HUAWEI TECHNOLOGIES ITALIA S.R.L.

Modello di organizzazione, gestione e controllo ai sensi del d.lgs. 231/2001

PARTE GENERALE

Approvato con delibera del Consiglio di Amministrazione del 9 Novembre 2014

INDICE

Premessa

Il Decreto Legislativo 8 giugno 2001, n. 231[1], recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica*" (di seguito, il "**Decreto**" o "**d.lgs. 231/2001**"), ha introdotto nel nostro sistema giuridico la responsabilità da reato anche per gli enti[2].

Tale estensione di responsabilità mira a coinvolgere nella punizione di alcuni illeciti penali il patrimonio degli enti e, quindi, gli interessi economici dei soci, i quali, sino all'entrata in vigore della legge in esame, non subivano conseguenze in caso di commissione di reati a vantaggio della società da parte di amministratori e/o dipendenti. Infatti, il principio di personalità della responsabilità penale faceva sì che i soci rimanessero indenni da profili di responsabilità penale, essendo semplicemente tenuti, ove ne ricorressero i presupposti, al risarcimento dei danni ed alla responsabilità civile *ex* articoli 196 e 197 c.p. in caso di insolvenza del reo.

L'innovazione normativa, quindi, comporta conseguenze di grande rilievo; dall'entrata in vigore della legge, infatti, la persona giuridica e i soci della stessa non potranno più considerarsi estranei ai reati commessi da amministratori e/o dipendenti, ed avranno quindi tutto l'interesse ad implementare un sistema di controllo e monitoraggio sugli stessi, tale da escludere o limitare la responsabilità penale della società[3].

In particolare, ai sensi del Decreto l'ente può essere chiamato a rispondere nel caso di commissione, o tentata commissione, di un reato da parte di una o più persone fisiche qualificate, ove tale reato risulti commesso nell'interesse dell'ente o a suo vantaggio.

In particolare, il reato deve essere stato commesso da determinati soggetti che abbiano con l'ente un rapporto funzionale e, precisamente, da coloro che si trovino:

– in posizione apicale rispetto alla struttura dell'ente, cioè al vertice del medesimo; ovvero

– in posizione di sottoposti a tali soggetti.

---

[1] Tale decreto, emanato sulla base della legge delega n. 300/2000, mira ad adeguare la legislazione interna ad alcune Convenzioni internazionali cui l'Italia ha da tempo aderito, quali:
- la Convenzione di Bruxelles del 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità europee,
- la Convenzione, anch'essa firmata a Bruxelles il 26 maggio 1997, sulla lotta alla corruzione nella quale siano coinvolti i funzionari delle Comunità europee o degli Stati membri, e
- la Convenzione OCSE del 17 dicembre 1997, sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche ed internazionali.

[2] Sotto il profilo dei soggetti cui la nuova normativa è applicabile, il Decreto individua i soggetti, con l'ampia definizione di "enti", destinatari della normativa, come segue:
- gli enti forniti di personalità giuridica;
- le società;
- le associazioni, anche sfornite di personalità giuridica;

mentre espressamente esclude:
- lo Stato;
- gli enti pubblici territoriali;
- gli enti che svolgono funzioni di rilievo costituzionale.

[3] Con riferimento alla natura della responsabilità amministrativa *ex* d.lgs. 231/2001, la Relazione illustrativa al decreto sottolinea la "*nascita di un tertium genus che coniuga i tratti essenziali del sistema penale e di quello amministrativo nel tentativo di contemperare le ragioni dell'efficacia preventiva con quelle, ancor più ineludibili, della massima garanzia"*.
Il d.lgs. 231/2001 ha, infatti, introdotto nel nostro ordinamento una forma di responsabilità delle società di tipo "amministrativo" – in ossequio al dettato dell'art. 27 della nostra Costituzione che sancisce il principio fondamentale secondo il quale "*La responsabilità penale è personale*" – ma con numerosi punti di contatto con una responsabilità di tipo "penale".
In tal senso si vedano – tra i più significativi – gli artt. 2, 8 e 34 del d.lgs. 231/2001 ove il primo riafferma il principio di legalità tipico del diritto penale; il secondo afferma l'autonomia della responsabilità dell'ente rispetto all'accertamento della responsabilità della persona fisica autrice della condotta criminosa; il terzo prevede la circostanza che tale responsabilità, dipendente dalla commissione di un reato, venga accertata nell'ambito di un procedimento penale e sia, pertanto, assistita dalle garanzie proprie del processo penale. Si consideri, inoltre, il carattere afflittivo delle sanzioni applicabili alla società.

Poiché l'obiettivo della norma è non solo punire ma anche prevenire la commissione di reati, il legislatore ha stabilito in alcune ipotesi una esimente generale, in altre una riduzione di pena, in caso di adozione di un idoneo sistema di prevenzione da parte dell'ente.

In particolare, l'articolo 6 del Decreto prevede una forma specifica di esenzione da responsabilità qualora l'ente, in caso di reato commesso da un soggetto in posizione apicale, dimostri di aver adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi.

Si ha esclusione della responsabilità ove le predette condizioni ricorrano, nel loro complesso, al momento della commissione del reato o illecito; tuttavia anche l'adozione e l'attuazione del "modello" avvenute in un momento successivo alla commissione del reato o illecito svolgono comunque effetti positivi in ordine alle sanzioni irrogabili all'ente (artt. 12 e 17 del Decreto).

Per maggiori dettagli sulla normativa di cui al Decreto si rinvia a quanto illustrato nell'**Appendice I** al presente documento.

CAPITOLO 1
ELEMENTI DEL MODELLO DI GOVERNANCE E DELL'ASSETTO ORGANIZZATIVO GENERALE DI HUAWEI TECHNOLOGIES ITALIA S.R.L.

1.1 Huawei Technologies Italia S.r.l.

1.1.1 Identità

Huawei Technologies Italia S.r.l. (di seguito anche "**Huawei**" o la "**Società**") è attiva nella fornitura di soluzioni ICT, nonché nella costruzione di reti di comunicazione elettronica per committenti nel settore pubblico e privato.

In particolare, la Società ha per oggetto le seguenti attività:

- la produzione, l'importazione, l'esportazione, l'acquisto e la vendita di sistemi di telecomunicazioni, di apparecchiature per la comunicazione e trasmissione di dati, di tecniche di sviluppo e di implementazione di sistemi ("*system integration*") di computer ed apparecchiature accessorie, nonché ogni altra apparecchiatura di telecomunicazione e di trasmissione dati, inclusi il software associato, la manutenzione, la consulenza tecnica e servizi accessori di assistenza;
- l'installazione, il collaudo e la manutenzione di ogni tipo di sistema e di apparecchiatura di telecomunicazione e di trasmissione dati nonché di beni e servizi correlati;
- l'istituzione di centri di ricerca per lo sviluppo di software e hardware;
- l'istituzione e gestione di centri per la formazione inerente il prodotto e di centri di assistenza per la manutenzione del prodotto;
- la partecipazione a "*joint ventures*" o ad altri raggruppamenti di aziende, la costituzione o l'acquisto di società o rami d'azienda per l'esecuzione di progetti nell'ambito delle telecomunicazioni.

In generale, la Società può compiere tutte le operazioni commerciali, immobiliari e finanziarie così come qualsiasi altra operazione su beni mobili o immobili che siano connesse direttamente o indirettamente, in tutto o in parte, con l'oggetto sociale di cui sopra, ovvero con altro fine simile o connesso allo stesso che possa facilitare l'espansione e lo sviluppo della Società, fermo restando che le attività finanziarie saranno svolte solamente in via collaterale o accessoria all'attività principale e comunque non nei confronti del pubblico.

La sede legale della Società è situata a Milano, ulteriori sedi operative sono presenti rispettivamente nelle città di Roma e di Torino.

La Società attualmente si avvale dell'operato di circa 400 lavoratori dipendenti, oltre a 150 unità distaccate presso la Società da altre società del gruppo cui appartiene la Società.

Huawei è interamente partecipata dalla società Huawei Technologies Cooperatief U.A.

1.1.2 Governo societario

Huawei ha adottato il sistema di *governance* tradizionale costituito da un Consiglio di Amministrazione e un Collegio Sindacale.

Ai sensi dello Statuto, la Società è amministrata da una Consiglio di Amministrazione, che dura in carica per il periodo fissato dalla deliberazione assembleare di nomina ovvero fino a dimissioni o revoca da parte dell'Assemblea degli amministratori, salve le cause di cessazione e di decadenza previste dalla legge e dallo Statuto. Possono essere nominati amministratori anche non soci.

Il Consiglio di Amministrazione può essere composto da un numero di amministratori variabile da due a sette, a discrezione dell'Assemblea.

Gli Amministratori sono rieleggibili.

La cessazione degli amministratori per scadenza del termine ha effetto dal momento in cui il nuovo organo amministrativo è stato ricostituito.

Il Consiglio, qualora non vi abbia provveduto l'Assemblea in sede di nomina del Consiglio stesso, deve designare tra i suoi membri un Presidente, e può nominare uno o più amministratori delegati.

Il Consiglio si riunisce presso la sede sociale o anche altrove, purché in un paese dell'Unione Europea, in Svizzera, nella Repubblica Popolare Cinese o in Hong Kong, ogni volta che il Presidente lo ritenga necessario, nonché quando ne venga fatta richiesta da almeno un terzo degli amministratori in carica.

Il Presidente convoca il Consiglio di Amministrazione, ne fissa l'ordine del giorno, ne coordina i lavori e provvede affinché tutti gli amministratori siano adeguatamente informati sulle materie da trattare.

La convocazione avviene mediante avviso spedito a tutti gli amministratori, sindaci effettivi e revisore, se nominati, tramite lettera raccomandata o fax o con qualsiasi altro mezzo idoneo ad assicurare la prova dell'avvenuto ricevimento, almeno 3 (tre) giorni prima dell'adunanza e, in caso di urgenza, almeno (un) giorno prima. Nell'avviso vengono fissati la data, il luogo e l'ora della riunione, nonché l'ordine del giorno.

Per la validità delle deliberazioni del Consiglio di Amministrazione sono necessari la presenza della maggioranza degli amministratori e il voto favorevole della maggioranza dei presenti. In caso di parità di voti, la proposta si intende respinta.

Anche senza convocazione formale, le adunanze del Consiglio di Amministrazione e le sue deliberazioni saranno valide quando intervengono tutti gli amministratori in carica ed i sindaci effettivi se nominati.

Le riunioni del Consiglio di Amministrazione si possono svolgere anche per audioconferenza o videoconferenza, alle seguenti condizioni di cui si darà atto nei relativi verbali: che siano presenti nello stesso luogo il Presidente ed il segretario della riunione, che provvederanno alla formazione e sottoscrizione del verbale, dovendosi ritenere svolta la riunione in detto luogo; che sia consentito al Presidente della riunione di accertare l'identità degli intervenuti, regolare lo svolgimento della riunione, constatare e proclamare i risultati della votazione; che sia consentito al soggetto verbalizzante di percepire adeguatamente gli eventi della riunione oggetto di verbalizzazione; che sia consentito agli intervenuti di partecipare alla discussione ed alla votazione simultanea sugli argomenti all'ordine del giorno, nonché di visionare, ricevere o trasmettere documenti.

Le decisioni del Consiglio di Amministrazione possono essere adottate mediante consultazione scritta: in tal caso dai documenti sottoscritti dagli amministratori devono risultare con chiarezza l'argomento oggetto della decisione ed il consenso alla stessa. Le procedure per la consultazione scritta sono previste dall’art. 20 dello Statuto.

L’organo amministrativo è investito dei più ampi poteri per la gestione ordinaria e straordinaria della Società, con facoltà di compiere tutti gli atti ritenuti opportuni per il conseguimento dell'oggetto Sociale, esclusi soltanto quelli riservati all'Assemblea dalla legge e dallo Statuto.

Il Presidente del Consiglio di Amministrazione, previa delibera consiliare, o i singoli amministratori, nell'ambito dei propri poteri, hanno pure la facoltà di nominare procuratori *ad negotia* per determinati atti o categorie di atti, determinandone i poteri.

Il potere di rappresentare la Società è esercitato dal Presidente del Consiglio di Amministrazione, senza limite alcuno.

In caso di nomina di amministratori delegati, essi esercitano la rappresentanza della Società nei limiti dei loro poteri di gestione.

La rappresentanza della Società spetta anche ai direttori, agli institori e ai procuratori, nei limiti dei poteri loro conferiti nell'atto di nomina.

I soci possono nominare un Collegio Sindacale o un revisore contabile, anche società di revisione.

Il Collegio Sindacale è composto da tre sindaci effettivi e due supplenti.

Il Collegio Sindacale esercita il controllo contabile, salvo che con decisione dei soci venga nominato un revisore contabile.

Le riunioni del Collegio Sindacale possono svolgersi con intervenuti dislocati in più luoghi mediante l'utilizzo di mezzi di telecomunicazione, secondo le modalità indicate dallo Statuto per il Consiglio di Amministrazione.

1.1.3 Assetto organizzativo

Attualmente la Società è amministrata da un Consiglio di Amministrazione composto da 3 componenti ed è dotata di un Collegio Sindacale composto da 3 sindaci effettivi e 2 supplenti.

Il consiglio di amministrazione è composto come segue:

(i) Xu Wenwei – Presidente del Consiglio di Amministrazione

(ii) Meng Wanzhou – consigliere

(iii) Yu Chengdong – consigliere.

Il controllo contabile è affidato alla società di revisione legale KPMG S.p.A.

Al fine di rendere chiaro il ruolo e le responsabilità di ciascuno nell'ambito del processo decisionale aziendale, la Società ha messo a punto un prospetto sintetico nel quale è schematizzato il proprio assetto organizzativo (c.d. organigramma).

Nell'organigramma sono specificate:

- le aree in cui si suddivide l'attività aziendale;
- le linee di dipendenza gerarchica delle singole unità aziendali;
- il titolo della posizione dei soggetti che operano nelle singole aree.

Le funzioni affidate a ciascun ruolo sono formalizzate in apposite *job descriptions*.

L'organigramma e le *job descriptions* sono costantemente verificati e aggiornati a cura della funzione HR.

L'organigramma è diffuso all'interno della Società (a mezzo intranet e comunicazione individuale) a cura della funzione HR.

L'attuale organigramma della Società è allegato alla presente Parte Generale, unitamente a copia delle deleghe consiliari attribuite ai suoi componenti (**Allegato 1**).

1.1.4 Assetto organizzativo in materia di salute e sicurezza sul lavoro e ambiente

La Società ha altresì definito un organigramma in materia di salute e sicurezza sul lavoro e ambiente (di seguito, "HSE").

In particolare, la Società si è dotata di una propria struttura organizzativa con specifici compiti e responsabilità in materia HSE, definiti formalmente in coerenza con lo schema organizzativo e funzionale dell'azienda, a partire dal datore di lavoro (così come definito

dall'art. 2, comma 1, lett. b) del d.lgs. 81/2008) sino al singolo lavoratore, con particolare riguardo alle figure specifiche operanti in tale ambito (RSPP - Responsabile del Servizio di Prevenzione e Protezione, MC - Medico Competente, RLS - Rappresentante dei lavoratore per la sicurezza, preposti, Responsabile Ambiente e Sicurezza).

In questo modo, la Società ha previsto una propria articolazione di funzioni atta ad assicurare la salvaguardia degli interessi protetti per il tramite della cooperazione di più soggetti che - sulla base della valorizzazione delle necessarie competenze differenziate - si dividono il lavoro ripartendosi i compiti, ai sensi di quanto viene puntualmente richiesto dal comma 3 dell'art. 30 del d.lgs. 81/2008 in materia di salute e sicurezza sul lavoro.

L'attuale assetto organizzativo della Società in materia HSE è strutturato secondo lo schema dell'organigramma allegato alla presente Parte Generale (**Allegato 2**). Tale organigramma è costantemente verificato ed aggiornato a cura della funzione HR.

CAPITOLO 2
IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI HUAWEI TECHNOLOGIES ITALIA S.R.L.

Il presente documento, in attuazione degli artt. 6 e 7 del Decreto, disciplina il modello di organizzazione, gestione e controllo di Huawei, finalizzato ad evitare la commissione di reati di cui al Decreto e leggi collegate da parte dei suoi soggetti apicali e sottoposti (di seguito, per brevità, il "**Modello**").

L'adozione del Modello, oltre a rappresentare un motivo di esenzione dalla responsabilità della Società con riferimento alla commissione di alcune tipologie di reato, è un atto di responsabilità sociale di Huawei, da cui scaturiscono benefici per una molteplicità di soggetti: soci, manager, dipendenti, creditori e tutti gli altri soggetti i cui interessi sono legati alla vita dell'impresa.

La presenza di un sistema di controllo dell'agire imprenditoriale, unitamente alla fissazione e divulgazione di principi etici, migliorando gli standard di comportamento adottati dalla Società, aumentano infatti la fiducia e l'ottima reputazione di cui la stessa gode nei confronti dei soggetti terzi e, soprattutto, assolvono una funzione normativa in quanto regolano comportamenti e decisioni di coloro che quotidianamente sono chiamati ad operare in favore della Società, in conformità ai suddetti principi etici e standard di comportamento.

In tale contesto, Huawei ha, quindi, inteso avviare una serie di attività volte a rendere il proprio modello organizzativo conforme ai requisiti previsti dal Decreto e coerente con il contesto normativo e regolamentare di riferimento, con i principi già radicati nella propria cultura di *governance* e con le indicazioni contenute nelle linee guida di categoria emanate dalle associazioni maggiormente rappresentative.

Inoltre, Huawei ha adottato tutta una serie di regole volte a disciplinare il proprio operato e di principi cui deve uniformarsi l'agire di tutti coloro che operano nel suo interesse. Gli stessi sono contenuti, tra l'altro, all'interno del Business Code of Conduct.

Con particolare riferimento ai reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 25-*septies* d.lgs. 231/2001) e ai reati ambientali (art. 25-*undecies* d.lgs. 231/2001), la Società si è dotata di un sistema integrato di gestione della salute e sicurezza sul lavoro e ambientale ("Sistema di Gestione HSE") con riferimento alle sedi operative di Roma e Milano, corredati da specifiche procedure e certificato in conformità:

- al British Standard OHSAS 18001:2007 ("*Occupational Health & Safety Management System*"), in linea con le indicazioni date dall'art. 30 del d.lgs. 81/2008[4];
- alla norma ISO 14001 ("*Environmental Management System*").

In particolare, lo standard OHSAS stabilisce quali sono i criteri per un sistema di gestione della salute e sicurezza sul lavoro al fine di consentire all'organizzazione aziendale di controllare i propri rischi di igiene e sicurezza e migliorare le proprie prestazioni (*OHSAS specification "give requirements for an occupational health and safety – OH&S – management system, to enable an organization to control its OH&S risks an improve its performances"*).

[4] Si rileva, infatti, che l'art. 30 del d.lgs. 81/2008 delinea un contenuto minimo dei modelli organizzativi ritenuti idonei a prevenire i reati in materia di tutela della salute e sicurezza sul lavoro e al comma 5 stabilisce che: "*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 (SGSL) 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 (...)*". Si veda in proposito quanto ulteriormente precisato nel paragrafo 1.8 dell'Appendice I.

La norma ISO 14001 rappresenta invece lo standard internazionale di riferimento per l'implementazione di un sistema di gestione ambientale e la sua successiva certificazione nel caso questo risponda ai requisiti richiesti.

Il Sistema di Gestione HSE è parte del sistema di gestione generale della Società – comprensivo della struttura organizzativa, delle procedure, dei ruoli e delle responsabilità assegnati alle competenti funzioni aziendali – che, nel rispetto delle vigenti normative sulla salute e sicurezza sul lavoro e della normativa ambientale applicabile alla Società, si prefigge il miglioramento dei livelli di sicurezza aziendali e di tutti gli aspetti ambientali legati alle attività industriali, garantendo il raggiungimento degli obiettivi che la Società si è data.

Inoltre, per quanto concerne i delitti informatici (art. 25-*bis*), la Società si è dotata di un sistema di gestione della sicurezza delle informazioni (ISMS) certificato ISO/IEC 27001:2005 relativo alle sedi operative di Roma e Milano, corredato da un set di procedure specifiche.

Lo standard ISO 27001 fornisce i requisiti per adottare un ISMS finalizzato ad una corretta gestione dei dati sensibili delle società. Tali requisiti sono generalmente utilizzati nella prassi applicativa relativa ai modelli organizzativi *ex* d.lgs. 231/2001 per la definizione dei presidi volti alla prevenzione dei delitti informatici richiamati dall'art. 24-*bis* del d.lgs. 231/2001.

Per il tramite dei sistemi di gestione sopra citati, Huawei è in grado di assicurare, attraverso la predisposizione delle apposite procedure, la conformità dei propri comportamenti agli obblighi giuridici posti dalla legislazione vigente nonché agli standard di controllo della migliore prassi internazionale, tracciandone, con apposita registrazione, l'avvenuta effettuazione.

Si rileva, infine, che l'attuale perimetro certificato nell'ambito dei sistemi di gestione in oggetto, rappresentato dalle sedi operative di Roma e Milano, è stato definito sulla base delle caratteristiche delle attività aziendali e delle relative modalità di svolgimento. I soggetti deputati al mantenimento e all'aggiornamento di tali sistemi (i.e. il datore di lavoro e l'RSPP, il responsabile ambientale, il Quality Manager) valutano periodicamente, con il supporto dell'organismo di vigilanza indicato nel Capitolo 3 della presente Parte Generale del Modello, la correttezza dell'attuale perimetro certificato.

2.1 Metodologia seguita per la predisposizione del Modello

In particolare, il processo di attività funzionali allo studio, elaborazione e redazione, da parte di Huawei, del proprio Modello è stato strutturato in quattro fasi:

- fase 1: identificazione delle aree di rischio;
- fase 2: rilevazione della situazione esistente (*as-is*);
- fase 3: *gap analysis* e piano di azione (*action plan*);
- fase 4: disegno del modello di organizzazione, gestione e controllo.

Qui di seguito sono sinteticamente descritti gli obiettivi e le attività svolte nel corso di ciascuna fase.

2.1.1 Identificazione delle aree di rischio

L'art. 6, comma 2, lett. a) del Decreto indica, tra i requisiti del modello, l'individuazione dei processi e delle attività nel cui ambito possono essere commessi i reati rilevanti ai fini della responsabilità amministrativa degli enti. Si tratta, in altri termini, di quelle attività e processi aziendali che comunemente vengono definiti "sensibili" (c.d. "*aree di rischio*").

In questo contesto si collocano gli obiettivi della fase 1, che sono:

- l'identificazione degli ambiti aziendali oggetto dell'intervento e l'individuazione preliminare dei processi e delle attività sensibili e strumentali ai reati contro la Pubblica Amministrazione richiamati dagli artt. 24 e 25 del d.lgs. 231/2001, ai reati societari richiamati dall'art. 25-*ter* del d.lgs. 231/2001, ai delitti informatici richiamati dall'art. 24-*bis* del d.lgs. 231/2002, ai reati in materia di tutela della salute e sicurezza sul lavoro richiamati dall'art. 25-*septies* del d.lgs. 231/2001 e ai reati ambientali richiamati dall'art. 25-*undecies* del d.lgs. 231/2001 (di seguito, congiuntamente, "Reati-Presupposto"), nonché
- l'identificazione dei responsabili dei processi/attività sensibili, ovvero le risorse con una conoscenza approfondita dei processi/attività sensibili e dei meccanismi di controllo attualmente in essere (di seguito, "*key officers*").

