri secondo i quali le apposite Autorità dovranno provvedere ad identificare i soggetti da includere nel perimetro di sicurezza nazionale cibernetica e le modalità con cui questi dovranno assolvere agli obblighi previsti dalla norma. Alla data del presente aggiornamento del Modello, la Società non è ancora stata formalmente individuata, ai sensi dell'art. 5 del Regolamento, quale operatore tenuto al rispetto delle misure e degli obblighi previsti dalla norma. Qualora la Società venisse formalmente individuata come operatore tenuto al rispetto delle misure e degli obblighi previsti dalla norma, verrebbe avviata una specifica attività di *risk assessment* funzionale all'aggiornamento del presente Modello 231.

- alterare documenti elettronici con finalità probatoria;
- accedere, senza averne autorizzazione, ad un sistema informatico o telematico o trattenersi contro la volontà espressa o tacita di chi ha diritto di escluderlo (il divieto include sia l'accesso ai sistemi informativi interni che l'accesso ai sistemi informativi di enti concorrenti, pubblici o privati, allo scopo di ottenere informazioni su sviluppi commerciali o industriali);
- procurarsi, riprodurre, diffondere, comunicare, ovvero portare a conoscenza di terzi: codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico altrui protetto da misure di sicurezza, oppure fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui, protetto da misure di sicurezza;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- aggirare o tentare di aggirare i sistemi di sicurezza aziendali (es: *Antivirus*, *Firewall*, *Proxy server*, ecc.);
- lasciare il proprio *personal computer* incustodito e senza protezione *password* o alterare le configurazioni impostate;
- utilizzare strumenti, informazioni, dati e sistemi informatici e telematici in modo da recare danno a terzi, in particolare interrompendo il funzionamento di un sistema informatico o alterando dati o programmi informatici, anche a seguito dell'accesso abusivo, ovvero mediante l'intercettazione di comunicazioni;
- detenere o diffondere indebitamente codici o programmi atti al danneggiamento informatico o all'interruzione di un servizio telematico;
- installare apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche tra soggetti pubblici o privati;
- alterare, falsificare, cancellare o copiare dati, informazioni, documenti (anche aventi efficacia probatoria) e programmi di soggetti pubblici o privati;
- utilizzare *software* e/o *hardware* atti ad intercettare, falsificare, alterare o eliminare il contenuto di comunicazioni e/o documenti informatici;
- installare *software* / programmi aggiuntivi diversi da quelli esistenti o senza previa verifica ed autorizzazione;
- danneggiare informazioni, dati, programmi informatici e sistemi informatici o telematici utilizzati da soggetti pubblici o privati;
- accedere abusivamente al proprio sistema informatico o telematico al fine alterare e/o cancellare dati e/o informazioni;
- detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso al sistema informatico o telematico proprio o di terzi (pubblici o privati), protetto da misure di sicurezza, al fine di acquisire informazioni riservate;
- fornire indicazioni o istruzioni idonee a consentire ad un terzo di accedere ad un sistema informatico altrui protetto da misure di sicurezza;
- violare gli obblighi previsti dalla Legge per il rilascio di un certificato qualificato e di utilizzare indebitamente la firma elettronica;
- prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza preventiva autorizzazione;
- utilizzare *password* di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile della funzione competente

per la gestione dei sistemi informativi;

- trasferire all'esterno della Società e/o trasmettere *file*, documenti o qualsiasi altra documentazione riservata di proprietà della Società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione dei soggetti competenti.