Propedeutica all'individuazione delle attività sensibili è stata l'analisi della documentazione relativa alla struttura societaria ed organizzativa di Huawei svolta al fine di meglio comprendere l'attività della Società e di identificare gli ambiti aziendali oggetto dell'intervento.

La raccolta della documentazione rilevante e l'analisi della stessa da un punto di vista sia tecnico-organizzativo sia legale ha permesso l'individuazione dei processi/attività sensibili e una preliminare identificazione delle funzioni responsabili di tali processi/attività.

2.1.2 Rilevazione della situazione esistente (as-is)

Obiettivo della fase 2 è stata l'effettuazione dell'analisi e della valutazione, attraverso le interviste ai *key officers*, delle attività sensibili precedentemente individuate, con particolare enfasi sui controlli.

Nello specifico, per ogni processo/attività sensibile individuato nella fase 1, sono state analizzate le sue fasi principali, le funzioni e i ruoli/responsabilità dei soggetti interni ed esterni coinvolti nonché gli elementi di controllo esistenti, al fine di verificare in quali aree/settori di attività e secondo quali modalità si potessero astrattamente commettere i Reati-Presupposto.

L'analisi è stata compiuta attraverso interviste personali con i *key officers* che hanno avuto anche lo scopo di stabilire per ogni attività sensibile i processi di gestione e gli strumenti di controllo, con particolare attenzione agli elementi di *compliance* e ai controlli preventivi esistenti a presidio delle stesse.

Nella rilevazione del sistema di controllo esistente sono stati presi come riferimento i seguenti principi di controllo:

- esistenza di procedure formalizzate;
- tracciabilità e verificabilità *ex post* delle operazioni tramite adeguati supporti documentali/informativi;
- segregazione dei compiti;
- esistenza di deleghe formalizzate coerenti con le responsabilità organizzative assegnate.

2.1.3 Gap analysis e piano di azione (action plan)

Lo scopo della fase 3 è consistito nell'individuazione i) dei requisiti organizzativi caratterizzanti un modello organizzativo idoneo a prevenire i Reati-Presupposto e ii) delle azioni di miglioramento del modello organizzativo esistente.

Al fine di rilevare ed analizzare in dettaglio il modello di controllo esistente a presidio dei rischi riscontrati ed evidenziati nell'attività di analisi sopra descritta e di valutare la

conformità del modello stesso alle previsioni del Decreto e dell'art. 30 del d.lgs. 81/2008 (cfr. paragrafo 1.8 dell'Appendice I), Huawei ha eseguito un'analisi comparativa (la c.d. "*gap analysis*") tra il modello organizzativo e di controllo esistente ("*as is*") e un modello astratto di riferimento valutato sulla base delle esigenze manifestate dalla disciplina di cui al d.lgs. 231/2001 e al citato art. 30 del d.lgs. 81/2008, con particolare attenzione all'organizzazione della Società, al sistema di procedure aziendali ed all'adempimento degli obblighi giuridici relativi alle *"attività sensibili"* ivi espressamente richiamati ("*to be*").

Attraverso il confronto operato con la *gap analysis* è stato possibile desumere aree di miglioramento del sistema di controllo interno esistente e, sulla scorta di quanto emerso, è stato predisposto un piano di attuazione teso a individuare i requisiti organizzativi caratterizzanti un modello di organizzazione, gestione e controllo conforme a quanto disposto dal Decreto e le azioni di miglioramento del sistema di controllo interno.

2.1.4 Disegno del modello di organizzazione, gestione e controllo

Scopo della fase 4 è stata la definizione del modello di organizzazione, gestione e controllo ai sensi del Decreto, articolato in tutte le sue componenti e regole di funzionamento, idoneo alla prevenzione dei Reati-Presupposto e personalizzato alla realtà aziendale, in conformità alle disposizioni del Decreto, all'art 30 del d.lgs. 81/2008 sui modelli di organizzazione e gestione in materia di salute e sicurezza sul lavoro e alle linee guida delle associazioni di categoria maggiormente rappresentative (tra le quali *in primis* Confindustria).

La realizzazione della fase 4 è stata supportata sia dai risultati delle fasi precedenti sia dalle scelte di indirizzo degli organi decisionali della Società.

2.2 Adozione del Modello

2.2.1 In generale

Il presente Modello, elaborato e redatto secondo quanto descritto in precedenza, è stato adottato con delibera del Consiglio di Amministrazione di Huawei, in conformità all'art. 6, comma 1, lett. a) del Decreto.

Il Modello rappresenta un insieme coerente di principi, procedure e disposizioni che: i) incidono sul funzionamento interno della Società e sulle modalità con le quali la stessa si rapporta con l'esterno e ii) regolano la diligente gestione di un sistema di controllo delle attività sensibili, finalizzato a prevenire la commissione, o la tentata commissione, dei Reati-Presupposto.

Sotto la propria esclusiva responsabilità, Huawei provvede all'attuazione del Modello nel proprio ambito organizzativo in relazione alle proprie caratteristiche e alle attività dalla stessa in concreto poste in essere nelle aree a rischio.

2.2.2 Modifiche e integrazioni del Modello

Essendo il presente Modello un atto di emanazione dell'"organo dirigente" (in conformità alle prescrizioni dell'art. 6, comma 1, lettera a) del Decreto), le successive modifiche ed integrazioni di carattere sostanziale del presente Modello sono rimesse alla competenza del Consiglio di Amministrazione di Huawei.

È peraltro riconosciuta al Presidente del Consiglio di Amministrazione di Huawei la facoltà di apportare al testo del presente Modello eventuali modifiche o integrazioni di carattere formale (quali, ad esempio, quelle necessarie per l'adeguamento del testo del presente Modello all'eventuale, futura variazione di riferimenti normativi).

2.3 Contenuto, struttura e funzione

Il presente Modello è stato predisposto sulla base delle norme contenute nel Decreto, delle indicazioni fornite dall'art. 30 del d.lgs. 81/2008 e delle linee guida elaborate dalle associazioni di categoria maggiormente rappresentative (tra le quali *in primis* Confindustria) e recepisce, altresì, gli orientamenti e le evoluzioni giurisprudenziali in materia.

Il Modello, strutturato in un complesso articolato di documenti, è composto dai seguenti elementi:

- individuazione delle attività aziendali nel cui ambito possono essere commessi i Reati-Presupposto;
- previsione di protocolli di controllo in relazione alle attività sensibili e strumentali individuate;
- individuazione delle modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
- vigenza di un codice etico contenente i principi fondamentali cui si ispira il sistema organizzativo, amministrativo e contabile e – quale parte di esso – il Modello;
- istituzione di un organismo di vigilanza cui sono deputate le funzioni previste dal Decreto;
- definizione dei flussi informativi da e verso l'organismo di vigilanza e specifici obblighi di informazione nei confronti dell'organismo di vigilanza;
- programma di verifiche periodiche sulle attività sensibili e strumentali e sui relativi protocolli di controllo;
- sistema disciplinare atto a sanzionare la violazione delle disposizioni contenute nel Modello;
- piano di formazione e comunicazione al personale dipendente e ad altri soggetti che interagiscono con la Società;
- criteri di aggiornamento e adeguamento del Modello.

Al fine di assicurare l'idoneità del Modello a prevenire i reati di cui sopra, sono state tenute in considerazione anche le seguenti linee guida elaborate da precedenti esperienze estere[5] e ispiratrici anche del legislatore italiano:

- l'organizzazione deve stabilire standard e procedure di controllo, rivolte al personale (e ad altri mandatari), che siano ragionevolmente atte a ridurre la possibilità di condotte illegali;
- a una o più persone di alto livello appartenenti all'organizzazione deve essere assegnata la responsabilità di sorvegliare la conformità agli standard e procedure definiti;
- l'organizzazione deve esercitare sufficiente attenzione e non deve delegare rilevanti poteri discrezionali a persone di cui conosceva – o avrebbe potuto conoscere, mediante l'esercizio della ordinaria diligenza – la propensione a svolgere attività illegali;

[5] Come riportato nelle linee guida predisposte da Confindustria, versione aggiornata del 31 marzo 2008, il riferimento internazionale comunemente accettato come modello di riferimento in tema di *governance* e controllo interno è il "CoSO Report", prodotto in USA nel 1992 dalla Coopers & Lybrand (ora PricewaterhouseCoopers) su incarico del *Committee of Sponsoring Organizations of the Treadway Commission* (con l'Institute of Internal Auditors e l'AICPA fra le Sponsoring Organizations) che lo ha adottato e proposto quale modello di riferimento per il sistema di controllo delle imprese. Ad esso si sono ispirate le regolamentazioni nazionali di tutti i principali Paesi (Regno Unito, Canada, ecc.). Pur senza essere direttamente menzionato è evidente il riferimento concettuale al CoSO Report in alcune norme italiane fra cui la Guida Operativa Collegio Sindacale (ottobre 2000), le Circolari dell'ISVAP e della Banca d'Italia.

- l'organizzazione deve fare passi concreti volti a comunicare in maniera efficace standard e procedure a tutto il personale (e altri mandatari), ad esempio prevedendo la partecipazione a programmi di formazione o distribuendo pubblicazioni che spiegano in termini pratici cosa è richiesto;
- l'organizzazione deve adottare misure ragionevoli, volte ad ottenere l'effettiva aderenza agli standard, ad esempio utilizzando sistemi di monitoraggio e di *auditing* ragionevolmente adatti a scoprire condotte in deroga dei dipendenti (e altri mandatari), ed introducendo e pubblicizzando un sistema di segnalazioni che consenta al personale (e agli altri mandatari) di riferire casi di violazione di norme (da parte di altri all'interno dell'organizzazione), senza timore di ritorsioni;
- gli standard devono essere resi esecutivi in maniera coerente mediante appropriati meccanismi disciplinari, che comprendano, se del caso, anche la punizione di persone responsabili di non aver scoperto una violazione per omessa o insufficiente vigilanza. L'adeguata punizione delle persone responsabili di una violazione è una componente necessaria dell'efficacia esecutiva; tuttavia, la congruità della punizione dovrà fare riferimento allo specifico caso esaminato;
- dopo avere scoperto una violazione, l'organizzazione deve compiere tutti i passi ragionevolmente necessari per dare una risposta appropriata alla violazione stessa e per prevenire l'avverarsi di violazioni similari in futuro; ciò comprende qualunque necessaria modifica al modello, allo scopo di prevenire e scoprire le violazioni di leggi.

Il Modello consta di (i) una Parte Generale, illustrativa del contesto normativo di riferimento, degli obiettivi, delle linee di struttura e delle modalità di implementazione dello stesso e (ii) una Parte Speciale relativa ai Reati-Presupposto.

Il Modello identifica le attività sensibili in relazione alle quali è più alto il rischio di commissione dei Reati-Presupposto, ed introduce sistemi di procedimentalizzazione e controllo delle attività, da svolgersi anche in via preventiva.

L'individuazione delle aree a rischio e la procedimentalizzazione delle attività consente di: (i) sensibilizzare dipendenti e management sulle aree ed i rispettivi aspetti della gestione aziendale che richiedono maggiore attenzione; (ii) esplicitare la ferma condanna di tutte le condotte che integrino la fattispecie di reato; (iii) sottoporre tali aree ad un sistema costante di monitoraggio e controllo, funzionale ad un intervento immediato in caso di commissione dei reati di cui sopra.

2.4 Rapporti con il Business Code of Conduct

Il Modello costituisce un documento giuridicamente distinto ed autonomo rispetto al Business Code of Conduct adottato da Huawei cui è allegato (**Allegato 3**). Tale Business Code of Conduct costituisce parte integrante del sistema di organizzazione, gestione e controllo nonché di prevenzione adottato dalla Società.

In particolare:

- il Business Code of Conduct rappresenta uno strumento adottato da Huawei, che contiene un insieme dei diritti, dei doveri e delle responsabilità della Società nei confronti di dipendenti, clienti, fornitori, Pubblica Amministrazione (in generale, quindi, con riferimento a soggetti portatori di interesse nei confronti della Società); il Business Code of Conduct mira quindi a raccomandare, promuovere o vietare determinati comportamenti, indipendentemente ed anche al di là di quanto previsto dal Decreto o dalla normativa vigente;
- il presente Modello è strumento adottato sulla base delle precise indicazioni normative contenute nel Decreto, orientato alla prevenzione dei reati contemplati dal Decreto da parte di soggetti apicali della Società e dei loro sottoposti.

2.5 Definizioni

Nel presente Modello, in aggiunta alle ulteriori espressioni definite di volta in volta nel testo e non riportate nel presente paragrafo, le seguenti espressioni avranno il significato qui di seguito indicato:

"**Clienti**"	soggetti, diversi dalle società del Gruppo, che hanno stipulato con Huawei un contratto per la fornitura di prodotti e servizi ICT da parte di Huawei.
"**Collaboratori**"	soggetti che intrattengono con Huawei rapporti di agenzia, rappresentanza, distribuzione commerciale ovvero altri rapporti di collaborazione coordinata e continuativa prevalentemente personale e senza vincolo di subordinazione (quali, a titolo esemplificativo e non esaustivo, lavoro a progetto, lavoro somministrato; inserimento; tirocinio estivo di orientamento) ovvero qualsiasi altro rapporto contemplato dall'art. 409 c.p.c.[6], le prestazioni di lavoro occasionale, nonché qualsiasi altra persona sottoposta alla direzione o vigilanza di qualsiasi soggetto in posizione apicale di Huawei ai sensi del d.lgs. 231/2001;
"**Consulenti**"	consulenti esterni incaricati di assistere Huawei nel compimento delle proprie attività, su base continuativa o occasionale;
"**Destinatari**"	soggetti cui si applicano le disposizioni del presente Modello e, in particolare, i Dipendenti, i Responsabili, i Collaboratori e gli Esponenti Aziendali nonché, nei casi ad essi specificamente riferiti nel presente Modello, i Consulenti e i Partners;
"**Dipendenti**"	soggetti che intrattengono con Huawei un rapporto di lavoro subordinato (compresi i dirigenti), inclusi i lavoratori a termine o a tempo parziale (nonché i lavoratori in distacco ovvero in forza con contratti di lavoro subordinato di cui alla legge 23 febbraio 2003, n. 30);
"**Esponenti Aziendali**"	come di volta in volta in carica, il Presidente, i membri del Consiglio di Amministrazione, del Collegio Sindacale, del comitato esecutivo (se esistente), i direttori generali (se esistenti), nonché qualsiasi altro soggetto in posizione apicale, per tale intendendosi qualsiasi persona che rivesta funzioni di rappresentanza, amministrazione o direzione di Huawei, ai sensi del d.lgs. 231/2001; a tal fine, si ricorda che, ai fini del Decreto:

[6] Art. 409. *Controversie individuali di lavoro.* – Si osservano le disposizioni del presente capo nelle controversie relative a: 1) rapporti di lavoro subordinato privato, anche se non inerenti all'esercizio di un'impresa; 2) rapporti di mezzadria, colonia parziaria, di compartecipazione agraria, di affitto a coltivatore diretto, nonché rapporti derivanti da altri contratti agrari, salva la competenza delle sezioni specializzate agrarie; 3) rapporti di agenzia, di rappresentanza commerciale ed altri rapporti che si concretino in una prestazione di opera coordinata e continuativa, prevalentemente personale, anche se non a carattere subordinato; 4) rapporti di lavoro di dipendenti di enti pubblici che svolgono esclusivamente o prevalentemente attività economica; 5) rapporti di lavoro di dipendenti di enti pubblici e altri rapporti di diritto pubblico, sempreché non siano devoluti dalla legge ad altro giudice.

	– si considera soggetto in posizione apicale colui che riveste funzioni di rappresentanza della Società (ad es. il Presidente della Società), nonché di amministrazione o direzione della Società (ad esempio gli amministratori e i direttori generali) ovvero di un'unità organizzativa dotata di autonomia finanziaria e funzionale; – in materia di salute e sicurezza sul lavoro, si considera soggetto in posizione apicale, colui che riveste poteri di direzione dell'ente (ad esempio, il datore di lavoro e/o il delegato funzionale *ex* art. 16 del d.lgs. 81/2008); resta inteso che le funzioni di cui sopra possono essere svolte anche presso una unità organizzativa dotata di autonomia finanziaria e funzionale (per esempio, il direttore di uno stabilimento munito di autonomi poteri di direzione).
"Organismo"	o "**Organismo di Vigilanza**" o "**Organismo di Huawei**", l'organismo di vigilanza, dotato di autonomi poteri di iniziativa e controllo in conformità al d.lgs. 231/2001, istituito da Huawei ai sensi dell'art. 6, comma 1, lett. b) del Decreto e indicato nel Capitolo 3 della presente Parte Generale del Modello;
"**Modello**"	modello di organizzazione, gestione e controllo ai sensi del d.lgs. 231/2001 della Società ed in particolare il presente documento con i suoi allegati e le sue successive modifiche ed integrazioni, unitamente a tutte le procedure, istruzioni, circolari, e altri documenti in esso richiamati;
"**Partners**"	soggetti terzi che sono parti di rapporti contrattuali con Huawei di medio-lungo periodo (vale a dire di durata pari o superiore a 18 mesi, tenuto conto anche di eventuali rinnovi contrattuali) quali, a titolo esemplificativo, fornitori (anche in forza di contratti di *outsourcing*), subappaltatori, sponsor o soggetti sponsorizzati o convenzionati, imprese partecipanti ad eventuali associazioni temporanee di imprese con Huawei, consorzi di ogni genere di cui sia parte Huawei, società comuni in cui Huawei sia in rapporto di controllo o collegamento ai sensi dell'art. 2359 c.c. (nonché i soci di Huawei in tali società comuni) o altri soggetti espressamente individuati come partners commerciali da Huawei in una o più operazioni. Per evitare dubbi, si chiarisce che i soggetti rientranti in una delle altre categorie di Destinatari (in particolare, quella di Clienti, Consulenti o Collaboratori) non rientrano, per ciò stesso, nella categoria dei Partners. In sede di attuazione del presente Modello ed allo scopo di renderne più agevole l'applicazione, l'Organismo di Vigilanza, a mezzo di apposite comunicazioni circolari, ha la facoltà di identificare espressamente ed in maggiore dettaglio i soggetti rientranti di volta in volta nella categoria dei Partners, anche mediante redazione di apposito elenco esemplificativo, tenendo conto delle attività in concreto esercitate dalla Società;
"**Responsabili**"	ciascun responsabile di una o più divisione o unità organizzativa dotata di autonomia finanziaria e/o funzionale

della Società, in conformità all'organigramma di Huawei come di volta in volta vigente.

CAPITOLO 3
L'ORGANISMO DI VIGILANZA DI HUAWEI TECHNOLOGIES ITALIA S.R.L.

3.1 L'Organismo di Vigilanza di Huawei

In base alle previsioni del Decreto – art. 6, comma 1, lett. a) e b) – l'ente può essere esonerato dalla responsabilità conseguente alla commissione di reati da parte dei soggetti qualificati *ex* art. 5 del Decreto stesso, se l'organo dirigente ha, fra l'altro:

- adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
- affidato il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo.

L'affidamento dei suddetti compiti ad un organismo dotato di autonomi poteri di iniziativa e controllo, unitamente al corretto ed efficace svolgimento degli stessi rappresentano, quindi, presupposti indispensabili per l'esonero dalla responsabilità dell'ente prevista dal Decreto.

Le Linee guida di Confindustria[7], che rappresentano il primo codice di comportamento per la redazione dei modelli di organizzazione, gestione e controllo di cui al Decreto redatto da un'associazione di categoria, individuano quali requisiti principali dell'organismo di vigilanza l'autonomia e indipendenza, la professionalità e la continuità di azione.

In particolare, secondo Confindustria:

i) i requisiti di autonomia ed indipendenza richiedono: l'inserimento dell'organismo di vigilanza "*come unità di staff in una posizione gerarchica la più elevata possibile*", la previsione di un "*riporto*" dell'organismo di vigilanza al massimo vertice aziendale operativo, l'assenza, in capo all'organismo di vigilanza, di compiti operativi che - rendendolo partecipe di decisioni ed attività operative - ne metterebbero a repentaglio l'obiettività di giudizio;

ii) il connotato della professionalità deve essere riferito al "*bagaglio di strumenti e tecniche*"[8] necessarie per svolgere efficacemente l'attività di organismo di vigilanza;

iii) la continuità di azione, che garantisce un'efficace e costante attuazione del modello organizzativo particolarmente articolato e complesso nelle aziende di grandi e medie

[7] Confindustria, *Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001*, aggiornate al 31 marzo 2008.

[8] "*Si tratta di tecniche specialistiche proprie di chi svolge attività "ispettiva", ma anche consulenziale di analisi dei sistemi di controllo e di tipo giuridico e, più in particolare, penalistico*". Confindustria, *Linee guida*, *cit*., nella versione aggiornata al 31 marzo 2008, 36. In particolare, si tratta di tecniche che possono essere utilizzate:
- in via preventiva, per adottare - all'atto del disegno del modello organizzativo e delle successive modifiche - le misure più idonee a prevenire, con ragionevole certezza, la commissione dei reati in questione;
- correntemente, per verificare che i comportamenti quotidiani rispettino effettivamente quelli codificati;
- *a posteriori*, per accertare come si sia potuto verificare un reato delle specie in esame e chi lo abbia commesso.

A titolo esemplificativo, le Linee guida di Confindustria menzionano le seguenti tecniche:
- campionamento statistico;
- tecniche di analisi e valutazione dei rischi e misure per il loro contenimento (procedure autorizzative; meccanismi di contrapposizione di compiti);
- *flow-charting* di procedure e processi per l'individuazione dei punti di debolezza;
- tecniche di intervista e di elaborazione di questionari;
- elementi di psicologia;
- metodi per l'individuazione di frodi.

dimensioni, è favorita dalla presenza di una struttura dedicata esclusivamente e a tempo pieno all'attività di vigilanza del modello e "*priva di mansioni operative che possano portarla ad assumere decisioni con effetti economici-finanziari*".

Circa l'identificazione dell'organismo di vigilanza e la sua composizione, il Decreto prevede esclusivamente che:

- negli enti di piccole dimensioni i compiti dell'organismo di vigilanza possono essere svolti direttamente dall'organo dirigente (art. 6, comma 4)[9];
- nelle società di capitali il collegio sindacale, il consiglio di sorveglianza e il comitato per il controllo della gestione possono svolgere le funzioni dell'organismo di vigilanza (art. 6, comma 4-*bis*)[10].

Le Linee guida di Confindustria[11] indicano inoltre quali opzioni possibili per l'ente, al momento dell'individuazione e configurazione dell'organismo di vigilanza:

(i) l'attribuzione del ruolo di organismo di vigilanza al comitato per il controllo interno, ove esistente, purché composto esclusivamente da amministratori non esecutivi e/o indipendenti;

(ii) l'attribuzione del ruolo di organismo di vigilanza alla funzione di *internal auditing*, ove esistente;

(iii) la creazione di un organismo *ad hoc*, a composizione monosoggettiva o plurisoggettiva, costituito, in quest'ultimo caso, da soggetti dell'ente (es. responsabile dell'*internal audit*, della funzione legale, ecc., e/o amministratore non esecutivo e/o indipendente e/o sindaco) e/o da soggetti esterni (es. consulenti, esperti, ecc.).