Inoltre, vige l'obbligo di:

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività lavorativa;
- custodire accuratamente le proprie credenziali di accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- garantire la tracciabilità dei documenti prodotti;
- assicurare meccanismi di protezione dei file, quali, ad esempio, *password* da aggiornare periodicamente, secondo le regole contenute all'interno dei protocolli aziendali;
- utilizzare e conservare in modo corretto le firme digitali della Società, le *password* e le proprie credenziali d'accesso ai sistemi informativi della Società, evitando che terzi soggetti possano venirne a conoscenza;
- rispettare i protocolli aventi ad oggetto, tra gli altri:
 - la gestione della sicurezza informatica;
 - l'utilizzo e il malfunzionamento degli strumenti informatici / telematici e delle reti aziendali;
 - l'accesso, la protezione e il controllo dei sistemi informatici;
 - la gestione delle *password*, della posta elettronica;
- installare esclusivamente *software* originali, debitamente autorizzati o licenziati;
- prendere parte ai programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti dalla commissione dei reati previsti dall'articolo 24 *bis* del Decreto;
- adottare specifiche misure di protezione e mappatura dei documenti elettronici utilizzati per comunicazioni verso l'esterno.

I. 2 Principi generali di comportamento applicabili ai reati di cui all'art. 25 *bis* 1

Per quanto concerne i reati di cui all'art. 25 *bis* 1 (“*Delitti contro l'industria e il commercio*”) del Decreto, l'esito delle attività di *risk assessment* svolte ha portato a ritenere concreta la possibilità di commissione degli stessi applicabile e rilevante in virtù dell'attività svolta dalla Società. Pertanto, per essi trovano applicazione i principi generali di comportamento di seguito descritti, nonché i principi generali di controllo descritti nella Parte Generale ed i principi generali di comportamento descritti nel Codice Etico di Gruppo.

A tutti coloro che operano per conto della Società è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di condotte:

- tali da integrare, in maniera diretta o indiretta, le fattispecie di reato previste dall'art. 25 *bis* 1 del Decreto, ovvero tali da agevolare la commissione;
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle

sopra considerate, possano potenzialmente diventarlo;

- non conformi alle leggi, ai regolamenti vigenti, nonché ai protocolli aziendali o, comunque, non in linea con i principi espressi nel Modello e nel Codice Etico di Gruppo.

Nell'ambito dei suddetti comportamenti è fatto divieto, in particolare, di:

- attuare comportamenti violenti o intimidatori o condizionare le attività commerciali, industriali o produttive di terzi con forme di intimidazione tipiche della criminalità organizzata, al fine di ostacolare / eliminare la concorrenza;
- attuare accordi collusivi con altre imprese, finalizzati all'aggiudicazione di gare di appalto ai danni di altri concorrenti, ovvero scoraggiare i concorrenti a presentare offerte competitive;
- porre in essere atti di violenza sulle cose di terzi (es. danneggiare o trasformare beni di terzi / concorrenti);
- porre in essere atti fraudolenti idonei a produrre uno sviamento della clientela altrui e un danno per le imprese concorrenti;
- compiere atti di concorrenza sleale ed in particolare:
 - diffondere notizie e apprezzamenti sui prodotti e sull'attività di un concorrente, idonei a determinarne il discredito, o appropriarsi di pregi dei prodotti o dell'impresa di un concorrente;
 - avvalersi direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale ed idoneo a danneggiare l'altrui azienda;
 - porre in essere comportamenti finalizzati alla contraffazione di segni distintivi di opere dell'ingegno o di prodotti industriali;
 - consegnare all'acquirente un prodotto diverso per origine, provenienza, qualità o quantità rispetto a quello concordato;
 - utilizzare segreti aziendali altrui;
 - porre in essere atti fraudolenti idonei a produrre uno sviamento della clientela altrui e un danno per le imprese concorrenti;
 - riprodurre abusivamente, imitare o manomettere marchi, segni distintivi, brevetti, disegni industriali o modelli in titolarità di terzi;
 - fare uso, in ambito industriale e/o commerciale, di marchi, segni distintivi, brevetti, disegni industriali o modelli contraffatti da soggetti terzi;
 - introdurre nel territorio dello Stato per farne commercio, detenere per vendere o mettere in qualunque modo in circolazione prodotti industriali con marchi o segni distintivi contraffatti o alterati da soggetti terzi.