In ottemperanza a quanto previsto nel Decreto e tenuto conto delle caratteristiche peculiari della propria struttura organizzativa, la Società, con delibera del Consiglio di Amministrazione in data 9 Novembre 2014 adottata con il parere favorevole del Collegio Sindacale, ha affidato la funzione di Organismo di Vigilanza deputato a vigilare sul funzionamento e l'osservanza del presente Modello e a curarne l'aggiornamento, a un organismo composto da n. 3 membri, come segue:

a. Luca Mastromatteo, Presidente ODV;
b. Tommaso Cappiello, Membro ODV;
c. Maurizio Prosseda, Membro ODV.

[9] Le Linee guida di Confindustria precisano che la disciplina dettata dal d.lgs. 231/2001 "*non fornisce indicazioni circa la composizione dell'Organismo di vigilanza (Odv). Ciò consente di optare per una composizione sia mono che plurisoggettiva. Nella composizione plurisoggettiva possono essere chiamati a far parte dell'Odv componenti interni ed esterni all'ente* (…). *Sebbene in via di principio la composizione sembri indifferente per il legislatore, tuttavia, la scelta tra l'una o l'altra soluzione deve tenere conto delle finalità perseguite dalla legge e, quindi, deve assicurare il profilo di effettività dei controlli in relazione alla dimensione ed alla complessità organizzativa dell'ente. Con riferimento alle imprese di piccole dimensioni, si deve ricordare che l'art. 6 comma 4 consente che i compiti di cui alla lettera b) dell'art. 6 comma 2, siano assolti dall'organo dirigente. Questa impostazione è stata confermata dalla giurisprudenza, che ha ribadito l'esigenza di scegliere il tipo di composizione anche in relazione alle dimensioni aziendali. Pertanto, nelle realtà di piccole dimensioni (...) che non si avvalgano della facoltà di cui al comma 4 dell'art. 6, la composizione monocratica ben potrebbe garantire le funzioni demandate all'Organismo, mentre in quelle di dimensioni medio grandi sarebbe preferibile una composizione di tipo collegiale. Ciò al fine di garantire una maggiore effettività dei controlli demandati dalla legge* ". Confindustria, *Linee guida*, *cit*., nella versione aggiornata al 31 marzo 2008, 32 s.
Si rileva inoltre che per quanto concerne gli enti di "*piccole dimensioni*" il Decreto non contiene una definizione di tali enti. Un'indicazione in tal senso, è tuttavia fornita dalle Linee guida di Confindustria, secondo le quali "*una piccola impresa va ricercata più che in parametri dimensionali, nella essenzialità della struttura interna gerarchica e funzionale*". Confindustria, Linee guida, cit., nella versione aggiornata al 31 marzo 2008, 50.

[10] Il comma 4-*bis* è stato aggiunto dal comma 12 dell'art. 14, legge 12 novembre 2011, n. 183, a decorrere dal 1° gennaio 2012, ai sensi di quanto disposto dal comma 1 dell'art. 36 della stessa legge n. 183/2011.

[11] Confindustria, *Linee guida*, *cit*., nella versione aggiornata al 31 marzo 2008, 43.

L'Organismo, come sopra costituito, è dotato, come richiesto dal Decreto, di autonomi poteri di iniziativa e controllo ed opera in posizione di indipendenza ed autonomia.

L'autonomia e indipendenza della quale l'Organismo di Vigilanza deve necessariamente disporre è garantita dal posizionamento riconosciuto all'Organismo di Vigilanza nell'organigramma aziendale, nonché dalle linee di riporto verso il vertice aziendale operativo attribuite all'Organismo di Vigilanza ai sensi del Modello.

La professionalità è assicurata dalle competenze specifiche maturate da ciascun membro dell'Organismo di Vigilanza con riferimento al settore in cui opera la Società, nonché dalla facoltà riconosciuta all'Organismo di Vigilanza di avvalersi delle specifiche professionalità sia dei responsabili di varie funzioni aziendali sia di consulenti esterni per l'esecuzione delle operazioni tecniche necessarie per lo svolgimento delle sue funzioni.

La continuità di azione è garantita dalla circostanza che l'Organismo di Vigilanza è dedicato all'attività di vigilanza in via primaria ed è privo di poteri operativi nella Società.

In considerazione della specificità dei compiti attribuiti all'Organismo e delle professionalità di volta in volta richieste, nello svolgimento delle funzioni di vigilanza, controllo ed aggiornamento l'Organismo si avvale della collaborazione delle funzioni interne della Società di volta in volta competenti.

In particolare, per le tematiche HSE, l'Organismo si avvale del supporto dell'RSPP e del responsabile ambientale.

Inoltre, ove siano richieste specializzazioni non presenti all'interno delle funzioni sopra indicate, l'Organismo potrà fare ricorso a consulenti esterni, i quali saranno nominati con delibera del Consiglio di Amministrazione, su specifica richiesta ed indicazione dell'Organismo stesso.

Qualsivoglia richiesta di supporto o comunicazioni di eventuali non conformità al presente modello e/o alla normativa applicabile possono essere indirizzate a ITcompliance@huawei.com

3.2 Nomina

L'Organismo di Vigilanza è istituito con delibera del Consiglio di Amministrazione, sentito il parere del Collegio Sindacale.

L'Organismo di Vigilanza resta in carica per il numero di esercizi sociali stabilito dal Consiglio di Amministrazione all'atto di nomina e comunque (ovvero in assenza di sua determinazione all'atto di nomina) non oltre tre esercizi, ed è rieleggibile.

Salvo diversa deliberazione del Consiglio di Amministrazione all'atto di nomina, l'Organismo di Vigilanza cessa per scadenza del termine alla data dell'Assemblea convocata per l'approvazione del bilancio relativo all'ultimo esercizio della sua carica, pur continuando a svolgere *ad interim* le proprie funzioni (in regime di c.d. *prorogatio*) fino a nomina di un nuovo Organismo.

3.3 Requisiti e decadenza

La nomina dell'Organismo di Vigilanza, ovvero di ciascuno dei suoi componenti in caso di Organismo di Vigilanza a composizione plurisoggettiva, è condizionata alla presenza dei requisiti soggettivi di eleggibilità di seguito elencati e descritti[12].

In particolare, all'atto del conferimento dell'incarico, il soggetto designato a ricoprire la carica di Organismo di Vigilanza (o, in caso di Organismo costituito in forma plurisoggettiva, ciascuno dei suoi componenti) deve rilasciare una dichiarazione, sostanzialmente conforme all'**Allegato 4**, nella quale attesti l'assenza di:

- relazioni di parentela, coniugio (o situazioni di convivenza di fatto equiparabili al coniugio) o affinità entro il quarto grado[13] con componenti del Consiglio di Amministrazione, sindaci e revisori incaricati dalla società di revisione legale, nonché soggetti apicali della Società;
- conflitti di interesse, anche potenziali, con la Società tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti propri dell'Organismo di Vigilanza, nonché coincidenze di interesse con la Società stessa esorbitanti da quelle ordinarie basate sull'eventuale rapporto di dipendenza o di prestazione d'opera intellettuale;
- titolarità, diretta o indiretta, di partecipazioni societarie di entità tale da permettere di esercitare una influenza dominante o notevole sulla Società, ai sensi dell'art. 2359 c.c.;
- funzioni di amministrazione con deleghe esecutive presso la Società o altre società del gruppo cui appartiene la Società;
- funzioni di amministrazione – nei tre esercizi precedenti alla nomina quale componente/esponente dell'Organismo di Vigilanza – di imprese sottoposte a fallimento, liquidazione coatta amministrativa o altre procedure concorsuali;

[12] "*Allo scopo di assicurare l'effettiva sussistenza dei descritti requisiti, sia nel caso di un Organismo di vigilanza composto da una o più risorse interne che nell'ipotesi in cui esso sia composto, in via esclusiva o anche, da più figure esterne, sarà opportuno che i membri possiedano, oltre alle competenze professionali descritte, i requisiti soggettivi formali che garantiscano ulteriormente l'autonomia e l'indipendenza richiesta dal compito (es. onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli organi sociali e con il vertice, ecc.). Tali requisiti andranno specificati nel Modello organizzativo. I requisiti di autonomia, onorabilità e professionalità potranno anche essere definiti per rinvio a quanto previsto per altri settori della normativa societaria. Ciò vale, in particolare, quando si opti per una composizione plurisoggettiva dell'Organismo di vigilanza ed in esso vengano a concentrarsi tutte le diverse competenze professionali che concorrono al controllo della gestione sociale nel tradizionale modello di governo societario (es. un amministratore non esecutivo o indipendente membro del comitato per il controllo interno; un componente del Collegio sindacale; il preposto al controllo interno). In questi casi l'esistenza dei requisiti richiamati viene già assicurata, anche in assenza di ulteriori indicazioni, dalle caratteristiche personali e professionali richieste dall'ordinamento per gli amministratori indipendenti, per i sindaci e per il preposto ai controlli interni*". Confindustria, *Linee guida*, *cit*., nella versione definitiva al 31 marzo 2008, 37 s.

[13] Al fine di individuare la nozione di "parenti e affini entro il 4° grado" deve farsi riferimento alle disposizioni dell'art. 74 e ss. codice civile.
Ai sensi di tali disposizioni, la parentela è il vincolo tra le persone che discendono da uno stesso stipite (ad es. due fratelli sono parenti in quanto discendono da uno stesso stipite, rappresentato dal genitore). I parenti possono essere in linea retta o collaterale: sono parenti in linea retta le persone di cui l'una discende dall'altra (ad es. nonno, padre e figlio), mentre sono parenti in linea collaterale quelle persone che, pur avendo uno stipite comune, non discendono l'un dall'altra (ad es. due fratelli tra loro oppure lo zio ed il nipote). Nella linea retta si computano tanti gradi quante sono le generazioni, escluso lo stipite (ad es. padre e figlio sono tra loro parenti di primo grado, nonno e nipote lo sono di secondo grado); nella linea collaterale i gradi si computano dalle generazioni, salendo da uno dei parenti fino allo stipite comune e da questo discendendo all'altro parente, sempre restando escluso lo stipite (ad es. due fratelli sono tra loro parenti di secondo grado). Quindi, i parenti entro il quarto grado sono a) in linea retta: genitori e figli nonché nonni, bisnonni, trisnonni e nipoti e b) in linea collaterale: fratelli tra loro, fratelli e figli di una stessa persona, figli e figli dei figli dei figli di una stessa persona, figli di due fratelli).
Ai sensi delle stesse disposizioni, l'affinità è il vincolo tra un coniuge e i parenti dell'altro coniuge. Nella linea e nel grado in cui taluno è parente d'uno dei coniugi, egli è affine dell'altro coniuge (ad es. una persona è parente in linea retta entro il quarto grado dei propri cugini più prossimi, per tali intendendosi i figli dei fratelli dei suoi genitori, ed è affine in pari linea e grado dei coniugi di tali cugini).

- rapporto di pubblico impiego presso amministrazioni centrali o locali nei tre anni precedenti alla nomina quale componente/esponente dell'Organismo di Vigilanza;
- sentenza di condanna anche non passata in giudicato, ovvero provvedimento che comunque ne accerti la responsabilità, in Italia o all'estero, per i delitti richiamati dal Decreto o delitti ad essi assimilabili;
- condanna, con sentenza anche non passata in giudicato, ovvero con provvedimento che comunque ne accerti la responsabilità, a una pena che importa l'interdizione, anche temporanea, dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

Laddove alcuno dei sopra richiamati motivi di ineleggibilità dovesse configurarsi a carico del componente/esponente dell'Organismo, questi dovrà darne notizia al Presidente del Consiglio di Amministrazione e al Presidente del Collegio Sindacale e decadrà automaticamente dalla carica.

3.4 Rinuncia e sostituzione

L'Organismo di Vigilanza (o, in caso di Organismo costituito in forma plurisoggettiva, ciascuno dei suoi componenti) che rinunzia all'ufficio deve darne comunicazione scritta al Presidente del Consiglio di Amministrazione e al Presidente del Collegio Sindacale.

La rinuncia ha effetto immediato. Il Consiglio di Amministrazione provvede alla sua sostituzione, nominando un nuovo organismo (o, in caso di organismo costituito in forma plurisoggettiva, un nuovo componente) nel più breve tempo possibile, con il parere del Collegio Sindacale.

I membri dell'Organismo di Vigilanza nominati durano in carica per il tempo per il quale avrebbero dovuto rimanervi i soggetti da essi sostituiti.

3.5 Indipendenza e revoca

L'adozione di sanzioni disciplinari nonché di qualsiasi atto modificativo o interruttivo del rapporto della Società con l'Organismo (o, in caso di Organismo costituito in forma plurisoggettiva, ciascuno dei suoi componenti) è disposta dal Consiglio di Amministrazione con parere favorevole del Collegio Sindacale e, in caso di approvazione degli interventi modificativi o interruttivi adottati senza la unanimità di decisione, è data adeguata informazione da parte del Presidente, o in sua carenza da parte del Presidente del Collegio Sindacale, all'Assemblea, alla prima occasione utile.

Fermo restando quanto precede, al fine di garantire la necessaria stabilità all'Organismo di Vigilanza, la revoca dell'Organismo di Vigilanza (o, in caso di Organismo costituito in forma plurisoggettiva, ciascuno dei suoi componenti), ovvero dei poteri ad esso attribuiti nell'ambito della relativa carica, può avvenire soltanto per giusta causa.

A tale proposito, per "*giusta causa*" si intende una grave negligenza nell'assolvimento dei compiti connessi con l'incarico quale (a titolo meramente esemplificativo): l'omessa redazione della relazione periodica al Consiglio di Amministrazione ed al Collegio Sindacale sull'attività svolta; l'omessa redazione di un programma semestrale o annuale di verifiche ovvero della sua attuazione; in particolare, costituisce grave negligenza l'"*omessa o insufficiente vigilanza*" da parte dell'Organismo di Vigilanza – secondo quanto previsto dall'art. 6, comma 1, lett. d), del Decreto – risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti della Società ai sensi del Decreto ovvero da provvedimento che comunque ne accerti la responsabilità.

L'attribuzione al soggetto che ricopra la funzione di Organismo di Vigilanza, o di un suo membro, di funzioni e responsabilità operative all'interno dell'organizzazione aziendale

comunque incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri dell'Organismo di Vigilanza comporta l'incompatibilità di tale soggetto con la funzione di Organismo di Vigilanza. Tale incompatibilità deve essere tempestivamente comunicata al Consiglio di Amministrazione e al Collegio Sindacale e dal primo accertata mediante deliberazione, con conseguente decadenza e sostituzione di tale soggetto.

In casi di particolare gravità, il Consiglio di Amministrazione potrà comunque disporre – sentito il parere del Collegio Sindacale – la sospensione dei poteri dell'Organismo di Vigilanza (o, in caso di organismo costituito in forma plurisoggettiva, di ciascuno dei suoi componenti) e la nomina di un Organismo (o, in caso di organismo costituito in forma plurisoggettiva, di un componente) *ad interim*.

3.6 Conflitti di interesse e concorrenza

Nel caso in cui, con riferimento a una data operazione a rischio o categoria di operazioni a rischio, l'Organismo di Vigilanza (o, in caso di Organismo costituito in forma plurisoggettiva, un suo componente) si trovi, o ritenga di trovarsi o di potersi venire a trovare, in una situazione di potenziale o attuale conflitto di interessi con la Società nello svolgimento delle sue funzioni di vigilanza, tale soggetto deve comunicare ciò immediatamente al Presidente del Consiglio di Amministrazione e al Presidente del Collegio Sindacale (nonché agli altri membri dell'Organismo di Vigilanza, se ciò sia applicabile).

La sussistenza di una situazione di potenziale o attuale conflitto di interessi determina, per tale soggetto, l'obbligo di astenersi dal compiere atti connessi o relativi a tale operazione nell'esercizio delle funzioni di vigilanza; in tal caso, l'Organismo di Vigilanza provvede a:

- sollecitare la nomina di altro soggetto quale suo sostituto per l'esercizio delle funzioni di vigilanza in relazione all'operazione o categoria di operazioni in questione;
- oppure,
- in caso di organismo di vigilanza a composizione plurisoggettiva ove il conflitto di interessi riguardi uno solo dei suoi membri, provvede a delegare la vigilanza relativa all'operazione o categoria di operazioni in questione agli altri membri dell'Organismo di Vigilanza.

A titolo esemplificativo, costituisce situazione di conflitto di interessi in una data operazione o categoria di operazioni il fatto che un soggetto sia legato ad uno o più altri soggetti coinvolti in una operazione o categoria di operazioni a causa di cariche sociali, rapporti di coniugio, parentela o affinità entro il quarto grado, lavoro, consulenza o prestazione d'opera retribuita, ovvero altri rapporti di natura patrimoniale che ne compromettano l'indipendenza ai sensi dell'art. 2399 lett. c) c.c.

All'Organismo di Vigilanza (o, in caso di organismo costituito in forma plurisoggettiva, a ciascuno dei suoi componenti) si applica il divieto di concorrenza di cui all'art. 2390 c.c.

3.7 Remunerazione e rimborsi spese

L'eventuale remunerazione spettante all'Organismo di Vigilanza (o, in caso di organismo costituito in forma plurisoggettiva, a ciascuno dei suoi componenti) è stabilita all'atto della nomina o con successiva decisione del Consiglio di Amministrazione, sentito il parere del Collegio Sindacale.

All'Organismo di Vigilanza (o, in caso di organismo costituito in forma plurisoggettiva, a ciascuno dei suoi componenti) spetta il rimborso delle spese sostenute per le ragioni dell'ufficio.

3.8 Poteri di spesa e nomina di consulenti esterni

L'Organismo di Vigilanza è dotato di poteri di spesa necessari al fine dell'esecuzione delle attività di verifica (ed esclusi in ogni caso gli interventi comportanti innovazioni di carattere strutturale dell'azienda) esercitabili nel rispetto delle procedure interne di volta in volta vigenti, sulla base di un budget adesso assegnato annualmente.

L'Organismo di Vigilanza può avvalersi – sotto la sua diretta responsabilità – nello svolgimento dei compiti affidatigli, della collaborazione di tutte le funzioni e strutture della Società ovvero di consulenti esterni.

All'atto del conferimento dell'incarico, il consulente esterno deve rilasciare apposita dichiarazione nella quale attesta:

- l'assenza dei sopra elencati motivi di ineleggibilità o di ragioni ostative all'assunzione dell'incarico (ad esempio: conflitti di interesse; relazioni di parentela con componenti del Consiglio di Amministrazione, soggetti apicali in genere, sindaci della Società e revisori incaricati dalla società di revisione legale, ecc.);
- la circostanza di essere stato adeguatamente informato delle disposizioni e delle regole comportamentali previste dal Modello e di impegnarsi a rispettarle.

3.9 Funzioni e poteri

Ciascun componente dell'Organismo di Vigilanza è individualmente titolare dei poteri di iniziativa e controllo spettanti all'Organismo di Vigilanza ai sensi del d.lgs. 231/2001 e del Modello. Tali poteri di iniziativa e controllo non sono in alcun modo limitati dalle deliberazioni o decisioni assunte dall'Organismo di Vigilanza ai sensi del regolamento dell'Organismo, siano esse prese a maggioranza o all'unanimità dei suoi componenti.

All'Organismo sono affidate le seguenti funzioni:

- vigilare sull'effettiva e concreta applicazione del Modello, verificando la congruità dei comportamenti all'interno della Società rispetto allo stesso;
- valutare la concreta adeguatezza del Modello a svolgere la sua funzione di strumento di prevenzione dei Reati-Presupposto;
- analizzare il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello;
- relazionare agli organi competenti sullo stato di attuazione del presente Modello;
- curare, sviluppare e promuovere il costante aggiornamento del Modello elaborando e formulando all'organo dirigente, mediante la presentazione di rapporti e/o relazioni scritte, proposte di modifica ed aggiornamento del Modello volte (i) a correggere eventuali disfunzioni o lacune, come emerse di volta in volta; (ii) ad adeguare il Modello a significative modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento dell'attività di impresa ovvero (iii) a recepire eventuali modifiche normative (si veda, a riguardo, quanto espressamente prevede il comma 4 dell'art. 30 del d.lgs. 81/2008 in materia di salute e sicurezza nei luoghi di lavoro secondo cui *"il riesame e l'eventuale modifica del modello organizzativo devono essere adottati quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico"*);
- assicurare il periodico aggiornamento del sistema di identificazione, mappatura e classificazione delle attività sensibili e strumentali;
- sottoporre proposte di integrazione ovvero di adozione di istruzioni per l'attuazione del presente Modello agli organi competenti;

- verificare l'attuazione e l'effettiva funzionalità delle modifiche apportate al presente Modello (*follow-up*).

Nell'espletamento di tali funzioni, l'Organismo ha il compito di:

- proporre e promuovere tutte le iniziative necessarie alla conoscenza del presente Modello all'interno ed all'esterno della Società;
- mantenere un collegamento costante con la società di revisione legale, salvaguardandone la necessaria indipendenza, e con gli altri consulenti e collaboratori coinvolti nelle attività di efficace attuazione del Modello;
- controllare l'attività svolta dalle varie funzioni all'interno della Società, accedendo alla relativa documentazione e, in particolare, controllare l'effettiva presenza, la regolare tenuta e l'efficacia della documentazione richiesta in conformità a quanto previsto nella Parte Speciale per le diverse tipologie di reati ivi contemplate;
- effettuare verifiche mirate su determinati settori o specifiche procedure dell'attività aziendale e condurre le indagini interne per l'accertamento di presunte violazioni delle prescrizioni del presente Modello;
- rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i responsabili delle varie funzioni;
- verificare che gli elementi previsti dalla Parte Speciale per le diverse tipologie di reati ivi contemplate (procedure di sistema, istruzioni operative, documenti tecnici, moduli, clausole standard, ecc.) siano comunque adeguati e rispondenti alle esigenze di osservanza di quanto prescritto dal Decreto, provvedendo, in caso contrario, a un aggiornamento degli elementi stessi;
- coordinarsi con le altre funzioni aziendali, al fine di studiare la mappa delle aree a rischio, monitorare lo stato di attuazione del presente Modello e predisporre interventi migliorativi o integrativi in relazione agli aspetti attinenti all'attuazione coordinata del Modello (istruzioni per l'attuazione del presente Modello, criteri ispettivi, definizione delle clausole standard, formazione del personale, provvedimenti disciplinari, ecc.);
- accedere liberamente presso la sede della Società, ovvero convocare, qualsiasi unità, esponente o dipendente della Società – senza necessità di alcun consenso preventivo - per richiedere ed acquisire informazioni, documentazione e dati, ritenuti necessari per lo svolgimento dei compiti previsti dal Decreto, da tutto il personale dirigente e dipendente;
- raccogliere, elaborare e conservare dati ed informazioni relative all'attuazione del Modello;
- promuovere l'attivazione di eventuali procedimenti disciplinari e proporre le eventuali sanzioni di cui al presente Modello;
- in caso di controlli, indagini, richieste di informazioni da parte di autorità competenti finalizzati a verificare la rispondenza del Modello alle previsioni del Decreto, curare il rapporto con i soggetti incaricati dell'attività ispettiva, fornendo loro adeguato supporto informativo;
- sentito il parere del Collegio Sindacale, disciplinare il proprio funzionamento anche attraverso l'introduzione di un regolamento delle proprie attività che disciplini, fra l'altro, le risorse a propria disposizione, la convocazione, il voto e le decisioni dell'Organismo stesso[14];

[14] Si veda in proposito quanto stabilito dalla Circolare di Confindustria del 12 Gennaio 2005, n. 18237

- sentito il parere del Collegio Sindacale, adottare su base semestrale un programma delle proprie attività, con particolare riferimento alle verifiche da svolgere, i cui risultati sono riferiti agli organi di amministrazione e controllo ai sensi del successivo paragrafo 3.10.3.