Inoltre, vige l'obbligo di:

- improntare tutte le attività e le operazioni svolte dalla Società al massimo rispetto delle leggi vigenti, nonché ai principi di correttezza, trasparenza, buona fede e tracciabilità della documentazione;
- assicurare la massima rispondenza tra i comportamenti effettivi e quelli richiesti dai protocolli aziendali ai fini della prevenzione dei delitti contro l'industria e il commercio;
- disporre regole sull'utilizzo di materiale protetto da privativa industriale;
- svolgere con la massima diligenza e accuratezza tutte le necessarie ricerche di anteriorità relative al marchio, brevetto, segno distintivo, disegno o modello che si intende utilizzare e/o mettere in commercio, al fine di verificare la sussistenza di eventuali diritti di privativa di terzi;

- ottenere dai rispettivi titolari e/o licenzianti dei relativi diritti di utilizzo sui marchi, brevetti, segni distintivi, disegni o modelli in questione, specifiche dichiarazioni volte ad attestare le seguenti principali circostanze:
 - di essere i legittimi titolari dei diritti di sfruttamento economico sui marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o comunque di aver ottenuto dai legittimi titolari l'autorizzazione alla loro concessione in uso a terzi;
 - di garantire che i marchi, brevetti, segni distintivi, disegni o modelli oggetto di cessione o di concessione in uso non violano alcun diritto di proprietà industriale in capo a terzi;
 - di impegnarsi a manlevare e tenere indenne la Società da qualsivoglia danno o pregiudizio, di natura patrimoniale e non, le potesse derivare, per effetto della non veridicità, inesattezza o incompletezza di tale dichiarazione;
- prendere parte ai programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti dalla commissione dei reati previsti dall'art. 25 *bis* 1 del Decreto.

I. 3 Principi generali di comportamento applicabili ai reati di cui all'art. 25 *quater*

Per quanto concerne i reati di cui all'art. 25 *quater* (“*Delitti con finalità di terrorismo o di eversione dell'ordine democratico*”) del Decreto, l'esito delle attività di *risk assessment* svolte ha portato a ritenere concreta la possibilità di commissione degli stessi applicabile e rilevante in virtù dell'attività svolta dalla Società. Pertanto, per essi trovano applicazione i principi generali di comportamento di seguito descritti, nonché i principi generali di controllo descritti nella Parte Generale ed i principi generali di comportamento descritti nel Codice Etico di Gruppo.

A tutti coloro che operano per conto della Società è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di condotte:

- tali da integrare le fattispecie di reato sopra considerate (art. 25 *quater* del Decreto), ovvero tali da agevolarne la commissione;
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure aziendali o, comunque, non in linea con i principi espressi nel Modello e nel Codice Etico di Gruppo;
- porre in essere comportamenti non conformi alle leggi e ai regolamenti vigenti in ogni contesto geografico ed ambito operativo, anche per quanto attiene la prevenzione dei reati in materia di terrorismo ed eversione dell'ordine democratico;
- instaurare rapporti (commesse, appalti, consulenze o qualsivoglia operazione commerciale e/o finanziaria) con soggetti, enti, società o associazioni in qualsiasi forma costituite, in Italia o all'estero - sia direttamente che per il tramite di interposta persona - che si sappia o si abbia ragione o sospetto di ritenere facciano parte o siano comunque legati o intrattengano rapporti di qualsiasi natura con associazioni o gruppi criminali (ad esempio inseriti nelle Liste di Riferimento definite da Banca d'Italia, ONU, UE, OFAC, ecc.), ovvero comunque dei quali non si sia accertata con accuratezza, diligenza ed in modo tracciabile e documentato l'identità, l'integrità e la correttezza, nonché, in caso di società, l'effettiva proprietà o i legami di

controllo;

- fornire, direttamente o indirettamente, fondi a favore di soggetti che intendono porre in essere uno o più delitti con finalità di terrorismo o di eversione dell'ordine democratico, ovvero a favore di soggetti che perseguono, direttamente o indirettamente, finalità di terrorismo o eversione dell'ordine democratico, agevolandoli nel perseguimento dei loro obiettivi criminosi attraverso la messa a disposizione di risorse finanziarie o comunque l'incremento delle loro disponibilità economiche. Rilevano, a tal fine, i fondi e le risorse economiche erogate a favore di un soggetto o di un gruppo nella consapevolezza - o quantomeno con il ragionevole sospetto - che:
 - persegua finalità di terrorismo o di eversione dell'ordine democratico;
 - il beneficiario dei fondi li destinerà a tali soggetti o gruppi;
 - le risorse finanziarie saranno utilizzate per commettere i delitti in oggetto;
- effettuare prestazioni in favore di terzi non direttamente correlate e corrispondenti a quanto contrattualmente pattuito con tali soggetti;
- effettuare pagamenti su conti cifrati o numerati o in denaro contante (salvo per importi modici) e in ogni caso a soggetti diversi dalla controparte contrattuale;
- effettuare pagamenti, nonché erogare liberalità o altre utilità, verso soggetti - persone fisiche o giuridiche - che siano iscritti nelle Liste stilate dalle organizzazioni internazionali (ad esempio, ONU, UE, OFAC, ecc.) al fine di prevenire il finanziamento del terrorismo;
- riconoscere compensi o provvigioni in favore di terzi che non trovino adeguata giustificazione o che non siano adeguatamente proporzionati all'attività svolta, anche in considerazione delle condizioni di mercato, del tipo di incarico da svolgere e delle prassi vigenti in ambito locale;
- assumere o assegnare commesse o effettuare qualsivoglia operazione che possa presentare carattere anomalo per tipologia o oggetto, ovvero che possa determinare l'instaurazione o il mantenimento di rapporti che presentino profili di anomalia dal punto di vista dell'affidabilità delle stesse e/o della reputazione delle controparti;
- utilizzare, anche occasionalmente, la Società o una sua funzione aziendale allo scopo di consentire o agevolare la commissione dei reati di cui alla presente Parte Speciale;
- assumere persone indicate nelle Liste di Riferimento o facenti parte di organizzazioni presenti nelle stesse;
- dare rifugio o fornire ospitalità, mezzi di trasporto, strumenti di comunicazione o ogni altro supporto a persone che partecipano ad associazioni eversive o con finalità di terrorismo.

Inoltre, vige l'obbligo di:

- assicurare la regolarità del ciclo passivo al fine di garantire che:
 - ogni pagamento sia effettuato tramite bonifico bancario, essendo vietato l'utilizzo di contanti o strumenti di pagamento analoghi, e in modo che ne sia garantita la tracciabilità (importo, nome / denominazione del destinatario, causale e numero di conto corrente);
 - il pagamento sia effettuato esclusivamente sul conto corrente indicato nel contratto o nella relativa documentazione contabile e a favore della controparte contrattuale, essendo esclusa la possibilità di effettuare pagamenti su conti cifrati, intestati a soggetti terzi, in un Paese terzo rispetto a quello delle parti contraenti o a quello di esecuzione del contratto o verso soggetti che siano iscritti nelle Liste stilate dalle organizzazioni internazionali (ad esempio, ONU, UE, OFAC, ecc.) al fine di prevenire il finanziamento del terrorismo ed il riciclaggio;
 - il pagamento corrisponda esattamente all'importo oggetto di pattuizione contrattuale;