Il Consiglio di Amministrazione di Huawei cura l'adeguata e tempestiva comunicazione alle strutture aziendali dei poteri e delle funzioni dell'Organismo di Vigilanza, stabilendo espressamente specifiche sanzioni disciplinari in caso di mancata collaborazione nei confronti dell'Organismo stesso, secondo quanto meglio precisato nei paragrafi che seguono[15].

Il Consiglio di Amministrazione adotta forme di tutela nei confronti dell'Organismo per evitare rischi di ritorsioni, comportamenti discriminatori o comunque condotte pregiudizievoli nei suoi confronti per l'attività svolta.

3.10 Obblighi di informazione all'Organismo di Huawei

3.10.1 Obblighi generali

Il corretto ed efficiente espletamento delle proprie funzioni da parte dell'Organismo si basa sulla disponibilità, da parte dello stesso, di tutte le informazioni relative alle aree a rischio nonché di tutti i dati concernenti condotte funzionali alla commissione di reato. Per tale motivo, all'Organismo di Huawei deve essere dato accesso a tutti i dati e le informazioni sopra menzionate relative alla Società.

All'interno di Huawei, i soggetti in posizione apicale ed i loro sottoposti saranno tenuti a comunicare all'Organismo di Huawei:

- le informazioni e la documentazione prescritta nella Parte Speciale del presente Modello con riferimento alle singole fattispecie di reato ivi previste;
- tutte le condotte che risultino in contrasto o in difformità o comunque non in linea con le previsioni del presente Modello;
- tutte le notizie utili in relazione alla effettiva attuazione del presente Modello, a tutti i livelli aziendali;
- ogni altra notizia o informazione relativa all'attività della Società nelle aree a rischio, che l'Organismo ritenga, di volta in volta, di acquisire.

Le segnalazioni di condotte non conformi al presente Modello dovranno avere ad oggetto ogni violazione o sospetto di violazione del Modello. L'Organismo agirà in modo da garantire i segnalanti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, assicurando altresì la riservatezza dell'identità del segnalante, fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede.

Le suddette segnalazioni dovranno essere effettuate esclusivamente attraverso uno o più "canali informativi dedicati" che saranno istituiti da Huawei, con le modalità di volta in volta stabilite e comunicate, con la funzione di facilitare il flusso di segnalazioni e informazioni verso l'Organismo e di ricevere tempestivamente dall'Organismo eventuali chiarimenti.

Gli obblighi di informazione su eventuali comportamenti contrari alle disposizioni contenute nel Modello rientrano nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro di cui agli artt. 2104 e 2105 c.c. Il corretto adempimento dell'obbligo di informazione da parte del prestatore di lavoro non può, pertanto, dar luogo all'applicazione di sanzioni disciplinari.[16]

[15] Si veda in proposito quanto stabilito dalla Circolare di Confindustria del 12 Gennaio 2005, n. 18237.

[16] *"Mediante la regolamentazione delle modalità di adempimento all'obbligo di informazione non si intende incentivare il fenomeno del riporto dei c.d.* rumors *interni (*whistleblowing*), ma piuttosto realizzare quel sistema di* reporting *di fatti e/o comportamenti reali che non segue la linea gerarchica e che consente al personale di*

3.10.2 Obblighi specifici

In aggiunta alle segnalazioni relative a violazioni di carattere generale sopra descritte, i Responsabili e gli Esponenti Aziendali di Huawei sono tenuti a comunicare all'Organismo completa informativa in relazione ai seguenti fatti, sia essa relativa a se stessi ovvero agli altri Destinatari, di cui essi siano comunque a conoscenza (unitamente a copia della documentazione di supporto, se ad essi disponibile o accessibile e, se indisponibile o inaccessibile, unitamente all'indicazione di dove e come tale documentazione è o si presume possa ragionevolmente essere ottenuta):

- 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 di cui al Decreto;
- richieste di assistenza legale inoltrate da Destinatari in caso di avvio di procedimento giudiziario per i reati rilevanti ai fini del Decreto, salvo espresso divieto dell'autorità giudiziaria;
- rapporti preparati dai responsabili di altre funzioni aziendali nell'ambito della loro attività di controllo e dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- le decisioni relative alla richiesta, erogazione ed utilizzazione di finanziamenti pubblici;
- le decisioni relative alla richiesta ed ottenimento di permessi e autorizzazioni rilasciate dalla pubblica amministrazione o da enti pubblici;
- i prospetti riepilogativi degli appalti affidati alla Società a seguito di gare a livello nazionale, europeo o di trattativa privata ovvero notizie relative a commesse attribuite da enti pubblici che svolgano funzioni di pubblica utilità.

I Collaboratori e Dipendenti di Huawei saranno tenuti a comunicare all'Organismo completa informativa (con copia della documentazione in loro possesso) in relazione ai fatti sopra indicati, se relativa a se stessi ovvero ad altri Destinatari. La documentazione di supporto, nel caso in cui non sia in possesso dei Dipendenti, è ricercata a cura dell'Organismo in forza dei suoi poteri ispettivi.

Le competenti funzioni aziendali di Huawei trasmettono tempestivamente all'Organismo completa informativa in relazione ai procedimenti svolti e alle eventuali sanzioni irrogate o agli altri provvedimenti adottati (ivi compresi i provvedimenti disciplinari verso i Dipendenti), ivi inclusi gli eventuali provvedimenti di archiviazione di tali procedimenti con le relative motivazioni.

Per quanto concerne agenti, *partners* commerciali, consulenti, collaboratori esterni, ecc., è contrattualmente previsto un obbligo di informativa immediata a loro carico nel caso in cui gli stessi ricevano, direttamente o indirettamente, da un dipendente/rappresentante della Società una richiesta di comportamenti che potrebbero determinare una violazione del Modello.

Periodicamente, l'Organismo di Huawei propone, se del caso, al Presidente della Società eventuali modifiche o integrazioni da apportare al presente paragrafo.

---

*riferire casi di violazione di norme da parte di altri all'interno dell'ente, senza timore di ritorsioni. In questo senso l'Organismo viene ad assumere anche le caratteristiche dell'*Ethic Officer*, senza - però - attribuirgli poteri disciplinari che sarà opportuno allocare in un apposito comitato o, infine, nei casi più delicati al Consiglio di amministrazione"*. Confindustria, *Linee guida*, *cit*., nella versione aggiornata al 31 marzo 2008, 46.

3.10.3 Linee di riporto

Nello svolgimento delle proprie attività, l'Organismo di Huawei riporta:

a) al Consiglio di Amministrazione ed al Collegio Sindacale della Società, su base periodica (almeno semestrale), a mezzo della presentazione di una relazione illustrativa del complesso delle attività dallo stesso svolte e dello stato di attuazione del Modello;

b) al Presidente del Consiglio di Amministrazione e al General Manager della Società, su base continuativa, mediante la presentazione di rapporti scritti, concernenti aspetti puntuali e specifici della propria attività, ritenuti di particolare rilievo e significato nel contesto dell'attività di prevenzione e controllo (ad esempio, eventuali violazioni del Modello segnalate e/o riscontrate).

L'Organismo di Huawei potrà inoltre essere convocato dagli organi sopra menzionati ogni qualvolta sia dagli stessi ritenuto opportuno, per riportare in merito a specifici fatti od accadimenti o per discutere di argomenti ritenuti di particolare rilievo nel contesto della funzione di prevenzione di reati.

Inoltre, l'Organismo di Huawei potrà riferire agli organi sopra menzionati specifici fatti od accadimenti, ogni qualvolta lo ritenga opportuno.

Di regola, in caso di violazione del Modello da parte di uno dei membri del Consiglio di Amministrazione o del Collegio Sindacale, l'Organismo riporta a tali organi per l'adozione di adeguati provvedimenti, in conformità al successivo paragrafo 5.3.1.

Peraltro, stante la necessità di garantire l'indipendenza dell'Organismo, laddove esso ritenga che per circostanze gravi e comprovabili sia necessario riportare direttamente all'Assemblea della Società informazioni che riguardano violazioni del Modello da parte dei membri del Consiglio di Amministrazione o del Collegio Sindacale[17], esso, o ciascuno dei suoi componenti, è autorizzato, mediante richiesta al Presidente del Consiglio di Amministrazione (o, in caso di assenza, impedimento o coinvolgimento di quest'ultimo, al Presidente del Collegio Sindacale) ad essere ammesso a partecipare alla prima Assemblea utile, al fine di riferire ai soci, ovvero, in casi di straordinaria gravità e urgenza, di esigere la convocazione senza indugio di una apposita Assemblea.

3.10.4 Verifiche

Il presente Modello è soggetto, tra le altre, alle seguenti verifiche, che saranno condotte dall'Organismo di Huawei con la cooperazione delle funzioni aziendali competenti:

(i) *verifiche degli atti*: l'Organismo di Huawei procede su base semestrale alla verifica dei principali atti societari (ivi inclusi gli atti ed attività riferibili al "*datore di lavoro*") e dei contratti di maggior rilevanza conclusi dalla Società in aree di attività a rischio, secondo i criteri da esso stabiliti.

(ii) *verifiche delle procedure*: l'Organismo di Huawei procede alla costante verifica dell'efficace attuazione e dell'effettivo funzionamento del Modello. Su base semestrale, l'Organismo di Huawei valuta, nel loro complesso, tutte le segnalazioni ricevute nel corso del semestre, le azioni intraprese in relazione a tali segnalazioni e gli eventi considerati rischiosi, con la collaborazione delle funzioni di volta in volta competenti.

[17] Sebbene i sindaci non possano essere considerati - in linea di principio - soggetti in posizione apicale, come affermato dalla stessa Relazione illustrativa del Decreto (pag. 7), tuttavia è astrattamente ipotizzabile il coinvolgimento, anche indiretto, degli stessi sindaci nella commissione dei reati di cui al d.lgs. 231/2001 (eventualmente a titolo di concorso con soggetti in posizione apicale).

L'Organismo di Huawei illustra analiticamente le suddette verifiche, indicando i metodi adottati ed i risultati ottenuti, nella propria relazione periodica al Consiglio di Amministrazione della Società.

CAPITOLO 4
PIANO DI FORMAZIONE E COMUNICAZIONE

4.1 Selezione e formazione del personale

4.1.1 Sistema di formazione

Con riferimento a Huawei, l'efficacia e l'effettività del presente Modello richiedono che lo stesso sia conosciuto ed attuato dai soggetti apicali della Società e dai loro sottoposti e, in particolare, dal personale della Società, a tutti i livelli.

A tal fine, l'attività di comunicazione e formazione, diversificata e tarata a seconda dei Destinatari cui essa si rivolge e dei livelli e delle funzioni dagli stessi rivestiti, è, in ogni caso, improntata a principi di completezza, chiarezza, accessibilità e continuità al fine di consentire ai diversi destinatari la piena consapevolezza di quelle disposizioni aziendali che sono tenuti a rispettare e delle norme etiche che devono ispirare i loro comportamenti.

L'attività di comunicazione e formazione è supervisionata ed integrata dall'Organismo di Vigilanza, con la collaborazione delle funzioni aziendali competenti, al quale sono assegnati, tra gli altri, i compiti di promuovere e definire le iniziative per la diffusione della conoscenza e della comprensione del Modello, nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei contenuti del Modello e di promuovere ed elaborare interventi di comunicazione e formazione sui contenuti del Decreto, sui contenuti del Sistema di Gestione HSE e dell'ISMS, sulla normativa che regolamenta l'attività dell'azienda e sulle norme comportamentali.

In particolare, la funzione cui fa capo la gestione delle risorse umane, in coordinamento con l'Organismo:

a) inserisce, tra i criteri di selezione del personale, la condivisione dei valori espressi dal presente Modello e la predisposizione ad osservare gli stessi;

b) diffonde la conoscenza del presente Modello attraverso i seguenti momenti formativi:

- Responsabili ed altri Dipendenti con funzioni di rappresentanza o poteri di firma ad efficacia esterna:
  - seminario iniziale (esteso annualmente a tutti i neo-assunti, in gruppo o individualmente a seconda del caso);
  - informativa nella lettera di assunzione per i neo-assunti con obbligo per gli stessi, di sottoscrivere una dichiarazione di osservanza dei contenuti del Modello ivi descritti, di cui il Sistema di Gestione HSE e l'ISMS costituiscono parte integrante;
  - seminari di aggiornamento;
  - comunicazioni occasionali di aggiornamento in caso di necessità o urgenza anche tramite collocazione di tali comunicazioni in apposita sezione del sito intranet aziendale, se disponibile, dedicato all'argomento e aggiornato dall'Organismo;
- Altri Dipendenti e Collaboratori:
  - nota informativa interna;
  - informativa nella lettera di assunzione per i neo-assunti;
  - comunicazioni occasionali di aggiornamento in caso di necessità o urgenza anche tramite collocazione di tali comunicazioni in apposita sezione del sito intranet aziendale, se disponibile, dedicato all'argomento e aggiornato dall'Organismo.

Fermo quanto precede, ogni Dipendente ha l'obbligo di: i) acquisire consapevolezza dei contenuti del Modello e partecipare - con obbligo di frequenza - ai momenti formativi organizzati dalla Società; ii) conoscere le modalità operative con le quali deve essere realizzata la propria attività; iii) contribuire attivamente, in relazione al proprio ruolo e alle proprie responsabilità, all'efficace attuazione del Modello, segnalando eventuali carenze riscontrate nello stesso.

La qualità dei momenti di formazione è perseguita dalla Società che, all'uopo, si deve avvalere di tutori esperti in materie giuridiche e organizzative attinenti al Decreto, la cui competenza è attestata dalla relativa documentazione curriculare soggetta a verifica dell'Organismo di Vigilanza in via preventiva.

A tali fini, ai Dipendenti e ai Collaboratori è garantita la possibilità di accedere e consultare la documentazione costituente il Modello anche direttamente sull'intranet aziendale, ove disponibile.

Ogni Dipendente e Collaboratore deve, inoltre, poter ottenere una copia cartacea del Modello. Inoltre, al fine di agevolare la comprensione del Modello, i Dipendenti e i Collaboratori, con modalità diversificate secondo il loro grado di coinvolgimento nelle attività individuate come sensibili ai sensi del d.lgs. 231/2001, sono tenuti a partecipare ad una specifica attività formativa.

Ai nuovi Dipendenti verrà consegnata, all'atto dell'assunzione, copia del Documento descrittivo del Modello e del Business Code of Conduct e sarà fatta loro sottoscrivere dichiarazione di osservanza dei contenuti ivi descritti.

Ai componenti degli organi sociali di Huawei sarà resa disponibile copia cartacea della versione integrale del Modello. Analogamente a quanto previsto per i Dipendenti, ai nuovi componenti degli organi sociali sarà consegnata copia cartacea della versione integrale del Modello al momento dell'accettazione della carica loro conferita e sarà fatta loro sottoscrivere dichiarazione di osservanza dei contenuti del Modello stesso.

Idonei strumenti di comunicazione saranno adottati per aggiornare i Dipendenti circa le eventuali modifiche apportate al Modello, nonché ogni rilevante cambiamento procedurale, normativo o organizzativo. Analoghe misure sono adottate in relazione ai Collaboratori.

4.1.2 Programma di formazione

La conoscenza da parte di tutti i Dipendenti e Collaboratori di Huawei, dei principi, delle disposizioni, delle procedure e dei documenti richiamati nel Modello rappresentano elementi di primaria importanza per l'efficace attuazione del Modello medesimo.

Huawei persegue, attraverso un adeguato programma di formazione rivolto a tutti i Dipendenti e Collaboratori, una loro sensibilizzazione continua sulle problematiche attinenti al Modello, al fine di consentire ai destinatari di detta formazione di raggiungere la piena consapevolezza delle direttive aziendali e di essere posti in condizioni di rispettarle in pieno.

La Società predispone, con il supporto di consulenti esterni con specifiche competenze in materia di responsabilità amministrativa degli enti, interventi formativi rivolti a tutti i dipendenti al fine di assicurare una adeguata conoscenza, comprensione e diffusione dei contenuti del Modello e di diffondere, altresì, una cultura aziendale orientata verso il perseguimento di una sempre maggiore trasparenza ed eticità.

Gli interventi formativi prevedono i seguenti contenuti:

- una parte generale avente ad oggetto il quadro normativo di riferimento (d.lgs. 231/2001 e reati ed illeciti amministrativi rilevanti ai fini della responsabilità amministrativa degli enti), il Modello (elementi costitutivi, Organismo di Vigilanza, sistema disciplinare, Codice Etico, ecc.) e i contenuti del Sistema di Gestione HSE e dell'ISMS;

- una parte speciale avente ad oggetto le attività individuate come sensibili (o strumentali) ai sensi del d.lgs. 231/2001 e i protocolli di controllo relativi a dette attività;
- una verifica del grado di apprendimento della formazione ricevuta.

L'attività formativa viene erogata attraverso le seguenti modalità:

- sessioni in aula, con incontri dedicati oppure mediante l'introduzione di moduli specifici nell'ambito di altre sessioni formative, a seconda dei contenuti e dei destinatari di queste ultime, con questionari di verifica del grado di apprendimento;
- *e-learning*: attraverso un modulo relativo alla Parte Generale per tutti i dipendenti, con esercitazioni intermedie e test di verifica di apprendimento.

I contenuti degli interventi formativi vengono costantemente aggiornati in relazione ad eventuali interventi di aggiornamento e/o adeguamento del Modello.

La partecipazione agli interventi formativi è obbligatoria. L'Organismo di Vigilanza raccoglie e archivia le evidenze/attestazioni relative all'effettiva partecipazione a detti interventi formativi.

4.2 Selezione e formazione di Consulenti e Partners

L'effettività del presente Modello può essere inficiata dall'instaurazione di rapporti di collaborazione o commerciali con soggetti estranei agli obiettivi ed ai valori da esso previsti.

In particolare, obiettivo di Huawei è estendere la comunicazione dei contenuti del Modello non solo ai propri Dipendenti ma anche ai soggetti che, pur non rivestendo la qualifica formale di dipendente, operano – anche occasionalmente – per il conseguimento degli obiettivi di Huawei in forza di rapporti contrattuali.

A tal fine, Huawei adotta criteri di selezione di Consulenti e di Partners volti a favorire il rispetto e l'attuazione del presente Modello e comunica ai suddetti Consulenti e Partners le procedure e i criteri adottati dalla Società. Ai Consulenti e Partners sarà, inoltre, fatta sottoscrivere una dichiarazione con la quale gli stessi attestino di essere a conoscenza del Modello adottato dalla Società e degli obblighi dallo stesso derivanti oltre che l'impegno, da parte degli stessi, ad osservare i contenuti del Modello ad essi applicabili.

4.3 Altri destinatari

L'attività di comunicazione dei contenuti del Modello è indirizzata anche nei confronti di quei soggetti terzi che intrattengano con Huawei rapporti di collaborazione contrattualmente regolati o che rappresentano la Società senza vincoli di dipendenza e che, sia pure non rientranti nelle categorie di Consulenti o Partners, svolgano attività di rilievo nelle aree a rischio.

A tal fine, ai soggetti terzi più significativi Huawei fornirà un estratto del Documento descrittivo del Modello ed il Business Code of Conduct. Ai terzi cui sarà consegnato l'estratto del Documento descrittivo del Modello ed il Business Code of Conduct, verrà fatta sottoscrivere una dichiarazione che attesti il ricevimento di tali documenti e l'impegno all'osservanza dei contenuti ivi descritti.

Huawei, tenuto conto delle finalità del Modello, valuterà l'opportunità di comunicare i contenuti del Modello stesso a terzi, non riconducibili alle figure sopra indicate a titolo esemplificativo, e più in generale al mercato.

CAPITOLO 5
SISTEMA DISCIPLINARE

5.1 Sanzioni nei confronti dei dipendenti

Aspetto essenziale per l'effettività del Modello è costituito, ai sensi di quanto previsto dall'articolo 6, comma 2, lettera e) e dall'articolo 7, comma 4, lettera b) del Decreto, dalla predisposizione di un adeguato sistema sanzionatorio per la violazione delle regole di condotta imposte ai fini della prevenzione dei reati di cui al Decreto, e, in generale, delle procedure ed istruzioni interne previste dal Modello stesso.

Con specifico riferimento ai reati in materia di salute e sicurezza sul lavoro, si osserva inoltre come sia lo stesso comma 3 dell'art. 30 del d.lgs. 81/2008 a richiedere che il Modello preveda *"un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello"*.

Per quanto riguarda Huawei, al fine di incentivare il rispetto e di promuovere l'attuazione del presente Modello, è predisposto un sistema disciplinare, volto a sanzionare le condotte ed i comportamenti in contrasto con le disposizioni in esso contenute.

L'osservanza delle disposizioni e delle regole comportamentali previste dal Modello costituisce adempimento da parte dei dipendenti di Huawei degli obblighi previsti dall'art. 2104, comma 2, c.c.; obblighi dei quali il contenuto del medesimo Modello rappresenta parte sostanziale ed integrante.

I comportamenti tenuti dai dipendenti in violazione delle disposizioni del presente Modello costituiscono, pertanto, illeciti disciplinari; la commissione di illeciti disciplinari è sanzionata dalla Società mediante l'applicazione di sanzioni, nel rispetto delle procedure previste dall'articolo 7 della legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori) e delle disposizioni del contratto collettivo di lavoro applicabile, in particolare allorquando si tratti di comminare una sanzione più grave del richiamo verbale.

Poiché le regole di condotta previste dal presente Modello sono assunte da Huawei in piena autonomia rispetto ai profili di illiceità eventualmente conseguenti alle condotte stesse, l'applicazione delle sanzioni disciplinari prescinde dall'esito dei procedimenti penali eventualmente iniziati nei confronti dei dipendenti[18].

Huawei rinvia, per la disciplina dei rapporti con i propri dipendenti, al contratto collettivo nazionale di lavoro per il personale dipendente da imprese esercenti servizi di telecomunicazione (di seguito, "CCNL").

Di seguito, si riportano le **norme di legge applicabili**:

Art. 2104 Codice Civile – Diligenza del prestatore di lavoro

Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse dell'impresa e da quello superiore della produzione nazionale.

[18] "*La valutazione disciplinare dei comportamenti effettuata dai datori di lavoro, salvo, naturalmente, il successivo eventuale controllo del giudice del lavoro, non deve, infatti, necessariamente coincidere con la valutazione del giudice in sede penale, data l'autonomia della violazione del codice etico e delle procedure interne rispetto alla violazione di legge che comporta la commissione di un reato. Il datore di lavoro non è tenuto quindi, prima di agire, ad attendere il termine del procedimento penale eventualmente in corso. I principi di tempestività ed immediatezza della sanzione rendono infatti non soltanto non doveroso, ma altresì sconsigliabile ritardare l'irrogazione della sanzione disciplinare in attesa dell'esito del giudizio eventualmente instaurato davanti al giudice penale*". Confindustria, *Linee guida*, *cit*., nella versione aggiornata al 31 marzo 2008, 30.

Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende.

Art.2105 Codice Civile – Obbligo di fedeltà'

Il prestatore di lavoro non deve trattare affari, per conto proprio o di terzi, in concorrenza con l'imprenditore, nè divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da poter recare ad essa pregiudizio.

Art. 2106 Codice Civile – Sanzioni disciplinari

La inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo all'applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione.

Art. 7, comma 1, Legge 20 maggio 1970, n. 300

Le norme disciplinari relative alle sanzioni alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alla procedura di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro ove esistano.

Norme estratte dal Contratto Collettivo Nazionale di Lavoro per le Imprese Esercenti Servizi di telecomunicazione attualmente in vigore:

Art. 7 – Reclami e controversie

1. Ferme restando le possibilità di accordo diretto tra le Parti interessate per eventuali reclami nell'applicazione del presente contratto, le controversie individuali e collettive tra azienda e lavoratori saranno risolte possibilmente in prima istanza tra la Direzione e la RSU e, in difetto di accordo, dalle rispettive competenti Organizzazioni sindacali.

(omissis)

Art. 36 - Trattamento in caso di malattia e infortunio non sul lavoro

1. Il lavoratore impossibilitato a presentarsi in servizio a causa di malattia deve darne tempestivamente avviso all'azienda entro il primo giorno in cui si è verificata l'assenza e, comunque, di norma, in anticipo rispetto all'inizio del proprio orario/turno di lavoro; sono fatte salve situazioni di comprovati motivi di carattere eccezionale. Contestualmente deve comunicare il luogo ove si trovi degente, se diverso dal domicilio, nonché eventuali variazioni successive del luogo stesso espressamente autorizzate dal medico.

2. Il lavoratore, inoltre, deve giustificare l'assenza facendo pervenire all'azienda il numero di protocollo identificativo del certificato inviato dal medico in via telematica entro il secondo giorno dall'inizio dell'assenza stessa. La comunicazione del numero di protocollo dovrà avvenire mediante l'utilizzo di posta elettronica o sms o con le modalità che potranno essere concordate a livello aziendale. In caso di mancata trasmissione telematica del certificato di malattia per qualsiasi motivo (quale a mero titolo esemplificativo medico o struttura curante non convenzionati con il SSN, eventi di malattia che richiedono ricovero ospedaliero o che vengono certificati da strutture di pronto soccorso, problemi tecnici di trasmissione del certificato telematico, insorgenza dello stato patologico all'estero) il lavoratore dovrà far pervenire all'azienda, entro il secondo giorno, la certificazione che il medico è tenuto a rilasciare su supporto cartaceo attestante la prognosi e la data di inizio della malattia. In questo caso, l'inoltro della certificazione medica potrà avvenire anche mediante l'utilizzo di fax o di posta elettronica, fermo restando, in tal caso, l'obbligo della successiva produzione della certificazione in originale.

3. Nel solo caso di mancata trasmissione telematica del certificato di malattia ed esclusivamente per le assenze dal servizio per malattia di durata non superiore ai tre giorni, ferma restando la comunicazione preventiva di cui al comma 1, il lavoratore potrà produrre la certificazione medica in originale al rientro in servizio.

4. In caso di prosecuzione dell'assenza per malattia il lavoratore, fermo restando l'obbligo di darne avviso, nei termini di cui sopra, all'azienda entro il primo giorno in cui egli avrebbe dovuto riprendere il servizio, dovrà inviare all'azienda il numero di protocollo identificativo del nuovo certificato ovvero far pervenire la relativa certificazione cartacea secondo le modalità sopra elencate entro il secondo giorno dalla scadenza del periodo di assenza indicato nel precedente certificato medico.

5. Il lavoratore è tenuto a comunicare all'azienda la durata della prognosi contestualmente al rilascio dei certificati di cui sopra.

6. In mancanza di ciascuna delle comunicazioni di cui ai precedenti punti da 1 a 4 nonché in caso di ritardo nella giustificazione dell'assenza, saranno considerate assenze ingiustificate le giornate non coperte da certificazione medica e quelle di ritardo nella comunicazione e nell'invio o nel recapito della certificazione.

7. In caso di assenza per malattia, l'azienda ha facoltà di far controllare lo stato di salute del lavoratore ai sensi delle vigenti norme di legge.

8. Fermo restando quanto previsto dalle vigenti leggi in materia, il lavoratore, pur in presenza di una espressa autorizzazione del medico curante ad uscire, è tenuto, fin dal primo giorno di assenza dal lavoro e per tutta la durata della malattia, a farsi trovare a disposizione nel domicilio comunicato all'azienda, dalle ore 10 alle ore 12 e dalle ore 17 alle ore 19, ovvero nelle diverse fasce orarie stabilite da norme legislative o amministrative locali o nazionali, di tutti i giorni, compresi quelli domenicali o festivi, per consentire l'accertamento del suo stato di salute.

9. Salvo casi di forza maggiore debitamente documentati il lavoratore, qualora debba allontanarsi durante le fasce di reperibilità dal luogo di degenza per prestazioni indilazionabili o accertamenti specialistici inerenti lo stato di malattia ovvero per altri gravi motivi, è tenuto a darne preventiva comunicazione all'azienda e successiva documentazione giustificativa.

(omissis)

16. Il mancato rispetto da parte del lavoratore degli obblighi indicati nel presente articolo potrà comportare, indipendentemente dalla perdita del trattamento di malattia con le modalità previste dalla legge vigente, l'adozione di provvedimenti disciplinari con la procedura di cui all'art. 46 (Provvedimenti disciplinari) del presente contratto.

Art. 45 – Rapporti in azienda

1. Le caratteristiche proprie del servizio fornito dalle imprese di gestione di reti e servizi di telecomunicazioni richiedono un elevato livello di collaborazione e senso di responsabilità da parte dei lavoratori nell'espletamento dei compiti loro affidati. In tale quadro, pertanto, tenuto soprattutto conto dell'esigenza di garantire alla clientela il miglior grado di servizio, i rapporti in azienda dovranno ispirarsi ai seguenti principi.

2. In armonia con la dignità del lavoratore i superiori improntеranno i rapporti con i dipendenti a sensi di collaborazione e urbanità.

3. Nell'ambito del rapporto di lavoro, il lavoratore dipende dai rispettivi superiori, come previsto dall'organizzazione aziendale.

4. I rapporti tra i lavoratori, a tutti i livelli di responsabilità nell'organizzazione aziendale, saranno improntati a reciproca correttezza ed educazione.

5. Dovranno essere osservate le norme di legge e del presente contratto, i regolamenti aziendali e le disposizioni di servizio ed in particolare l'attività lavorativa assegnata andrà eseguita con la diligenza, la professionalità e l'impegno necessari per assicurare il raggiungimento degli obiettivi aziendali.

6. Il lavoratore che è anche cliente dell'azienda in cui lavora è tenuto a gestire le pratiche connesse alle utenze di proprio interesse nella più assoluta trasparenza e nel rispetto delle procedure chiedendo le necessarie autorizzazioni.

7. Il lavoratore deve osservare l'orario di lavoro ed adempiere alle formalità prescritte dall'azienda per il controllo delle presenze con espresso divieto di fare variazioni o cancellature sulla scheda/badge, di ritirare quella di un altro lavoratore o di tentare in qualsiasi modo di alterare le indicazioni dell'orologio controllo, nonché di compiere volontariamente movimenti irregolari degli strumenti di controllo delle presenze.

8. Il lavoratore che non avrà fatto il regolare movimento della scheda/badge sarà considerato ritardatario e quando non possa far constatare in modo sicuro la sua presenza nel luogo di lavoro sarà considerato assente.

9. Si dovrà mantenere assoluta segretezza sugli interessi dell'azienda ed il più stretto riserbo, anche successivamente alla cessazione dal servizio, su notizie e dati riservati riconducibili alla sfera di interessi dell'azienda.

10. Il lavoratore non dovrà trarre profitto, anche a prescindere da eventuali danni causati all'azienda stessa, da quanto forma oggetto delle sue funzioni né esplicare direttamente o per interposta persona, anche fuori dall'orario di lavoro, mansioni ed attività - a titolo gratuito od oneroso - che possano determinare, anche indirettamente, un conflitto di interessi con l'Azienda; in particolare dovrà astenersi da qualunque attività o da qualsiasi forma di partecipazione, diretta o indiretta, in imprese od organizzazioni di fornitori, clienti, concorrenti e distributori.

11. Durante l'orario giornaliero il lavoratore dovrà disimpegnare con assiduità e diligenza i compiti attribuitigli, mantenere nei rapporti con la clientela una condotta uniformata a principi di correttezza e di integrità, non attendere ad occupazioni estranee al servizio e, in periodo di malattia od infortunio, ad attività lavorativa ancorché non remunerata.

12. I lavoratori non dovranno sottrarre o danneggiare i beni materiali o immateriali in proprietà o in uso alla azienda compreso il patrimonio informatico. Inoltre non dovranno falsificare o alterare dati, documenti, apparecchiature, procedure o software aziendali né duplicare, installare e/o detenere programmi ed ogni altro prodotto software senza esplicita autorizzazione.

13. Non è possibile valersi di mezzi di comunicazione, di strumenti informatici, di collegamenti in rete o di quant'altro ancora è di proprietà o in uso dell'azienda per ragioni che non siano di servizio.

14. Dovranno essere scrupolosamente osservate le disposizioni che regolano l'accesso ai locali dell'azienda da parte del personale e non potranno essere introdotte - salvo che non siano debitamente autorizzate - persone estranee nei locali non aperti al pubblico.

15. Nei confronti di colleghi, clienti e terzi, i lavoratori dovranno attenersi a comportamenti improntati al massimo rispetto della condizione sessuale, della dignità e del diritto della persona e conseguentemente astenersi dal porre in essere comportamenti riconducibili a forme di molestie sessuali anche perpetrate deliberatamente in ragione della posizione ricoperta.

16. Le infrazioni a tali disposizioni come previsto nei successivi artt. 46 e 47 daranno luogo a provvedimenti disciplinari che potranno giungere fino al licenziamento per mancanze ai sensi dell'art. 48.

17. Quando sia richiesto dalla natura del comportamento del lavoratore o dalla necessità di effettuare accertamenti in relazione al comportamento medesimo, l'azienda può disporre l'allontanamento temporaneo del lavoratore dal servizio.

Art. 46 – Provvedimenti disciplinari

1. L'inosservanza, da parte del lavoratore, delle disposizioni di legge, contrattuali o di normativa aziendale può dar luogo, secondo la gravità della infrazione, all'applicazione dei seguenti provvedimenti:

a) richiamo verbale;

b) ammonizione scritta;

c) multa non superiore a tre ore della retribuzione base;

d) sospensione dal lavoro e dalla retribuzione fino ad un massimo di tre giorni;

e) licenziamento per mancanze ai sensi del successivo art. 48.

2. Il datore di lavoro non potrà adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.

3. Salvo che per il richiamo verbale, la contestazione dovrà essere effettuata per iscritto ed i provvedimenti disciplinari non potranno essere applicati prima che siano trascorsi cinque giorni nel corso dei quali il lavoratore potrà presentare le sue giustificazioni.

4. Se il provvedimento non verrà comunicato entro i dieci giorni dalla scadenza del termine assegnato per presentare le giustificazioni, queste si riterranno accolte.

5. Il lavoratore potrà presentare le sue giustificazioni anche verbalmente, con l'eventuale assistenza di un rappresentante dell'Associazione Sindacale cui aderisce o conferisce mandato, ovvero di un componente la RSU.

6. La adozione del provvedimento dovrà essere motivata e comunicata per iscritto.

7. I provvedimenti disciplinari di cui sopra alle lettere b), c) e d) potranno essere impugnati dal lavoratore in sede sindacale, secondo le norme contrattuali relative alle controversie individuali (cfr. art. 7 Reclami e controversie).

8. Il licenziamento per mancanze di cui al successivo art. 48 potrà essere impugnato secondo le procedure previste dalle vigenti norme di legge.

9. Non si terrà conto a nessun effetto dei provvedimenti disciplinari decorsi due anni dalla loro applicazione.

Art. 47 – Ammonizioni, multe e sospensioni

1. Incorre nei provvedimenti di ammonizione scritta, multa o sospensione il lavoratore che:

a) non si presenti in servizio o abbandoni il proprio posto di lavoro senza giustificato motivo, oppure non giustifichi l'assenza entro il giorno successivo a quello di inizio dell'assenza stessa salvo il caso di impedimento giustificato;

b) senza giustificato motivo ritardi l'inizio del lavoro o lo sospenda o ne anticipi la cessazione;

c) non osservi una condotta uniformata a principi di correttezza verso i colleghi e/o compia lieve insubordinazione nei confronti dei superiori;

d) non mantenga nei rapporti con i clienti o con i fornitori condotta uniformata a principi di correttezza;

e) esegua negligentemente il lavoro affidatogli e/o arrechi per colpa danni a tutto quanto forma oggetto del patrimonio di beni e servizi dell'azienda;

f) esegua all'interno dell'azienda attività di lieve entità per conto proprio o di terzi fuori dell'orario di lavoro e senza sottrazione, ma con uso di mezzi dell'azienda medesima;

g) introduca persone non autorizzate in locali aziendali;

h) durante l'orario di lavoro venga trovato in stato di manifesta ubriachezza o sotto l'effetto di sostanze stupefacenti;

i) contravvenga al divieto di fumare laddove questo esista e sia indicato da apposito cartello;

2. L'ammonizione verrà applicata per le mancanze di minor rilievo. La multa e la sospensione per quelle di maggior rilievo.

3. L'elencazione sopra riportata deve intendersi a titolo esemplificativo e non esaustivo facendo salvo il principio dell'analogia per quanto applicabile.

4. L'importo delle multe che non costituiscono risarcimento di danni è devoluto alle istituzioni assistenziali e previdenziali di carattere aziendale o, in mancanza di queste, all'Istituto assicuratore.

Art. 48 – Licenziamento per mancanze

A) LICENZIAMENTO CON PREAVVISO

1. In tale provvedimento incorre il lavoratore che commetta infrazioni alla disciplina ed alla diligenza del lavoro che, pur essendo di maggior rilievo di quelle contemplate nell'art. 47 (ammonizioni scritte, multe e sospensioni), non siano così gravi da rendere applicabile la sanzione di cui alla seguente lettera B.

2. A titolo indicativo rientrano nelle infrazioni di cui sopra:

a) l'insubordinazione ai superiori;

b) la rissa nel luogo di lavoro, fuori dai reparti operativi;

c) i danni rilevanti arrecati per colpa grave a tutto quanto forma oggetto del patrimonio di beni e

servizi dell'azienda;

d) l'assenza ingiustificata per un periodo superiore a 4 giorni consecutivi o ripetuta per 3 volte in un

anno nel giorno seguente alle festività o alle ferie;

e) l'abbandono del posto di lavoro da parte del personale addetto a mansioni di sorveglianza, custodia e controllo, al di fuori delle ipotesi previste dal punto e) della lettera B;

f) l'utilizzo di prodotti "software" o altri mezzi in uso all'azienda per eseguire attività connesse a finalità personali dalle quali derivi direttamente o indirettamente un lucro per il lavoratore e/o un danno per l'azienda;

g) i comportamenti lesivi della dignità della persona in ragione della condizione sessuale;

h) la recidiva in qualunque delle mancanze contemplate nell'art. 47, qualora siano stati applicati due provvedimenti di sospensione nell'ambito del biennio precedente;

i) la condanna ad una pena detentiva con sentenza passata in giudicato, per azione commessa non in connessione con lo svolgimento del rapporto di lavoro, che leda la figura morale del lavoratore;

B) LICENZIAMENTO SENZA PREAVVISO

3. In tale provvedimento incorre il lavoratore che provochi all'azienda grave nocumento morale o materiale o che compia, in connessione con lo svolgimento del rapporto di lavoro, azioni che costituiscono delitto a termine di legge.

4. A titolo indicativo rientrano nelle infrazioni di cui sopra:

a) la grave insubordinazione ai superiori;

b) la rissa nel luogo di lavoro, all'interno dei reparti operativi;

c) i danni rilevanti arrecati per dolo a tutto quanto forma oggetto del patrimonio di beni, e servizi dell'azienda;

d) la sottrazione, la manomissione o la distruzione intenzionali di tutto quanto forma oggetto del patrimonio materiale e/o immateriale dell'azienda;

e) l'abbandono ingiustificato del posto di lavoro, da cui possa derivare un pregiudizio alla incolumità delle persone od alla sicurezza degli impianti o comunque compimento di azioni che implichino gli stessi pregiudizi;

f) il furto in azienda;

g) lo svolgimento, a titolo gratuito od oneroso, di attività in contrasto o in concorrenza anche indiretta con l'azienda, ivi compresa qualunque forma di partecipazione in imprese od organizzazioni di fornitori, clienti, concorrenti o distributori;

h) lo svolgimento di altra attività lavorativa, ancorché non remunerata, in dichiarato stato di malattia o di infortunio;

i) la richiesta o l'accettazione, a qualsiasi titolo, di compensi di carattere economico in connessione agli adempimenti della prestazione lavorativa;

l) la violazione del segreto sugli interessi dell'azienda, del segreto telefonico e/o di quello delle comunicazioni come definiti dalla vigente legislazione penale (titolo XII, libro II, capo III, sez. V, del Codice Penale);

m) l'introduzione di persone non autorizzate in locali aziendali allorquando da tale comportamento derivi un grave pregiudizio all'azienda;

n) fumare dove ciò può provocare pregiudizio alla incolumità delle persone od alla sicurezza degli impianti;

o) il compimento di comportamenti lesivi della dignità della persona, in ragione della condizione sessuale, riconducibili alla sfera del rapporto gerarchico;

p) visualizzare il traffico telefonico dei clienti, qualora ciò non sia riconducibile all'ordinario svolgimento dell'attività lavorativa (in coerenza con il quadro legislativo, regolatorio e con le pronunce delle Autorità garanti sulla materia).

Art. 49 – Sospensione cautelare

1. In caso di licenziamento di cui all'art. 48 (Licenziamento disciplinare), l'azienda potrà disporre la sospensione cautelare non disciplinare del lavoratore con effetto immediato, per un periodo massimo di quindici giorni.

2. Il datore di lavoro comunicherà per iscritto al lavoratore i fatti rilevanti ai fini del provvedimento e ne esaminerà le eventuali deduzioni contrarie. Ove il licenziamento venga applicato, esso avrà effetto dal momento della disposta sospensione.

Norme di Raccordo Huawei Technologies Italia S.r.l. provvedimenti disciplinari

La recidiva prevista dal punto 2, lettera h), art. 48 del vigente CCNL, ha effetto qualora il lavoratore incorra in una terza infrazione, tra quelle previste dall'art. 47 CCNL, a condizione che nell'ambito del biennio precedente siano stati applicati due provvedimenti di sospensione pari a tre giorni ciascuno (durata massima della sospensione contrattualmente prevista).

Policies aziendali. rinvio

Le policies aziendali sotto indicate con le eventuali successive modifiche ed integrazioni, hanno efficacia disciplinare ai sensi dell'art. 2104, comma 2, del codice civile:

- ✓ Attendance;
- ✓ Information Security;
- ✓ Data Protection;
- ✓ Management of relationships with Public Authorities;

- ✓ Anti Bribery (1-5);
- ✓ Fuel Expense Management;
- ✓ Beneficial Car
- ✓ Il Modello 231

Norma transitoria - *La Società curerà la traduzione in italiano delle Policies sopra indicate, entro sei mesi dalla data di entrata in vigore del presente codice-*

Il codice disciplinare aziendale – che, riportato in allegato al presente Modello, ne costituisce parte integrante – contiene le summenzionate norme di legge rilevanti in materia, le previsioni del CCNL che regolano i provvedimenti disciplinari e le policies aziendali ivi espressamente richiamate. Esso risulta l'unico riferimento giusprivatistico regolante la materia, cui fa pertanto riferimento il presente Modello al fine di sanzionare gli illeciti disciplinari derivanti dall'inosservanza delle disposizioni e delle regole comportamentali previste dal Modello stesso.

5.2 Sanzioni nei confronti dei dirigenti

In caso di violazione, da parte di Dirigenti, delle procedure ed istruzioni interne previste dal presente Modello o di adozione, nell'espletamento di attività sensibili o strumentali, di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal Contratto Collettivo Nazionale di Lavoro per dirigenti applicabile.

Se la violazione del Modello determina la sopravvenuta carenza del rapporto di fiducia tra la Società e il dirigente, la sanzione è individuata nel licenziamento per giusta causa.

5.3 Sanzioni nei confronti di altri soggetti

5.3.1 Amministratori e sindaci

Per quanto riguarda Huawei, fermo restando quanto stabilito dal precedente paragrafo 3.10.3, in caso di violazione del presente Modello da parte di alcuno degli amministratori e dei sindaci della Società, l'Organismo informa il Consiglio di Amministrazione e il Collegio Sindacale di tale violazione per l'adozione di adeguati provvedimenti, che possono consistere, in relazione alla gravità del comportamento, in:

- censura scritta a verbale;
- sospensione del diritto al gettone di presenza o alla indennità di carica fino ad un massimo corrispondente a tre riunioni dell'organo:
- segnalazione all'Assemblea per gli opportuni provvedimenti (revoca per giusta causa, azione di responsabilità, altro).

5.3.2 Consulenti e Partners

In caso di violazione del presente Modello da parte di lavoratori autonomi, fornitori, Consulenti, Partners o altro soggetto avente rapporti contrattuali con Huawei, tale da determinare il rischio di commissione di un reato sanzionato dal Decreto, l'Organismo informa le funzioni aziendali competenti per l'adozione degli opportuni provvedimenti, quali la risoluzione dei rapporti contrattuali con gli stessi o l'applicazione di penali, in conformità alle norme di legge che disciplinano i rapporti con tali soggetti e le specifiche clausole contrattuali che saranno inserite nei relativi contratti, fatta salva l'eventuale richiesta di risarcimento danni qualora da tale comportamento derivino danni concreti alla Società.

Tali clausole, facendo esplicito riferimento al rispetto delle disposizioni e delle regole di comportamento previste dal Modello, potranno prevedere, ad esempio, l'obbligo da parte di questi soggetti terzi, di non adottare atti o assumere comportamenti tali da determinare una

violazione del Modello e/o del Decreto da parte di Huawei. In caso di violazione di tale obbligo, dovrà essere prevista la risoluzione del contratto con eventuale applicazione di penali.

CAPITOLO 6
AGGIORNAMENTO DEL MODELLO

In conformità a quanto previsto dall'art. 6, comma 1, lett. b) del Decreto, all'Organismo di Vigilanza è affidato il compito di curare l'aggiornamento del Modello.

A tal fine l'Organismo di Vigilanza, anche avvalendosi del supporto delle funzioni aziendali preposte al monitoraggio delle innovazioni normative, delle modifiche organizzative e attinenti alle tipologie di attività svolte dalla Società – e in particolare dei relativi flussi informativi a tali fini con continuità assicurati in favore dell'Organismo – identifica e segnala al Consiglio di Amministrazione l'esigenza di procedere all'aggiornamento del Modello, fornendo altresì indicazioni in merito alle modalità secondo cui procedere alla realizzazione dei relativi interventi.

Il Consiglio di Amministrazione valuta l'esigenza di aggiornamento del Modello segnalata dall'Organismo di Vigilanza e, sentito il Collegio Sindacale, delibera in merito all'aggiornamento del Modello in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza di:

- modifiche normative in tema di responsabilità amministrativa degli enti e significative innovazioni nell'interpretazione delle disposizioni in materia;
- identificazione di nuove attività sensibili (o strumentali), o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività d'impresa, modificazioni dell'assetto interno della Società e/o delle modalità di svolgimento delle attività d'impresa;
- emanazione e modifica di linee guida da parte dell'associazione di categoria di riferimento comunicate al Ministero della Giustizia a norma dell'art. 6 del Decreto e degli artt. 5 e ss. del D.M. 26 giugno 2003, n. 201;
- commissione delle violazioni rilevanti ai fini della responsabilità amministrativa degli enti da parte dei destinatari delle previsioni del Modello o, più in generale, di significative violazioni del Modello;
- scoperta di significative violazioni delle norme relative alla tutela della salute e sicurezza sul lavoro ovvero mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico;
- riscontro di carenze e/o lacune nelle previsioni del Modello a seguito di verifiche sull'efficacia del medesimo.

Contestualmente all'assunzione delle proprie delibere attinenti allo svolgimento di attività di aggiornamento del Modello, il Consiglio di Amministrazione identifica le funzioni aziendali che saranno tenute ad occuparsi della realizzazione e attuazione dei predetti interventi di aggiornamento e le correlate modalità degli stessi, autorizzando l'avvio di un apposito progetto.

Le funzioni incaricate realizzano gli interventi deliberati secondo le istruzioni ricevute e, previa informativa all'Organismo di Vigilanza, sottopongono all'approvazione del Consiglio di Amministrazione le proposte di aggiornamento del Modello scaturenti dagli esiti del relativo progetto.

Il Consiglio di Amministrazione, sentito il Collegio Sindacale, approva gli esiti del progetto, dispone l'aggiornamento del Modello e identifica le funzioni aziendali che saranno tenute ad occuparsi dell'attuazione delle modifiche/integrazioni derivanti dagli esiti del progetto medesimo e della diffusione dei relativi contenuti all'interno e all'esterno della Società.

L'approvazione dell'aggiornamento del Modello viene immediatamente comunicata all'Organismo di Vigilanza, il quale, a sua volta, vigila sulla corretta attuazione e diffusione degli aggiornamenti operati.

L'Organismo di Vigilanza provvede, altresì, mediante apposita relazione, a informare il Consiglio di Amministrazione circa l'esito dell'attività di vigilanza intrapresa in ottemperanza alla delibera che dispone l'aggiornamento del Modello.

Il Modello è, in ogni caso, sottoposto a procedimento di revisione periodica con cadenza triennale da disporsi mediante delibera del Consiglio di Amministrazione

APPENDICE I
LA RESPONSABILITÀ AMMINISTRATIVA DELLE PERSONE GIURIDICHE EX D.LGS. 231/2001

1.1 Fattispecie di reato

I reati per i quali l'ente può essere ritenuto responsabile ai sensi del d.lgs. 231/2001 – se commessi nel suo interesse o a suo vantaggio dai soggetti qualificati *ex* art. 5, comma 1, del Decreto stesso – possono essere compresi, per comodità espositiva, nelle seguenti categorie:

- delitti contro la pubblica amministrazione (richiamati dagli artt. 24 e 25 d.lgs. 231/2001)[19];
- delitti in materia di criminalità informatica (richiamati dall'art. 24-*bis* d.lgs. 231/2001)[20];
- delitti di criminalità organizzata (richiamati dall'art. 24-*ter* d.lgs. 231/2001)[21];
- delitti contro la fede pubblica (richiamati dall'art. 25-*bis* d.lgs. 231/2001)[22];

[19] Si tratta dei reati seguenti: malversazione a danno dello Stato o dell'Unione europea (art. 316-*bis* c.p.), indebita percezione di erogazioni a danno dello Stato (art. 316-*ter* c.p.), truffa aggravata a danno dello Stato (art. 640, comma 2, n. 1, c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.), frode informatica a danno dello Stato o di altro ente pubblico (art. 640-*ter* c.p.), corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 318, 319 e 319-*bis* c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), corruzione in atti giudiziari (art. 319-*ter* c.p.), istigazione alla corruzione (art. 322 c.p.), concussione, induzione indebita a dare o promettere utilita' e corruzione (art. 317 c.p.), istigazione alla corruzione e concussione di membri delle Comunità europee, funzionari delle Comunità europee, degli Stati esteri e delle organizzazioni pubbliche internazionali (art. 322-*bis* c.p.)

[20] L'art. 24-*bis* è stato introdotto nel d.lgs. 231/2001 dall'art. 7 della legge 18 marzo 2008, n. 48. Si tratta dei delitti di falsità riguardanti documenti informatici (art. 491-*bis* c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.), detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematica (art. 615-*quater* c.p.), diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* c.p.), intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.), installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.), danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.), danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter* c.p.), danneggiamento di sistemi informatici o telematica (art. 635-*quater* c.p.), danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies*) e frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.).

[21] L'art. 24-*ter* è stato introdotto nel d.lgs. 231/2001 dall'art. 2, comma 29, della legge 15 luglio 2009, n. 94. Si tratta dei seguenti reati: associazione per delinquere finalizzata alla riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.); alla tratta di persone (art. 601 c.p.), all'acquisto e alienazione di schiavi (602 c.p.) e all'immigrazione clandestina (art. 12, comma 3-*bis* d.lgs. n. 286/1998), richiamati dall'art. 416, comma 6, c.p.; associazioni di tipo mafioso anche straniere (art. 416-*bis* c.p.); scambio elettorale politico-mafioso (art. 416-*ter* c.p.); sequestro di persona a scopo di estorsione (art. 630 c.p.); delitti commessi avvalendosi delle condizioni previste dall'art. 416-*bis* c.p. (si tratta di tutti quei delitti commessi avvalendosi della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva); delitti commessi al fine di agevolare l'attività delle associazioni previste dall'art. 416-*bis*; associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 d.P.R. n. 309/1990); associazione per delinquere, fuori dai casi previsti dal comma 6 del medesimo articolo (art. 416 c.p.); 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 o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'articolo 2, terzo comma, della legge 18 aprile 1975, n. 110 (delitti richiamati dall'art. 407, comma 2, lettera a), numero 5), c.p.p.).

[22] L'art. 25-*bis* è stato introdotto nel d.lgs. 231/2001 dall'art. 6 del D.L. 350/2001, convertito in legge, con modificazioni, dall'art. 1 della L. 409/2001. Si tratta dei reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.), alterazione di monete (art. 454 c.p.), spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.), spendita di monete falsificate ricevute in buona fede (art. 457 c.p.), falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.), contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.), fabbricazione o detenzione di filigrane

- delitti contro l'industria e il commercio (richiamati dall'art. 25-*bis*.1 d.lgs. 231/2001)[23];
- reati societari (richiamati dall'art. 25-*ter* d.lgs. 231/2001)[24];
- delitti in materia di terrorismo e di eversione dell'ordine democratico (richiamati dall'art. 25-*quater* d.lgs. 231/2001)[25];
- delitti di pratiche di mutilazione degli organi genitali femminili (richiamati dall'art. 25-*quater*.1 d.lgs. 231/2001)[26];
- delitti contro la personalità individuale (richiamati dall'art. 25-*quinquies* d.lgs. 231/2001)[27];
- reati in materia di abusi di mercato (richiamati dall'art. 25-*sexies* d.lgs. 231/2001)[28];

---

o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.), uso di valori di bollo contraffatti o alterati (art. 464 c.p.).
Il novero dei reati presupposto è stato successivamente ampliato dall'art. 15, comma 7, della legge 23 luglio 2009, n. 99, il quale ha reso rilevanti ai fini della sussistenza della responsabilità amministrativa dell'ente le fattispecie di cui agli artt. 473 c.p. (contraffazione, alterazione o uso di segni distintivi di opere dell'ingegno o di prodotti industriali) e 474 c.p. (introduzione nello Stato e commercio di prodotti con segni falsi).

[23] L'art. 25-*bis*.1 è stato introdotto nel d.lgs. 231/2001 dall'art. 15, comma 7, della legge 23 luglio 2009, n. 99. Si tratta dei seguenti 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 di prodotti agroalimentari (art. 517-*quater* c.p.).

[24] L'art. 25-*ter* è stato introdotto nel d.lgs. 231/2001 dall'art. 3 del d.lgs. 61/2002. Si tratta dei reati di false comunicazioni sociali e false comunicazioni sociali in danno della società, dei soci o dei creditori (artt. 2621 e 2622 c.c.), impedito controllo (art. 2625, 2° comma, c.c.), formazione fittizia del capitale (art. 2632 c.c.), indebita restituzione dei conferimenti (art. 2626 c.c.), illegale ripartizione degli utili e delle riserve (art. 2627 c.c.), illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.), operazioni in pregiudizio dei creditori (art. 2629 c.c.), omessa comunicazione del conflitto d'interessi (art. 2629-*bis* c.c.), indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.), illecita influenza sull'assemblea (art. 2636 c.c.), aggiotaggio (art. 2637 c.c.), ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).

[25] L'art 25-*quater* è stato introdotto nel d.lgs. 231/2001 dall'art. 3 della legge 14 gennaio 2003, n. 7. Si tratta dei "*delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali*", nonché dei delitti, diversi da quelli sopra indicati, "*che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999*". Tale Convenzione, punisce chiunque, illegalmente e dolosamente, fornisce o raccoglie fondi sapendo che gli stessi saranno, anche parzialmente, utilizzati per compiere: (i) atti diretti a causare la morte - o gravi lesioni - di civili, quando l'azione sia finalizzata ad intimidire una popolazione, o coartare un governo o un'organizzazione internazionale; (ii) atti costituenti reato ai sensi delle convenzioni in materia di: sicurezza del volo e della navigazione, tutela del materiale nucleare, protezione di agenti diplomatici, repressione di attentati mediante uso di esplosivi. La categoria dei "*delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali" è* menzionata dal Legislatore in modo generico, senza indicare le norme specifiche la cui violazione comporterebbe l'applicazione del presente articolo. Si possono, in ogni caso, individuare quali principali reati presupposti l'art. 270-*bis* c.p. (*Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*) il quale punisce chi promuove, costituisce organizza, dirige o finanzia associazioni che si propongono il compimento di atti violenti con finalità terroristiche od eversive, e l'art. 270-*ter* c.p. (*Assistenza agli associati*) il quale punisce chi dà rifugio o fornisce vitto, ospitalità mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano alle associazioni con finalità terroristiche od eversive.

[26] L'art. 25-*quater*.1 è stato introdotto nel d.lgs. 231/2001 dall'art. 8 della legge 9 gennaio 2006, n. 7. Si tratta dei delitti di pratiche di mutilazione degli organi genitali femminili (art. 583-*bis* c.p.).

[27] L'art. 25-*quinquies* è stato introdotto nel d.lgs. 231/2001 dall'art. 5 della legge 11 agosto 2003, n. 228 e successivamente modificato dall'art. 10 della legge 6 febbraio 2006, n. 38, nonchè dal d.lgs n. 39/2014. Si tratta dei reati di riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.), tratta di persone (art. 601 c.p.), acquisto e alienazione di schiavi (art. 602 c.p.), prostituzione minorile (art. 600-*bis* c.p.), pornografia minorile (art. 600-*ter* c.p.), detenzione di materiale pornografico (art. 600-*quater* c.p.), pornografia virtuale (art. 600-*quater*.1 c.p.), iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinquies* c.p.).

- reati transnazionali (richiamati dall'art. 10 della legge 16 marzo 2006, n. 146, di "*ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 e il 31 maggio 2001*")[29];
- delitti commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (richiamati dall'art. 25-*septies* d.lgs. 231/2001)[30];
- delitti di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (richiamati dall'art. 25-*octies* d.lgs. 231/2001)[31];
- delitti in materia di violazione del diritto d'autore (richiamati dall'art. 25-*novies* d.lgs. 231/2001)[32];
- reato di "*induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*" (richiamato dall'art. 25-*decies* d.lgs. 231/2001)[33];
- reati ambientali (richiamati dall'art. 25-*undecies* d.lgs. 231/2001)[34];

---

[28] L'art. 25-*sexies* è stato introdotto nel d.lgs. 231/2001 dall'art. 9 della legge 18 aprile 2005, n. 62 (legge comunitaria 2004). Si tratta dei reati di abuso di informazioni privilegiate (art. 184 d.lgs. 58/1998) e di manipolazione del mercato (art. 185 d.lgs. 58/1998).

[29] La definizione di "reato transnazionale" è contenuta nell'art. 3 della medesima legge 146/2006, laddove si specifica che si considera tale "*il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato*", con l'ulteriore condizione che sussista almeno uno dei seguenti requisiti: "*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*" [art. 3, lett. a), b), c) e d)].
I reati transnazionali in relazione ai quali l'art. 10 della legge 146/2006 prevede la responsabilità amministrativa degli enti, sono i seguenti: reati associativi di cui agli artt. 416 c.p. ("associazione per delinquere") e 416-*bis* c.p. ("associazione di tipo mafioso"), all'art. 291-*quater* del d.p.r. 23 gennaio 1973, n. 43 ("associazione per delinquere finalizzata al contrabbando di tabacchi esteri") e all'art. 74 del d.p.r. 9 ottobre 1990, n. 309 ("associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope"); reati concernenti il "traffico di migranti" di cui all'art. 12, commi 3, 3-*bis*, 3-*ter* e 5, del d.lgs. 25 luglio 1998, n. 286; reati concernenti l'"intralcio alla giustizia" di cui agli artt. 377-*bis* c.p. ("induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria") e 378 c.p. ("favoreggiamento personale").
È da notare che, in questo caso, l'ampliamento dei reati che comportano la responsabilità dell'ente non è stato operato – come in precedenza – con l'inserimento di ulteriori disposizioni nel corpo del d.lgs. 231/2001, bensì mediante un'autonoma previsione contenuta nel suddetto art. 10 della legge 146/2006, il quale stabilisce le specifiche sanzioni amministrative applicabili ai reati sopra elencati, disponendo – in via di richiamo – nell'ultimo comma che "*agli illeciti amministrativi previsti dal presente articolo si applicano le disposizioni di cui al d.lgs. 8 giugno 2001, n. 231*".

[30] L'art. 25-*septies* è stato introdotto nel d.lgs. 231/2001 dall'art. 9 della legge 3 agosto 2007, n. 123 e successivamente modificato dall'art. 300 del d.lgs. 9 aprile 2008, n. 81. Si tratta dei delitti di omicidio colposo (art. 589 c.p.) e lesioni colpose gravi o gravissime (art. 590, terzo comma, c.p.), commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

[31] L'art. 25-*octies* è stato introdotto nel d.lgs. 231/2001 dall'art. 63 del d.lgs. 21 novembre 2007, n. 231. Si tratta dei delitti di ricettazione (art. 648 c.p.), riciclaggio (art. 648-*bis* c.p.) e impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.). Inserimento del reato di autoriciclaggio con la l. 186/2014

[32] L'art. 25-*novies* è stato introdotto nel d.lgs. 231/2001 dall'art. 15, comma 7, della legge 23 luglio 2009, n. 99. Si tratta di alcuni reati contro la proprietà industriale previsti all'art. 171, comma 1, lett. a-*bis*), all'art. 171, comma 3, all'art. 171-*bis*, all'art. 171-*ter*, all'art. 171-*septies* e all'art. 171-*octies* della legge 22 aprile 1941, n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).

[33] L'art. 25-*decies* è stato introdotto nel d.lgs. 231/2001 dall'art. 4 della legge 3 agosto 2009, n. 116 e sostituito dall'art. 2, comma 1, d.lgs. 121/2011. La legge 116/2009 (recante "*Ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione, adottata dalla Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4, firmata dallo Stato italiano il 9 dicembre 2003, nonché norme di adeguamento interno e modifiche al codice penale e al codice di procedura penale*") ha quindi reso rilevante ai fini della sussistenza della responsabilità amministrativa dell'ente la fattispecie di cui all'art. 377-*bis* c.p. a prescindere dal carattere transnazionale della condotta.

- delitto di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (richiamato dall'art. 25-*duodecies* d.lgs. 231/2001)[35].

In base all'art. 187-quinquies del d.lgs. 58/1998 (di seguito anche "T.U. della finanza" o "TUF"), l'ente può essere, altresì, ritenuto responsabile del pagamento di una somma pari all'importo della sanzione amministrativa pecuniaria irrogata per gli illeciti amministrativi di abuso di informazioni privilegiate (art. 187-*bis* d.lgs. 58/1998) e di manipolazione del mercato (187-*ter* d.lgs. 58/1998), se commessi, nel suo interesse o a suo vantaggio, da persone riconducibili alle categorie dei "soggetti apicali" e dei "soggetti sottoposti all'altrui direzione o vigilanza". Per di più, l'ultimo comma del citato art. 187-*quinquies* dispone che agli illeciti amministrativi sopra richiamati si applichino talune norme del d.lgs. 231/2001, ivi espressamente richiamate, concernenti, fra l'altro, i modelli di organizzazione, gestione e controllo con efficacia esimente[36].

---

[34] L'art. 25-*undecies* è stato introdotto nel d.lgs. 231/2001 dall'art. 2 del d.lgs. 7 luglio 2011, n. 121, recante "*Attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni*". Si tratta dei reati in materia ambientale previsti dalla norme di seguito elencate:

- il nuovo art. 727-bis c.p. ("*Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette*"), introdotto nel codice penale dall'art. 1 del d.lgs. 121/2011;
- il nuovo art. 733-bis c.p. ("*Distruzione o deterioramento di habitat all'interno di un sito protetto*"), introdotto nel codice penale dall'art. 1 del d.lgs. 121/2011;
- d.lgs. 152/2006 (il c.d. "*Codice dell'ambiente*"): art. 137, commi 2, 3, 5 primo e secondo periodo, 11 e 13 (scarichi di acque reflue industriali contenenti sostanze pericolose od effettuate oltre i limiti consentiti, scarichi nelle acque del mare); art. 256, commi 1 lett. a) e lett. b), 3 primo e secondo periodo, 5 e 6 primo periodo (attività non autorizzata di gestione rifiuti, anche pericolosi, realizzazione o gestione di discariche non autorizzate); art. 257, commi 1 e 2 (bonifica dei siti); art. 258, comma 4 secondo periodo (violazione di obblighi di comunicazione e tenuta dei registri, adesione al sistema cd. SISTRI); art. 259, comma 1 (illecito traffico di rifiuti); art. 260, commi 1 e 2 (attività organizzata per il traffico illecito di rifiuti, anche ad alta radioattività); art. 260-bis, commi 6, 7 secondo e terzo periodo, 8 primo periodo e secondo periodo (falsità e alterazioni dei certificati di analisi di rifiuti e schede del sistema cd. SISTRI); art. 279, comma 5 (installazione o esercizio di stabilimenti in assenza di valida autorizzazione e in violazione dei limiti per le emissioni, relativi alla qualità dell'aria);
- legge 150/1992 ("*Disciplina dei reati relativi all'applicazione in Italia della convenzione sul commercio internazionale delle specie animali e vegetali in via di estinzione (...) nonché norme per la commercializzazione e la detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l'incolumità pubblica*"): art. 1, commi 1 e 2 (commercializzazione alcune specie animali e vegetali protette); art. 2, commi 1 e 2 (commercializzazione alcune specie animali protette); art. 6, comma 4 (illegale detenzione di esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e per l'incolumità pubblica); art. 3 bis, comma 1 (falsità o alterazioni nella documentazione e certificazione relativa ad esemplari animali o vegetali; si richiamano le pene previste per i reati di cui al libro II, titolo VII, capo III del codice penale: "Della falsità in atti");
- legge 549/1993 ("*Misure a tutela dell'ozono stratosferico e dell'ambiente*"): art. 3, comma 6 (che punisce la produzione, il consumo, l'importazione, l'esportazione, la detenzione e la commercializzazione di alcune sostanza lesive, ricomprese nelle Tabelle A e B allegate alla legge);
- d.lgs. 202/2007 ("*Attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni*"): art. 8, commi 1 e 2 (inquinamento doloso); art. 9, commi 1 e 2 (inquinamento colposo).

[35] L'art. 25-*duodecies* è stato introdotto nel d.lgs. 231/2001 dall'art. 2, comma 1, d.lgs. 16 luglio 2012, n. 109. Si tratta del delitto di cui all'articolo 22, comma 12-*bis*, del decreto legislativo 25 luglio 1998, n. 286.

[36] Art. 187-*quinquies* del d.lgs. 58/1998: "Responsabilità dell'ente – [1] *L'ente è responsabile del pagamento di una somma pari all'importo della sanzione amministrativa irrogata per gli illeciti di cui al presente capo commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente 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).* [2] *Se, in seguito alla commissione degli illeciti di cui al comma 1, il prodotto o il profitto conseguito dall'ente è di rilevante entità, la sanzione è aumentata fino a dieci volte tale prodotto o profitto.* [3] *L'ente non è responsabile se dimostra che le persone indicate nel comma 1 hanno agito esclusivamente nell'interesse proprio o di terzi.* [4] *In relazione agli illeciti di cui al comma 1 si applicano, in quanto compatibili, gli articoli 6, 7, 8 e 12 del decreto legislativo 8 giugno 2001, n. 231. Il Ministero della giustizia formula le osservazioni di cui all'articolo 6 del decreto legislativo*

Inoltre, il Consiglio dell'Unione europea ha previsto che gli Stati membri debbano adottare le misure necessarie al fine di perseguire, in sede penale i fenomeni di corruzione nel settore privato (Consiglio UE, Decisione quadro del 22 luglio 2003, 2003/568/GAI, relativa alla corruzione nel settore privato)[37].

1.2 Sanzioni

Per quanto attiene alle (rilevanti) sanzioni applicabili alla società che incorra nella responsabilità di cui al Decreto, esse possono essere distinte in sanzioni di tipo pecuniario (attualmente fino ad un massimo di 1,55 milioni di euro)[38] e di tipo interdittivo, quali la proibizione di contrarre con la pubblica amministrazione[39], il divieto di pubblicità,

8 giugno 2001, n. 231, sentita la CONSOB, con riguardo agli illeciti previsti dal presente titolo." Per un commento a tale disposizione si veda Bartolomucci, *Market abuse e «le» responsabilità amministrative degli emittenti*, in *Le Società*, 2005, 919.