- vi sia piena coincidenza tra destinatari / ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni;
- assicurare che pagamenti o rimborsi di spese, compensi, sconti, note di accredito o la riduzione in qualsiasi altra forma della somma dovuta in favore di soggetti interni o soggetti terzi alla Società avvengano solo qualora:
 - trovino adeguata giustificazione alla luce del rapporto contrattuale con essi costituito;
 - rappresentino il corrispettivo di beni, servizi, prestazioni, ecc. effettivamente ricevute dalla Società;
 - siano supportati da giustificativi ed idoneamente documentati;
- identificare l'attendibilità dei consulenti, fornitori, promotori e, più in generale, delle controparti terze (di seguito, congiuntamente, controparti), al fine di verificarne l'onorabilità e l'affidabilità, anche sotto il profilo della correttezza e tracciabilità delle transazioni economiche con gli stessi, evitando di instaurare o proseguire rapporti con soggetti che non presentino o mantengano nel tempo adeguati requisiti di trasparenza e correttezza;
- monitorare nel tempo il permanere in capo alle controparti dei requisiti di affidabilità, correttezza, professionalità e onorabilità;
- selezionare le controparti sulla base di criteri di trasparenza, di economicità e correttezza, garantendo la tracciabilità delle attività atte a comprovare i menzionati criteri;
- effettuare una attività di *due diligence* finalizzata all'accertamento della reputazione, onorabilità, affidabilità, professionalità, competenza ed esperienza delle controparti, nonché atta ad identificare eventuali condizioni di incompatibilità e conflitto di interessi o la sussistenza di condanne penali o sanzioni a carico delle stesse;
- accertare la località della sede o residenza della controparte, la quale non deve essere situata in Paesi a "regime fiscale privilegiato", salvo che si tratti di contratti da stipularsi con controparti residenti in tali Paesi e tali Paesi siano i medesimi in cui saranno svolte le prestazioni oggetto del contratto;
- determinare i requisiti minimi in possesso dei soggetti offerenti e fissare i criteri di valutazione delle offerte;
- identificare l'organo / unità responsabile dell'esecuzione dei contratti, con indicazione di compiti, ruoli e responsabilità.

I. 4 Principi generali di comportamento applicabili ai reati di cui all'art. 25 *quinquies*

Per quanto concerne i reati di cui all'art. 25 *quinquies* del Decreto ("*Delitti contro la personalità individuale*"), l'esito delle attività di *risk assessment* svolte ha portato a ritenere concreta la possibilità di commissione degli stessi applicabile e rilevante in virtù dell'attività svolta dalla Società. Pertanto, per essi trovano applicazione i principi generali di comportamento di seguito descritti, nonché i principi generali di controllo descritti nella Parte Generale ed i principi generali di comportamento descritti nel Codice Etico di Gruppo.

A tutti coloro che operano per conto della Società è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di condotte:

- tali da integrare le fattispecie di reato di cui all'art. 25 *quinquies*, anche nella forma del concorso

o del tentativo, ovvero tali da agevolare la commissione;

- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure aziendali o, comunque, non in linea con i principi espressi dal Modello e dal Codice Etico di Gruppo;

Nell'ambito dei suddetti comportamenti è fatto divieto, in particolare, di:

- considerare prevalente qualsiasi condizione economica rispetto alla tutela dei lavoratori ed alle normative vigenti in materia;
- utilizzare, assumere o impiegare manodopera, anche mediante società di lavoro interinale, sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno;
- corrispondere ai lavoratori retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o territoriali di riferimento o comunque sproporzionate rispetto alla quantità e qualità del lavoro prestato;
- violare volontariamente la normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie, ecc.;
- sottoporre i lavoratori a condizioni di lavoro, a metodi di sorveglianza o a situazioni alloggiative degradanti;
- utilizzare gli strumenti informatici aziendali al fine di procurarsi e detenere materiale pedopornografico;
- utilizzare, anche occasionalmente, la Società, un suo bene o una sua funzione aziendale allo scopo di consentire o agevolare la commissione di uno o più reati connessi alla tratta di persone o alla pedopornografia;
- fornire, direttamente o indirettamente, fondi a favore di soggetti che intendono porre in essere uno o più reati connessi alla tratta di persone o alla pedopornografia ovvero a favore di soggetti che perseguono, direttamente o in qualità di prestanome, tali finalità, agevolandoli nel perseguimento dei loro obiettivi criminosi attraverso la messa a disposizione di risorse finanziarie o comunque l'incremento delle loro disponibilità economiche. Ai fini che qui rilevano, vengono in considerazione i fondi e le risorse economiche erogate a favore di un soggetto o di un gruppo nella consapevolezza - o quantomeno con il ragionevole sospetto - che:
 - questo persegue finalità connesse alla tratta di persone o alla pedopornografia;
 - l'intermediario a cui sono destinati i fondi li destinerà a tali gruppi.

Inoltre, vige l'obbligo di:

- nel caso in cui si faccia ricorso al lavoro interinale mediante apposite agenzie, assicurarsi che tali agenzie non agiscano in violazione della normativa in materia di intermediazione illecita e sfruttamento del lavoro, richiedendo espressamente l'impegno al rispetto del Modello adottato dalla Società;
- assicurarsi, con apposite clausole contrattuali, che eventuali soggetti terzi con cui la Società collabora (fornitori, consulenti, ecc.) non agiscano in violazione della normativa in materia di intermediazione illecita e sfruttamento del lavoro, richiedendo espressamente l'impegno al rispetto del Modello adottato dalla Società.

I. 5 Principi generali di comportamento applicabili ai reati di cui all'art. 25 *novies*

Per quanto concerne i reati di cui all'art. 25 *novies* del Decreto (*"Delitti in violazione del diritto d'autore"*), l'esito delle attività di *risk assessment* svolte ha portato a ritenere concreta la possibilità di commissione degli stessi applicabile e rilevante in virtù dell'attività svolta dalla Società. Pertanto, per essi trovano applicazione i principi generali di comportamento di seguito descritti, nonché i principi generali di controllo descritti nella Parte Generale ed i principi generali di comportamento descritti nel Codice Etico di Gruppo.

A tutti coloro che operano per conto della Società è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di condotte:

- tali da integrare le fattispecie di reato di cui all'art. 25 *novies*, anche nella forma del concorso o del tentativo, ovvero tali da agevolarne la commissione;
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure aziendali o, comunque, non in linea con i principi espressi nel Modello e nel Codice Etico di Gruppo.

Nell'ambito dei suddetti comportamenti è fatto divieto, in particolare, di:

- effettuare *download* illegali o trasmettere a soggetti terzi contenuti protetti dal diritto d'autore;
- introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso;
- utilizzare, sfruttare, diffondere o riprodurre indebitamente a qualsiasi titolo, in qualsiasi forma, a scopo di lucro o a fini personali, opere dell'ingegno di qualsiasi natura coperte dal diritto d'autore.

Inoltre, vige l'obbligo di:

- utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste;
- utilizzare unicamente materiale pubblicitario (es. materiale fotografico) autorizzato;
- rispettare i protocolli aziendali, nonché le clausole e gli strumenti previsti nei contratti, finalizzati alla tutela del materiale protetto da diritto d'autore;
- assicurare il controllo della corrispondenza alla normativa del materiale promozionale / pubblicitario presentato all'esterno;
- prendere parte ai programmi di formazione, informazione e sensibilizzazione rivolti al personale al fine di diffondere una chiara consapevolezza sui rischi derivanti dalla commissione dei reati previsti dall'articolo 25 *novies* del Decreto;
- adottare specifiche misure di protezione volte a garantire l'integrità delle informazioni messe a disposizione del pubblico tramite la rete *internet* e dei programmi e delle altre opere d'ingegno coperte dal diritto d'autore;
- adottare specifiche misure a garanzia del corretto utilizzo dei materiali coperti da diritti d'autore, anche attraverso procedure di controllo della installazione di *software* sui sistemi

operativi;

- adottare strumenti di protezione (quali, ad esempio, diritti di accesso) relativi alla conservazione e all'archiviazione di contenuti protetti dal diritto d'autore.