[37] Si segnala, in proposito, che l'art. 28 della legge 25 febbraio 2008, n. 34 (Legge comunitaria 2007) prevede, tra l'altro, la delega al Governo ad adottare, entro dodici mesi dall'entrata in vigore della legge, un decreto legislativo recante le norme occorrenti per dare attuazione alla decisione quadro 2003/568/GAI del Consiglio UE del 22 luglio 2003 (relativa alla lotta contro la corruzione nel settore privato). Quanto ai principi e criteri direttivi che il Governo è chiamato a rispettare per dare attuazione alla citata decisione quadro, si segnala la previsione, contenuta nell'art. 29 della medesima legge, della necessità di:

a) introdurre nel libro II, titolo VIII, capo II, del codice penale una fattispecie criminosa la quale punisca con la reclusione da uno a cinque anni la condotta di chi, nell'ambito di attività professionali, intenzionalmente sollecita o riceve, per sé o per un terzo, direttamente o tramite un intermediario, un indebito vantaggio di qualsiasi natura, oppure accetta la promessa di tale vantaggio, nello svolgimento di funzioni direttive o lavorative non meramente esecutive per conto di una entità del settore privato, per compiere o omettere un atto, in violazione di un dovere, sempreché tale condotta comporti o possa comportare distorsioni di concorrenza riguardo all'acquisizione di beni o servizi commerciali;
b) prevedere la punibilità con la stessa pena anche di colui che, intenzionalmente, nell'ambito di attività professionali, direttamente o tramite intermediario, dà, offre o promette il vantaggio di cui alla lettera a);
c) introdurre fra i reati di cui alla sezione III del capo I del decreto legislativo 8 giugno 2001, n. 231, le fattispecie criminose di cui alle lettere a) e b), con la previsione di adeguate sanzioni pecuniarie e interdittive nei confronti delle entità nel cui interesse o vantaggio sia stato posto in essere il reato.

[38] La sanzione pecuniaria è determinata dal giudice penale attraverso un sistema basato su "quote" in numero non inferiore a cento e non superiore a mille e di importo variabile fra un minimo di Euro 258,22 ad un massimo di Euro 1549,37. Nella commisurazione della sanzione pecuniaria il giudice determina:

– il numero delle quote, tenendo conto della gravità del fatto, del grado della responsabilità della società nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti;
– l'importo della singola quota, sulla base delle condizioni economiche e patrimoniali della società.

[39] Un significativo precedente giurisprudenziale in tema di sanzioni interdittive è costituito dalla decisione sul caso Siemens-Enelpower. Il Giudice per le Indagini Preliminari di Milano, Guido Salvini, ha applicato per la prima volta in via cautelare – in data 27 aprile 2004 – la misura dell'interdizione dai rapporti con la pubblica amministrazione a carico di Siemens Ag, nell'ambito dell'inchiesta Enelpower, per la durata di un anno. Successivamente, in data 5 maggio 2004, ha disposto l'integrazione dell'originario provvedimento restringendone l'applicazione allo specifico ramo d'azienda nell'ambito del quale sarebbe avvenuta la presunta corruzione messa in atto da *manager* di Siemens nei confronti di due amministratori di Enelpower. In altre parole, l'interdizione alla partecipazione agli appalti pubblici è stata circoscritta al solo ramo d'azienda della divisione Power Generation (una delle 14 divisioni del gruppo tedesco), che si occupa della produzione di energia elettrica mediante turbogas. Rimangono estranee al divieto di contrattare con la pubblica amministrazione tutte le società del gruppo Siemens in Italia, che hanno pertanto potuto continuare a svolgere le proprie attività anche nell'ambito di appalti pubblici.
Il provvedimento integrativo del GIP di Milano appare riconducibile al citato art. 14, comma 1, del d.lgs. 231/2001, ai sensi del quale "*Le sanzioni interdittive hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente*". Si ricorda, altresì, che il secondo comma della medesima disposizione prevede che "*Il divieto di contrattare con la pubblica amministrazione può anche essere limitato a determinati tipi di contratto o a determinate amministrazioni.*" Inoltre, ai sensi dell'art. 46 del d.lgs. 231/2001 "*Nel disporre le misure cautelari, il giudice tiene conto della specifica idoneità di ciascuna in relazione alla natura e al grado delle esigenze cautelari da soddisfare nel caso concreto. Ogni misura cautelare deve essere proporzionata all'entità del fatto e alla sanzione che si ritiene possa essere applicata all'ente. L'interdizione dall'esercizio dell'attività può essere disposta in via cautelare soltanto quando ogni altra misura risulti inadeguata*".
La stessa relazione illustrativa al d.lgs. 231/2001 precisa che la sanzione interdittiva non deve ispirarsi a un criterio applicativo generalizzato e indiscriminato: "*Le sanzioni, per quanto possibile, devono colpire il ramo di attività in*

l'interdizione dall'esercizio dell'attività, in via temporanea o definitiva, la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi e ciò secondo una graduazione crescente in base alla gravità o reiterazione dell'illecito[40].

Per quanto attiene alla sanzione pecuniaria, essa è obbligatoriamente applicata, in base all'articolo 10, 1 comma, in ogni ipotesi di responsabilità amministrativa da reato, mentre le altre sanzioni sono accessorie a quella pecuniaria ed eventuali a seconda del reato effettivamente commesso o tentato.

I criteri di commisurazione della sanzione pecuniaria sono di due tipi:

a) quelli oggettivi, legati alla gravità del fatto ed al grado della responsabilità dell'ente, nonché alle attività poste in essere per eliminare o limitare le conseguenze dannose del fatto e prevenire la commissione di ulteriori illeciti, che incidono sulla determinazione del numero delle quote applicate;

b) quelli soggettivi, legati alle condizioni economiche e patrimoniali dell'ente, che incidono sulla determinazione del valore pecuniario della quota, al fine di assicurare l'efficacia della sanzione.

La sanzione pecuniaria è inoltre soggetta ad un regime di riduzione, da un terzo alla metà, in virtù di determinati fatti, che potrebbero definirsi attenuanti, di carattere oggettivo.

Per quanto attiene alle sanzioni interdittive, i criteri di scelta per la determinazione del tipo e della durata della sanzione interdittiva sono quelli già previsti per la sanzione pecuniaria e con riferimento alla loro idoneità a prevenire illeciti ulteriori; esse hanno quindi valenza preventiva, oltre che punitiva.

Da notare che la legge prevede la possibilità che, in luogo della sanzione della interdizione dalla attività - che può assumere i contorni di una vera e propria condanna a morte[41] per l'ente - il giudice possa disporre la prosecuzione dell'attività da parte di un commissario giudiziale, appositamente nominato, al fine preminente di evitare gravi pregiudizi per la collettività[42] o rilevanti ripercussioni per l'occupazione. In tal caso il profitto derivante dalla prosecuzione dell'attività viene confiscato.

Segnaliamo infine che l'articolo 17 del Decreto prevede l'esclusione della applicazione di sanzioni interdittive ove, prima della dichiarazione di apertura del dibattimento di primo grado, vengano eliminate le carenze organizzative che hanno determinato il reato, mediante l'adozione di modelli organizzativi idonei, e sempreché il danno sia stato risarcito e sia stato messo a disposizione il profitto conseguito ai fini della confisca.

Per completezza, segnaliamo da ultimo che, ai sensi degli artt. 9-11 del D.P.R. 14 novembre 2002, n. 313 (già articolo 80 del Decreto), è stata prevista l'istituzione, presso il casellario

---

cui si è sprigionato l'illecito in omaggio a un principio di economicità e proporzione. La necessità di questa selezione – conviene ripeterlo – deriva proprio dalla estrema frammentazione dei comparti produttivi che oggi segna la vita delle imprese".

Altro significativo precedente giurisprudenziale è costituito dalla sentenza dibattimentale emessa dal Tribunale di Milano in data 20 marzo 2007, sul caso My Chef S.r.l. Il Tribunale di Milano, accertata la responsabilità della My Chef S.r.l. per l'illecito amministrativo previsto dagli artt. 5 e ss. del d.lgs. 231/2001 in relazione al reato di corruzione commesso dai soggetti apicali appartenenti alla stessa, ha inflitto alla società, oltre alla sanzione pecuniaria e alla confisca del profitto del reato, la sanzione interdittiva del divieto di contrattare con la Pubblica Amministrazione per un anno, prevedendo altresì, quale pena accessoria, la pubblicazione della sentenza per estratto sul quotidiano il "Sole 24Ore".

40 A ciò si aggiunge sempre la confisca del vantaggio economico tratto dalla società come conseguenza del reato, confisca che può essere applicata dal giudice per equivalente, a valere su qualsiasi bene o conto aziendale e, in taluni casi, la pubblicazione della sentenza di condanna.

41 Cfr. l'articolo 16 del d.lgs. 231/2001 che prevede l'ipotesi della sanzione interdittiva applicata in via definitiva.

42 Ciò nel caso di ente che svolge un pubblico servizio o un servizio di pubblica utilità.

giudiziale centrale, dell'anagrafe nazionale delle sanzioni amministrative irrogate alle società o altri enti. Tale anagrafe raccoglie i provvedimenti sanzionatori divenuti irrevocabili ove rimangono per cinque anni dall'applicazione della sanzione pecuniaria o per dieci anni dall'applicazione della sanzione interdittiva, se negli stessi periodi non sia stato commesso un ulteriore illecito amministrativo.

1.3 I presupposti della responsabilità dell'ente

L'ente può essere chiamato a rispondere nel caso di commissione, o tentata commissione, di un reato da parte di una o più persone fisiche qualificate, ove tale reato risulti commesso nell'interesse dell'ente o a suo vantaggio.

In particolare, il reato deve essere stato commesso da determinati soggetti che abbiano con l'ente un rapporto funzionale e, precisamente, da coloro che si trovino:

- in posizione apicale rispetto alla struttura dell'ente, cioè al vertice del medesimo; ovvero
- in posizione di sottoposti a tali soggetti[43].

E' opportuno, altresì, ribadire che la società non risponde, per espressa previsione legislativa (art. 5, comma 2, del Decreto), se le persone sopra indicate hanno agito nell'esclusivo interesse proprio o di terzi[44].

[43] Per quanto attiene ai "sottoposti" degli apicali, devono considerarsi tali tutti i soggetti che operano in posizione sottoposta alla "direzione o alla vigilanza" dei vertici dell'ente, ossia ogni persona che abbia, con l'ente, un qualsivoglia rapporto funzionale (tra cui, ad esempio, i preposti e tutti i lavoratori subordinati).

[44] La Relazione illustrativa al d.lgs. 231/2001, nella parte relativa all'art. 5, comma 2, d.lgs. 231/2001, afferma: *"Il secondo comma dell'articolo 5 dello schema mutua dalla lett. e) della delega la clausola di chiusura ed esclude la responsabilità dell'ente quando le persone fisiche (siano esse apici o sottoposti) abbiano agito nell'interesse esclusivo proprio o di terzi. La norma stigmatizza il caso di "rottura" dello schema di immedesimazione organica; si riferisce cioè alle ipotesi in cui il reato della persona fisica non sia in alcun modo riconducibile all'ente perché non realizzato neppure in parte nell'interesse di questo. E si noti che, ove risulti per tal via la manifesta estraneità della persona morale, il giudice non dovrà neanche verificare se la persona morale abbia per caso tratto un vantaggio (la previsione opera dunque in deroga al primo comma)."* Si veda, inoltre, Gennai-Traversi, op. cit., 38: *"La responsabilità dell'ente è (...) esclusa* – a norma dell'art. 5, comma 2 - *quando gli autori del reato hanno agito nell'interesse esclusivo proprio o di terzi. Tale previsione, che si colloca come condizione negativa in ordine alla configurabilità della responsabilità dell'ente, è pienamente coerente con l'impostazione sistematica del provvedimento legislativo. L'essere stato il reato commesso nell'interesse esclusivo di soggetti diversi dall'ente, recide infatti il collegamento che riconduce il fatto criminoso alla persona giuridica. In tale fattispecie rimane del tutto indifferente anche l'esistenza di un eventuale vantaggio che l'ente può aver tratto dal reato. E ciò in deroga alla generale statuizione del medesimo art. 5, comma 1."* Si vedano altresì De Simone, op. cit., 101 e Ferrua, Il processo penale contro gli enti: incoerenza e anomalie nelle regole di accertamento, in Responsabilità degli enti per illeciti amministrativi dipendenti da reato, AA.VV., a cura di Garuti, cit., 231. La Circolare Assonime La responsabilità amministrativa degli enti, cit., 5, afferma quanto segue: *"La formulazione del citato comma 1 dell'art. 5 (presenza della preposizione disgiuntiva "o") sembra dunque consentire di ritenere gli enti responsabili vuoi quando, pur avendo agito a tal fine, non si sia recato un beneficio all'ente, vuoi quando, pur non avendo agito a tal fine, si rechi un beneficio all'ente"*. La legge aggiunge tuttavia che l'*"ente non risponde se le persone (...) hanno agito nell'interesse esclusivo proprio o di terzi"* (art. 5, comma 2). Le due disposizioni non sono di facile coordinamento. La Relazione illustrativa sembra chiarire che l'ente che trae un "vantaggio" da un reato che però non sia stato commesso per perseguire l'interesse dell'ente stesso, non potrebbe essere sanzionato secondo le regole proprie del d.lgs. n. 231. L'esclusività dell'interesse in capo al soggetto che ha compiuto il reato renderebbe, di fatto, irrilevante, ai fini dell'applicazione della sanzione, l'eventuale vantaggio ottenuto di riflesso dall'ente. L'ente è dunque responsabile: a) quando coloro che hanno commesso il reato hanno agito per favorire l'ente stesso, anche se dalla condotta criminosa l'ente non ha ricavato alcun vantaggio; b) quando ha comunque ricevuto un vantaggio dalla commissione del reato, a meno che non si riesca a dimostrare che coloro che hanno agito erano mossi dall'esclusivo interesse personale (o di terzi).

1.4 Vicende modificative dell'ente

Il d.lgs. 231/2001 disciplina il regime della responsabilità patrimoniale dell'ente anche in relazione alle vicende modificative dell'ente quali la trasformazione, la fusione, la scissione e la cessione d'azienda.

Secondo l'art. 27, comma 1, del d.lgs. 231/2001, dell'obbligazione per il pagamento della sanzione pecuniaria risponde l'ente con il suo patrimonio o con il fondo comune, laddove la nozione di patrimonio deve essere riferita alle società e agli enti con personalità giuridica, mentre la nozione di "fondo comune" concerne le associazioni non riconosciute. Tale previsione costituisce una forma di tutela a favore dei soci di società di persone e degli associati ad associazioni, scongiurando il rischio che gli stessi possano essere chiamati a rispondere con il loro patrimonio personale delle obbligazioni derivanti dalla comminazione all'ente delle sanzioni pecuniarie[45]. La disposizione in esame rende, inoltre, manifesto l'intento del Legislatore di individuare una responsabilità dell'ente autonoma rispetto non solo a quella dell'autore del reato (si veda, a tale proposito, l'art. 8 del d.lgs. 231/2001)[46] ma anche rispetto ai singoli membri della compagine sociale[47].

Gli artt. 28-33 del d.lgs. 231/2001 regolano l'incidenza sulla responsabilità dell'ente delle vicende modificative connesse a operazioni di trasformazione, fusione, scissione e cessione di azienda. Il Legislatore ha tenuto conto di due esigenze contrapposte:

- da un lato, evitare che tali operazioni possano costituire uno strumento per eludere agevolmente la responsabilità amministrativa dell'ente;
- dall'altro, non penalizzare interventi di riorganizzazione privi di intenti elusivi. La Relazione illustrativa al d.lgs. 231/2001 afferma "*Il criterio di massima al riguardo seguito è stato quello di regolare la sorte delle sanzioni pecuniarie conformemente ai principi dettati dal codice civile in ordine alla generalità degli altri debiti dell'ente originario, mantenendo, per converso, il collegamento delle sanzioni interdittive con il ramo di attività nel cui ambito è stato commesso il reato*".

In caso di trasformazione, l'art. 28 del d.lgs. 231/2001 prevede (in coerenza con la natura di tale istituto che implica un semplice mutamento del tipo di società, senza determinare l'estinzione del soggetto giuridico originario) che resta ferma la responsabilità dell'ente per i reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto.

In caso di fusione, l'ente che risulta dalla fusione (anche per incorporazione) risponde dei reati di cui erano responsabili gli enti partecipanti alla fusione (art. 29 del d.lgs. 231/2001). L'ente risultante dalla fusione, infatti, assume tutti i diritti e obblighi delle società partecipanti all'operazione (art. 2504-*bis*, primo comma, c.c.)[48] e, facendo proprie le attività aziendali,

[45] Gennai-Traversi, *op. cit*., 164: "*ciò in deroga alla disciplina generale secondo la quale delle obbligazioni sociali rispondono anche i soci illimitatamente responsabili (artt. 2267, 2304 e 2318 cod. civ.), così come gli associati per le obbligazioni dell'associazione (art. 38 cod. civ.)*".

[46] Art. 8 del d.lgs. 231/2001: "Autonomia della responsabilità dell'ente – *1. la responsabilità dell'ente sussiste anche quando: a) l'autore del reato non è stato identificato o non è imputabile; b) il reato si estingue per una causa diversa dall'amnistia. 2. Salvo che la legge disponga diversamente, non si procede nei confronti dell'ente quando è concessa amnistia per un reato in relazione al quale è prevista la sua responsabilità e l'imputato ha rinunciato alla sua applicazione. 3. L'ente può rinunciare all'amnistia*."

[47] Così Roberti, *La responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni prive di personalità giuridica e le vicende modificative*, in *Nuove leggi civile commentate*, 2001, 1135.

[48] Art. 2504-*bis* c.c.: "Effetti della fusione – *La società che risulta dalla fusione o quella incorporante assumono i diritti e gli obblighi delle società estinte.*" Il d.lgs. 6/2003 ha così modificato il testo dell'art. 2504-*bis*: "Effetti della fusione - *La società che risulta dalla fusione o quella incorporante assumono i diritti e gli obblighi delle società partecipanti alla fusione, proseguendo in tutti i loro rapporti, anche processuali, anteriori alla fusione."*

accorpa altresì quelle nel cui ambito sono stati posti in essere i reati di cui le società partecipanti alla fusione avrebbero dovuto rispondere[49].

L'art. 30 del d.lgs. 231/2001 prevede che, nel caso di scissione parziale, la società scissa rimane responsabile per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto.

Gli enti beneficiari della scissione (sia totale che parziale) sono solidalmente obbligati al pagamento delle sanzioni pecuniarie dovute dall'ente scisso per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto, nel limite del valore effettivo del patrimonio netto trasferito al singolo ente.

Tale limite non si applica alle società beneficiarie, alle quali risulta devoluto, anche solo in parte, il ramo di attività nel cui ambito è stato commesso il reato[50].

Le sanzioni interdittive relative ai reati commessi anteriormente alla data in cui la scissione ha avuto effetto si applicano agli enti cui è rimasto o è stato trasferito, anche in parte, il ramo di attività nell'ambito del quale il reato è stato commesso.

L'art. 31 del d.lgs. 231/2001 prevede disposizioni comuni alla fusione e alla scissione, concernenti la determinazione delle sanzioni nell'eventualità che tali operazioni straordinarie siano intervenute prima della conclusione del giudizio. Viene chiarito, in particolare, il principio per cui il giudice deve commisurare la sanzione pecuniaria, secondo i criteri previsti dall'art. 11, comma 2, del d.lgs. 231/2001[51], facendo riferimento in ogni caso alle condizioni

---

[49] La Relazione illustrativa al d.lgs. 231/2001 chiarisce che "*Ad evitare che, con particolare riguardo alle sanzioni interdittive, la regola ora enunciata determini una "dilatazione" di dubbia opportunità della misura punitiva - coinvolgendo aziende "sane" in provvedimenti diretti a colpire aziende "malate" (si pensi al caso in cui una modesta società, responsabile di un illecito sanzionabile con il divieto di contrattare con la pubblica amministrazione, venga incorporata da una grande società con azioni quotate in borsa) - provvedono, per vero, da un lato, la disposizione generale che limita comunque le sanzioni interdittive all'attività o alle strutture in cui l'illecito è stato commesso (articolo 14, comma 1, dello schema); e, dall'altro, la* (…) *facoltà dell'ente risultante dalla fusione di chiedere, nei congrui casi, la sostituzione delle sanzioni stesse con sanzioni pecuniarie.*" Il Legislatore allude, a tale ultimo proposito, all'art. 31, comma 2, del d.lgs. 231/2001, secondo cui "*Salvo quanto previsto dall'articolo 17, l'ente risultante dalla fusione e l'ente al quale, nel caso di scissione, è applicabile la sanzione interdittiva possono chiedere al giudice la sostituzione della medesima con la sanzione pecuniaria, qualora, a seguito della fusione o della scissione, si sia realizzata la condizione prevista dalla lettera b) del comma 1 dell'articolo 17, e ricorrano le ulteriori condizioni di cui alle lettere a) e c) del medesimo articolo.*" Si ricorda che l'art. 17 prevede quanto segue: "1. *Ferma l'applicazione delle sanzioni pecuniarie, le sanzioni interdittive non si applicano quando, prima della dichiarazione di apertura del dibattimento di primo grado, concorrono le seguenti condizioni: a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si e' comunque efficacemente adoperato in tal senso; b) l'ente ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi; c) l'ente ha messo a disposizione il profitto conseguito ai fini della confisca."*

[50] Tale previsione appare parzialmente in linea con quanto disposto dall'art. 2504-*decies*, comma 2, c.c., ai sensi del quale "*Ciascuna società è solidalmente responsabile, nei limiti del valore effettivo del patrimonio netto ad essa trasferito o rimasto, dei debiti della società scissa non soddisfatti dalla società a cui essi fanno carico.*" Il d.lgs. 6/2003 ha trasferito tale previsione nell'art. 2506-*quater* c.c., modificandola come segue: "*Ciascuna società è solidalmente responsabile, nei limiti del valore effettivo del patrimonio netto ad essa assegnato o rimasto, dei debiti della società scissa non soddisfatti dalla società cui fanno carico*". Secondo Gennai-Traversi, *op. cit*., 175: "*Per quanto riguarda invece la scissione totale, dall'enunciato dell'art. 30, comma 2, si evince - pur in mancanza di una previsione espressa - che la responsabilità amministrativa per gli illeciti dipendenti da reati commessi anteriormente alla scissione è riferibile non già alla società scissa, ma esclusivamente alle società beneficiarie della scissione stessa, in quanto sono i soggetti normativamente indicati quali obbligati, in solido tra loro, al pagamento delle sanzioni pecuniarie dovute dall'ente scisso. Il che è peraltro consequenziale al fatto che, una volta intervenuta la scissione totale, la società originaria normalmente si estingue e, in ogni caso, rimane priva del suo patrimonio*".

[51] Art. 11 del d.lgs. 231/2001: "Criteri di commisurazione della sanzione pecuniaria - *1. Nella commisurazione della sanzione pecuniaria il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. 2. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione.*(…)".

economiche e patrimoniali dell'ente originariamente responsabile, e non a quelle dell'ente cui dovrebbe imputarsi la sanzione a seguito della fusione o della scissione.