I. 6 Principi generali di comportamento applicabili ai reati di cui all'art. 25 *duodecies*

Per quanto concerne i reati di cui all'art. 25 *duodecies* del Decreto (*"Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare"*), l'esito delle attività di *risk assessment* svolte ha portato a ritenere concreta la possibilità di commissione degli stessi applicabile e rilevante in virtù dell'attività svolta dalla Società. Pertanto, per essi trovano applicazione i principi generali di comportamento di seguito descritti, nonché i principi generali di controllo descritti nella Parte Generale ed i principi generali di comportamento descritti nel Codice Etico di Gruppo.

A tutti coloro che operano per conto della Società è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di condotte:

- tali da integrare le fattispecie di reato di cui all'art. 25 *duodecies*, anche nella forma del concorso o del tentativo, ovvero tali da agevolarne la commissione;
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure aziendali o, comunque, non in linea con i principi espressi dal Modello e dal Codice Etico di Gruppo.

Nell'ambito dei suddetti comportamenti è fatto divieto, in particolare, di:

- considerare prevalente qualsiasi condizione economica rispetto alla tutela dei lavoratori ed alle normative vigenti in materia;
- omettere di segnalare carenze o irregolarità nella documentazione ricevuta dai potenziali candidati, ovvero dai dipendenti;
- effettuare il trasporto di stranieri nel territorio dello Stato Italiano;
- compiere altri atti diretti a procurarne illegalmente l'ingresso di stranieri nel territorio dello Stato Italiano o di altro Stato.

Inoltre, vige l'obbligo di:

- rispettare le procedure aziendali in materia di selezione, assunzione e amministrazione del personale;
- rispettare la normativa di riferimento per l'assunzione di personale extra-comunitario;
- monitorare periodicamente la regolarità amministrativa dei permessi di soggiorno degli eventuali lavoratori extra-comunitari;
- rendere tracciabile, in ogni sua fase, il processo di selezione dei profili ricercati e di assunzione del personale;
- nel caso in cui si faccia ricorso al lavoro interinale mediante apposite agenzie, assicurarsi che tali agenzie si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno, richiedendo espressamente l'impegno al rispetto del Modello adottato dalla Società;
- archiviare debitamente la documentazione relativa al personale della Società;

- rispettare le procedure aziendali in materia di qualificazione e monitoraggio dei fornitori utilizzati;
- assicurarsi, con apposite clausole contrattuali, che eventuali soggetti terzi con cui la Società collabora (fornitori, consulenti, ecc.) si avvalgano di lavoratori in regola con la normativa in materia di permesso di soggiorno, richiedendo espressamente l'impegno al rispetto del Modello adottato della Società;
- prevedere, nei contratti di somministrazione dei lavoratori, di appalto e di subappalto, clausole contrattuali che impegnino la controparte al rispetto delle disposizioni in materia di immigrazione e regolarità del soggiorno di cittadini di Paesi extracomunitari;
- garantire la regolare tenuta ed aggiornamento dell'anagrafica fornitori, procedendo dapprima alla loro qualifica;
- verificare, preliminarmente alla sottoscrizione di contratti con terze parti, che queste abbiano adempiuto al versamento degli oneri previdenziali dovuti, mediante richiesta del Documento Unico di Regolarità Retributiva (DURC);
- segnalare eventuali situazioni di criticità di cui si venga a conoscenza nel corso del rapporto contrattuale con terze parti in merito alla tutela dei lavoratori ed alle normative vigenti in materia, ai fini dell'aggiornamento della *blacklist* di Gruppo.

I. 7 Principi generali di comportamento applicabili ai reati di cui all'art. 25 *sexiesdecies*

Per quanto concerne i reati di cui all'art. 25 *sexiesdecies* del Decreto, considerando i rapporti di ciclo passivo intrattenuti dalla Società con i fornitori di merci, siccome emersi e rappresentati all'esito delle attività di *risk assessment*, la loro rilevanza / applicabilità è stata valutata marginale.

Nonostante ciò, in ottica prudenziale, la Società ha ritenuto opportuno tenerne ugualmente traccia nelle aree a rischio reato in linea teorica impattate ("Approvvigionamento di beni, lavori e servizi" e "Gestione dei rapporti con la Pubblica Amministrazione e con le Autorità di Vigilanza").

Ad oggi, infatti, MIL (i) non importa merce acquistata da fornitori residenti in Paesi non aderenti all'Unione Doganale Europea; (ii) conseguentemente, non è soggetta al versamento dei dazi doganali; (iii) in conclusione, non è tenuta a intrattenere rapporti con le Autorità Doganali competenti.

Tanto premesso, per essi trovano dunque applicazione i principi generali di comportamento di seguito descritti, nonché i principi generali di controllo descritti nella Parte Generale ed i principi generali di comportamento descritti nel Codice Etico.

A tutti coloro che operano per conto della Società è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di condotte tali da:

- tali da integrare le fattispecie di reato sopra considerate, anche nella forma del concorso o del tentativo, ovvero tali da agevolarne la commissione;
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;

- non conformi alle leggi, ai regolamenti vigenti, nonché alle procedure aziendali o, comunque, non in linea con i principi espressi nel Modello e nel Codice Etico di Gruppo.

Inoltre, vige l'obbligo di:

- monitorare costantemente l'evoluzione del quadro normativo di riferimento, al fine di garantire l'adeguamento dell'operatività aziendale alle novità normative in materia di adempimenti doganali;
- assicurare la correttezza e trasparenza nei rapporti con le Autorità doganali;
- assicurare che l'ingresso nel territorio dell'Unione Doganale delle merci soggette a diritti di confine avvenga sempre mediante la loro presentazione all'ufficio doganale competente;
- assicurare che, in tutti gli altri casi in cui le merci sono ammesse nel territorio doganale in sospensione di imposta, siano svincolate da tale regime nel rispetto delle formalità prescritte dalla normativa applicabile;
- assicurare, conseguentemente, il pagamento dei diritti di confine dovuti;
- nell'eventualità di coinvolgimento di soggetti esterni per la gestione delle pratiche doganali, prevedere nei relativi contratti specifiche clausole che impegnino contrattualmente i consulenti al rispetto della normativa doganale, oltre che alla correttezza e trasparenza nei rapporti con le Autorità e all'obbligo di rendicontazione delle attività svolte;
- nell'eventualità di coinvolgimento di soggetti esterni per la gestione delle pratiche doganali, prevedere il monitoraggio delle attività svolte da tali soggetti, al fine di assicurare completezza e accuratezza dei documenti necessari all'importazione delle merci soggette a diritti di confine.

Si ritengono infine integralmente richiamati i principi generali di comportamento presenti nella Parte Speciale A "Reati contro la Pubblica Amministrazione".

I. 8 Principi generali di comportamento descritti dal Codice Etico di Gruppo

Per quanto riguarda le fattispecie di reato che presentano una non significativa probabilità di commissione (ovvero, i reati indicati negli artt. 25 *bis*, 25 *quater* 1, 25 *sexies*, 25 *terdecies* e 25 *quaterdecies*) trovano applicazione, oltre ai principi generali di controllo descritti nella Parte Generale, i principi generali di comportamento descritti nel Codice Etico di Gruppo. Il contenuto del Codice Etico di Gruppo si fonda sui valori propri del patrimonio culturale dell'azienda e si ispira ai principi etici dettati dall'evoluzione del mercato e del contesto sociale in cui il Gruppo FS Italiane opera. Tutti i Destinatari del Codice (ovvero, gli Organi Sociali di MIL, il *management*, il personale e tutti coloro che, direttamente o indirettamente, stabilmente o temporaneamente, instaurino con MIL rapporti e relazioni) devono avere piena conoscenza delle norme contenute nel Codice e, conseguentemente, conformare ogni azione e comportamento ai valori e ai contenuti in esso espressi.