In caso di sanzione interdittiva, l'ente che risulterà responsabile a seguito della fusione o della scissione potrà chiedere al giudice la conversione della sanzione interdittiva in sanzione pecuniaria, a patto che: (i) la colpa organizzativa che ha reso possibile la commissione del reato sia stata eliminata, e (ii) l'ente abbia provveduto a risarcire il danno e messo a disposizione (per la confisca) la parte di profitto eventualmente conseguito[52]. L'art. 32 del d.lgs. 231/2001 consente al giudice di tener conto delle condanne già inflitte nei confronti degli enti partecipanti alla fusione o dell'ente scisso al fine di configurare la reiterazione, a norma dell'art. 20 del d.lgs. 231/2001, in rapporto agli illeciti dell'ente risultante dalla fusione o beneficiario della scissione, relativi a reati successivamente commessi[53]. Per le fattispecie della cessione e del conferimento di azienda è prevista una disciplina unitaria (art. 33 del d.lgs. 231/2001)[54], modellata sulla generale previsione dell'art. 2560 c.c.[55]; il cessionario, nel caso di cessione dell'azienda nella cui attività è stato commesso il reato, è solidalmente obbligato al pagamento della sanzione pecuniaria comminata al cedente, con le seguenti limitazioni:

– è fatto salvo il beneficio della preventiva escussione del cedente;

[52] La Relazione illustrativa al d.lgs. 231/2001 chiarisce: "*L'ente risultante dalla fusione e l'ente che, in caso di scissione, risulterebbe esposto ad una sanzione interdittiva possono ovviamente evitarne in radice l'applicazione provvedendo alla riparazione delle conseguenze del reato, nei sensi e nei termini indicati in via generale dall'articolo 17. Si è ritenuto tuttavia opportuno prevedere* (…)*, che quando l'operatività della citata disposizione risultasse preclusa dal superamento del limite temporale dell'apertura del dibattimento, l'ente interessato abbia comunque facoltà di richiedere al giudice la sostituzione della sanzione interdittiva con una sanzione pecuniaria di ammontare pari da una a due volte quella inflitta all'ente per il medesimo reato. La sostituzione è ammessa alla condizione che, a seguito della fusione o della scissione, si sia realizzata una modifica organizzativa idonea a prevenire la commissione di nuovi reati della stessa specie e che, inoltre, l'ente abbia risarcito il danno o eliminato le conseguenze del reato e messo a disposizione per la confisca il profitto eventualmente conseguito (s'intende, per la parte riferibile all'ente stesso). Resta salva, in ogni caso, la facoltà di chiedere la conversione anche in executivis a norma dell'articolo 78*".

[53] Art. 32 d.lgs. 231/2001: "Rilevanza della fusione o della scissione ai fini della reiterazione - *1. Nei casi di responsabilità dell'ente risultante dalla fusione o beneficiario della scissione per reati commessi successivamente alla data dalla quale la fusione o la scissione ha avuto effetto, il giudice può ritenere la reiterazione, a norma dell'articolo 20, anche in rapporto a condanne pronunciate nei confronti degli enti partecipanti alla fusione o dell'ente scisso per reati commessi anteriormente a tale data. 2. A tale fine, il giudice tiene conto della natura delle violazioni e dell'attività nell'ambito della quale sono state commesse nonché delle caratteristiche della fusione o della scissione. 3. Rispetto agli enti beneficiari della scissione, la reiterazione può essere ritenuta, a norma dei commi 1 e 2, solo se ad essi è stato trasferito, anche in parte, il ramo di attività nell'ambito del quale è stato commesso il reato per cui è stata pronunciata condanna nei confronti dell'ente scisso*". La Relazione illustrativa al d.lgs. 231/2001 chiarisce che "*La reiterazione, in tal caso, non opera peraltro automaticamente, ma forma oggetto di valutazione discrezionale da parte del giudice, in rapporto alle concrete circostanze. Nei confronti degli enti beneficiari della scissione, essa può essere inoltre ravvisata solo quando si tratti di ente cui è stato trasferito, anche in parte, il ramo di attività nel cui ambito è stato commesso il precedente reato*".

[54] Art. 33 del d.lgs. 231/2001: " Cessione di azienda. - *1. Nel caso di cessione dell'azienda nella cui attività è stato commesso il reato, il cessionario è solidalmente obbligato, salvo il beneficio della preventiva escussione dell'ente cedente e nei limiti del valore dell'azienda, al pagamento della sanzione pecuniaria. 2. L'obbligazione del cessionario è limitata alle sanzioni pecuniarie che risultano dai libri contabili obbligatori, ovvero dovute per illeciti amministrativi dei quali egli era comunque a conoscenza. 3. Le disposizioni del presente articolo si applicano anche nel caso di conferimento di azienda*". Sul punto la Relazione illustrativa al d.lgs. 231/2001 chiarisce: "*Si intende come anche tali operazioni siano suscettive di prestarsi a manovre elusive della responsabilità: e, pur tuttavia, maggiormente pregnanti risultano, rispetto ad esse, le contrapposte esigenze di tutela dell'affidamento e della sicurezza del traffico giuridico, essendosi al cospetto di ipotesi di successione a titolo particolare che lasciano inalterata l'identità (e la responsabilità) del cedente o del conferente*".

[55] Art. 2560 c.c.: "Debiti relativi all'azienda ceduta – *L'alienante non è liberato dai debiti, inerenti l'esercizio dell'azienda ceduta anteriori al trasferimento, se non risulta che i creditori vi hanno consentito. Nel trasferimento di un'azienda commerciale risponde dei debiti suddetti anche l'acquirente dell'azienda, se essi risultano dai libri contabili obbligatori*".

– la responsabilità del cessionario è limitata al valore dell'azienda ceduta e alle sanzioni pecuniarie che risultano dai libri contabili obbligatori ovvero dovute per illeciti amministrativi dei quali era, comunque, a conoscenza.

Al contrario, resta esclusa l'estensione al cessionario delle sanzioni interdittive inflitte al cedente[56].

1.5 Reati commessi all'estero

Secondo l'art. 4 del d.lgs. 231/2001, l'ente può essere chiamato a rispondere in Italia in relazione a reati – rilevanti ai fini della responsabilità amministrativa degli enti – commessi all'estero[57]. La Relazione illustrativa al d.lgs. 231/2001 sottolinea la necessità di non lasciare sfornita di sanzione una situazione criminologica di frequente verificazione, anche al fine di evitare facili elusioni dell'intero impianto normativo in oggetto.

I presupposti (previsti dalla norma ovvero desumibili dal complesso del d.lgs. 231/2001) su cui si fonda la responsabilità dell'ente per reati commessi all'estero sono:

(i) il reato deve essere commesso all'estero da un soggetto funzionalmente legato all'ente, ai sensi dell'art. 5, comma 1, del d.lgs. 231/2001;

(ii) l'ente deve avere la propria sede principale nel territorio dello Stato italiano;

(iii) l'ente può rispondere solo nei casi e alle condizioni previste dagli artt. 7, 8, 9, 10 c.p. (nei casi in cui la legge prevede che il colpevole - persona fisica - sia punito a richiesta del Ministro della Giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti dell'ente stesso)[58].

---

[56] Secondo Roberti, *op. cit.*, 1141, la cessione d'azienda porterebbe a escludere le sanzioni interdittive. Più in generale, sul tema delle responsabilità amministrativa in relazione alle vicende modificative degli enti, si vedano, fra gli altri, Castellini, *Per trasformazioni e fusioni si segue il Codice Civile*, in *Guida al Diritto*, 2001, n. 26, 80, Roberti, *op. cit.*, 1127 ss.; De Marzo, *Il d.lgs. n. 231/2001: responsabilità patrimoniale e vicende modificative dell'ente*, in *Corriere Giuridico*, 2001, n. 11, 1527 ss; Busson, *Responsabilità patrimoniale e vicende modificative dell'ente*, in AA.VV., *Responsabilità degli enti*, *cit.* a cura di Garuti, 183 ss.; Iannacci, *Operazioni straordinarie – Le vicende modificative dell'ente e la responsabilità amministrativa*, in *Diritto e Pratica delle Società*, 2002, n. 3, 12 ss.; Apice, *Responsabilità amministrativa degli enti: profili civilistici*, in *Diritto e Pratica delle Società*, 2002, n. 3, 8 ss; De Angelis, *Responsabilità patrimoniale e vicende modificative dell'ente (trasformazione, fusione, scissione, cessione d'azienda)*, in *Le Società*, 2001, n. 11, 1326 ss.; Napoleoni, *Le vicende modificative dell'ente*, in *Responsabilità degli enti per i reati commessi nel loro interesse*, supplemento al n. 6/03 *Cassazione penale*, 99 ss.

[57] L'art. 4 del d.lgs. 231/2001 prevede quanto segue: "*1. Nei casi e alle condizioni previsti dagli articoli 7, 8, 9 e 10 del codice penale, gli enti aventi nel territorio dello Stato la sede principale rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto. 2. Nei casi in cui la legge prevede che il colpevole sia punito a richiesta del Ministro della giustizia, si procede contro l'ente solo se la richiesta è formulata anche nei confronti di quest'ultimo*".

[58] Art. 7 c.p.: "Reati commessi all'estero - *E' punito secondo la legge italiana il cittadino o lo straniero che commette in territorio estero taluno dei seguenti reati:1) delitti contro la personalità dello Stato italiano; 2) delitti di contraffazione del sigillo dello Stato e di uso di tale sigillo contraffatto; 3) delitti di falsità in monete aventi corso legale nel territorio dello Stato, o in valori di bollo o in carte di pubblico credito italiano; 4) delitti commessi da pubblici ufficiali a servizio dello Stato, abusando dei poteri o violando i doveri inerenti alle loro funzioni; 5) ogni altro reato per il quale speciali disposizioni di legge o convenzioni internazionali stabiliscono l'applicabilità della legge penale italiana*". Art. 8 c.p.: "Delitto politico commesso all'estero - *Il cittadino o lo straniero, che commette in territorio estero un delitto politico non compreso tra quelli indicati nel numero 1 dell'articolo precedente, è punito secondo la legge italiana, a richiesta del Ministro della giustizia. Se si tratta di delitto punibile a querela della persona offesa, occorre, oltre tale richiesta, anche la querela. Agli effetti della legge penale, è delitto politico ogni delitto, che offende un interesse politico dello Stato, ovvero un diritto politico del cittadino. E' altresì considerato delitto politico il delitto comune determinato, in tutto o in parte, da motivi politici.*" Art. 9 c.p.: "Delitto comune del cittadino all'estero - *Il cittadino, che, fuori dei casi indicati nei due articoli precedenti, commette in territorio estero un delitto per il quale la legge italiana stabilisce l'ergastolo, o la reclusione non inferiore nel minimo a tre anni, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato. Se si tratta di delitto per il quale è stabilita una pena restrittiva della libertà personale di*

Il rinvio agli artt. 7-10 c.p. è da coordinare con le previsioni degli articoli da 24 a 25-*undecies* del d.lgs. 231/2001, sicché - anche in ossequio al principio di legalità di cui all'art. 2 del d.lgs. 231/2001 - a fronte della serie di reati menzionati dagli artt. 7-10 c.p., la società potrà rispondere soltanto di quelli per i quali la sua responsabilità sia prevista da una disposizione legislativa *ad hoc*[59];

(iv) sussistendo i casi e le condizioni di cui ai predetti articoli del codice penale, nei confronti dell'ente non proceda lo Stato del luogo in cui è stato commesso il fatto.

1.6 Procedimento di accertamento dell'illecito

La responsabilità per illecito amministrativo derivante da reato viene accertata nell'ambito di un procedimento penale. A tale proposito, l'art. 36 del d.lgs. 231/2001 prevede *"La competenza a conoscere gli illeciti amministrativi dell'ente appartiene al giudice penale competente per i reati dai quali gli stessi dipendono. Per il procedimento di accertamento dell'illecito amministrativo dell'ente si osservano le disposizioni sulla composizione del tribunale e le disposizioni processuali collegate relative ai reati dai quali l'illecito amministrativo dipende"*.

Altra regola, ispirata a ragioni di effettività, omogeneità ed economia processuale[60], è quella dell'obbligatoria riunione dei procedimenti: il processo nei confronti dell'ente dovrà rimanere riunito, per quanto possibile, al processo penale instaurato nei confronti della persona fisica autore del reato presupposto della responsabilità dell'ente (art. 38 del d.lgs. 231/2001). Tale regola trova un contemperamento nel dettato dell'art. 38, comma 2, del d.lgs. 231/2001, che, viceversa, disciplina i casi in cui si procede separatamente per l'illecito amministrativo[61]. L'ente partecipa al procedimento penale con il proprio rappresentante legale, salvo che questi sia imputato del reato da cui dipende l'illecito amministrativo[62]; quando il legale

---

minore durata, il colpevole è punito a richiesta del Ministro della giustizia ovvero a istanza o a querela della persona offesa. Nei casi preveduti dalle disposizioni precedenti, qualora si tratti di delitto commesso a danno delle Comunità europee, di uno Stato estero o di uno straniero, il colpevole è punito a richiesta del Ministro della giustizia, sempre che l'estradizione di lui non sia stata conceduta, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto." Art. 10 c.p.: "Delitto comune dello straniero all'estero – *Lo straniero, che, fuori dei casi indicati negli articoli 7 e 8, commette in territorio estero, a danno dello Stato o di un cittadino, un delitto per il quale la legge italiana stabilisce l'ergastolo, o la reclusione non inferiore nel minimo a un anno, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato, e vi sia richiesta del Ministro della giustizia, ovvero istanza o querela della persona offesa. Se il delitto è commesso a danno delle Comunità europee di uno Stato estero o di uno straniero, il colpevole è punito secondo la legge italiana, a richiesta del Ministro della giustizia, sempre che: 1) si trovi nel territorio dello Stato; 2) si tratti di delitto per il quale è stabilita la pena dell'ergastolo ovvero della reclusione non inferiore nel minimo di tre anni; 3) l'estradizione di lui non sia stata conceduta, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto, o da quello dello Stato a cui egli appartiene*".

[59] Così De Simone, *op. cit.*, 96 ss., il quale fornisce ulteriori ragguagli sulle fattispecie di reato.

[60] Così, testualmente, si esprime la Relazione illustrativa al d.lgs. 231/2001.

[61] Art. 38, comma 2, d.lgs. 231/2001: "*Si procede separatamente per l'illecito amministrativo dell'ente soltanto quando: a) è stata ordinata la sospensione del procedimento ai sensi dell'articolo 71 del codice di procedura penale* [sospensione del procedimento per l'incapacità dell'imputato, n.d.r.]*; b) il procedimento e' stato definito con il giudizio abbreviato o con l'applicazione della pena ai sensi dell'articolo 444 del codice di procedura penale* [applicazione della pena su richiesta, n.d.r.]*, ovvero e' stato emesso il decreto penale di condanna; c) l'osservanza delle disposizioni processuali lo rende necessario*." Per completezza, si richiama inoltre l'art. 37 del d.lgs. 231/2001, ai sensi del quale "*Non si procede all'accertamento dell'illecito amministrativo dell'ente quando l'azione penale non può essere iniziata o proseguita nei confronti dell'autore del reato per la mancanza di una condizione di procedibilità*" (vale a dire quelle previste dal Titolo III del Libro V c.p.p.: querela, istanza di procedimento, richiesta di procedimento o autorizzazione a procedere, di cui, rispettivamente, agli artt. 336, 341, 342, 343 c.p.p.).

[62] "*La ratio della previsione che esclude la possibilità che il rappresentante dell'ente sia la stessa persona imputata del reato appare evidente: posto che al primo soggetto spetta il compito di assicurare all'ente le prerogative difensive nel procedimento relativo all'illecito, la potenziale conflittualità tra gli interessi delle due figure potrebbe rendere inconciliabili le linee di difesa. Se così è, non pare dubbio che il medesimo divieto debba operare anche quando il legale rappresentante dell'ente sia imputato di un reato connesso o collegato a quello dal*

rappresentante non compare, l'ente costituito è rappresentato dal difensore (art. 39, commi 1 e 4, del d.lgs. 231/2001)[63].

1.7 Il Modello di organizzazione, gestione e controllo per la prevenzione dei reati

Poiché l'obiettivo della norma è non solo punire ma anche prevenire la commissione di reati, il legislatore ha stabilito in alcune ipotesi una esimente generale, in altre una riduzione di pena, in presenza di un sistema di prevenzione idoneo.

In particolare, l'articolo 6 del Decreto, nell'introdurre il suddetto regime di responsabilità amministrativa, prevede una forma specifica di esenzione da detta responsabilità qualora l'ente, in caso di reato commesso da un soggetto in posizione apicale, dimostri che:

a) l'organo dirigente dell'ente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo;

c) le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti modelli di organizzazione e gestione;

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

Si ha esclusione della responsabilità ove le predette condizioni ricorrano, nel loro complesso, al momento della commissione del reato o illecito; tuttavia anche l'adozione e l'attuazione del modello avvenute in un momento successivo alla commissione del reato o illecito svolgono comunque effetti positivi in ordine alle sanzioni irrogabili all'ente (artt. 12 e 17 del Decreto).

Nel caso, invece, di un reato commesso da soggetti sottoposti all'altrui direzione o vigilanza, la società risponde se la commissione del reato è stata resa possibile dalla violazione degli obblighi di direzione o vigilanza alla cui osservanza la società è tenuta[64]. A tal proposito, tuttavia, l'articolo 7 del d.lgs. 231/2001 stabilisce che la violazione degli obblighi di direzione o vigilanza è esclusa se la società, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, gestione e controllo idoneo a prevenire i reati della specie di quello verificatosi.

Il Decreto individua le esigenze a cui debbono rispondere i modelli di organizzazione, gestione e controllo in relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, dettando nella sostanza lo schema di detti modelli, e cioè:

a) individuare le attività nel cui ambito possono essere commessi reati;

b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

---

quale dipende l'illecito amministrativo"; così Ceresa- Gastaldo, *Il "processo alle società" nel d.lgs. 8 giugno 2001, n. 231*, Torino, 24.

[63] "*Ove il rappresentante legale dell'ente sia altresì imputato del reato da cui dipende l'illecito amministrativo, la partecipazione al procedimento penale dell'ente stesso dovrà necessariamente avvenire mediante la nomina di un diverso rappresentante legale per il processo*" (Garuti, in AA.VV., *Responsabilità degli enti*, *cit*., 282 s.).

[64] A tal proposito vedi, tra le altre, la decisione del Tribunale di Milano del 27 aprile 2004 secondo la quale "*Perché possa configurarsi la responsabilità dell'ente per i reati commessi da soggetti sottoposti all'altrui direzione e vigilanza (art. 5, comma 1, lett. b)) è necessario che, ai sensi dell'art. 7 del d.lgs. n. 231 del 2001, la commissione del reato sia stata resa possibile dalla violazione degli obblighi di vigilanza e controllo alla cui osservanza la struttura è tenuta*"

c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;

d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;

e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Inoltre, esso stabilisce che il modello può essere efficacemente attuato solo a fronte di:

a) una verifica periodica del modello e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;

b) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

1.8 Caratteristiche dei modelli organizzativi ai sensi dell'art. 30 del d.lgs. n. 81/2008 (cosiddetto "Testo Unico sulla sicurezza")

Sin da subito si è posto il problema interpretativo del rapporto tra i modelli di organizzazione e controllo previsti dal d.lgs. 231/2001 e le specifiche regole cautelari esistenti in materia di sicurezza sul lavoro basate già su di una articolata *"procedimentalizzazione"* volta al contenimento dei rischi di infortunio sul lavoro[65].

Il coordinamento tra la disciplina sulla responsabilità amministrativa delle società (d.lgs. 231/2001) e quella propria della *"salute e sicurezza sul lavoro"* è oggi realizzato dall'art. 30 del Testo Unico sulla sicurezza (d.lgs. 81/2008), con il quale il legislatore stabilisce in modo esplicito quali sono le caratteristiche che il modello deve presentare per avere efficacia esimente della responsabilità amministrativa delle persone giuridiche *ex* d.lgs. 231/2001.

L'art. 30 si colloca all'interno della Sezione II del Capo III del d.lgs. 81/2008, laddove viene disciplinata la specifica fase della valutazione dei rischi, a dimostrazione dello stretto rapporto esistente tra la fase di *risk assessment* e i modelli di organizzazione e gestione, confermando che solamente sulla base di un approfondito *risk assessment* può essere costruito un idoneo sistema di "governo del rischio".

Il risultato della valutazione del rischio (quale previsto anche dall'art. 6, comma 2 lett. a) e dall'art. 7 comma 3 del d.lgs. 231/2001) deve d'altronde porre in evidenza quelle che sono le attività aziendali in relazione alle quali risulti possibile la commissione dei reati sopra richiamati per violazione delle norme antinfortunistiche (*"attività sensibili"*), e quindi i profili delle medesime attività che postulino la necessaria osservanza della legge, la predisposizione di presidi cautelari finalizzati a rilevare tempestivamente le situazioni di rischio, individuando - conseguentemente - le disposizioni normative di prevenzione pertinenti.

E' chiaro, quindi, che il primo requisito che il modello di organizzazione, gestione e controllo deve avere, al fine di evitare la commissione di infortuni sul lavoro o, comunque, al fine di avere efficacia esimente della responsabilità amministrativa delle società per i reati in materia antinfortunistica *ex* art. 25-*septies*, è quello di assicurare il rispetto della normativa in materia prevenzionale.

[65] Aldovrandi, *I "modelli di organizzazione e gestione" nel D.Lgs. 8 giugno 2001, n.231: aspetti problematici "dell'ingerenza penalistica" nel "governo" delle società* in *Relazione presentata al convegno "Corporate Governarce – strutture ed esperienze a confronto*, tenutosi presso l'Università degli Studi di Milano Bicocca il 7 giugno 2007.

E così il comma 1 dell'art. 30 del d.lgs. 81/2008 afferma che il modello di organizzazione e gestione deve assicurare, prioritariamente e come precondizione, la conformità normativa della società a quelli che sono gli obblighi di prevenzione in materia di sicurezza e salute ed, in particolare, l'adempimento di tutti gli obblighi giuridici relativi:

"a) al rispetto degli standard tecnico-strutturali di legge relative ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;

c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazione dei rappresentanti per la sicurezza;

d) alle attività di sorveglianza sanitaria;

e) alle attività di informazione e formazione dei lavoratori;

f) alle attività di vigilanza con riferimenti al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate".

E' pertanto necessario che la società, sulla base dei propri processi aziendali (normali, anomali, comprese le potenziali situazioni di emergenza) predisponga delle procedure idonee a garantire la conformità dei propri comportamenti al rispetto della legislazione vigente, tracciandone, con apposita registrazione, l'avvenuta effettuazione dell'attività di controllo (art. 30, comma 2).

Al pari, è necessario che il modello organizzativo preveda una articolazione di funzioni atta ad assicurare la salvaguardia degli interessi protetti.

Organizzare la sicurezza - infatti - significa assicurare un risultato in modo stabile, mediante l'adozione di misure appropriate ed il loro eventuale aggiornamento tramite la cooperazione di più soggetti che - sulla base della valorizzazione delle necessarie competenze differenziate - si dividono il lavoro ripartendosi i compiti.

La società - quindi - in relazione alla natura, dimensioni e tipo di attività svolta, deve stabilire come organizzare – dal punto di vista funzionale – le attività di gestione**,** individuando quali compiti devono essere svolti da parte di ogni attore che partecipa ai processi decisionali (art. 30, comma 3).

La struttura funzionale organizzativa, con compiti e responsabilità in materia di salute e sicurezza sul lavoro, deve essere formalmente definita, a partire dal datore di lavoro fino a raggiungere ogni singolo lavoratore riservando particolare attenzione alle figure specifiche previste dalla normativa di riferimento (es. responsabile del servizio di prevenzione e protezione, medico competente, addetto al primo soccorso, ecc.).

Tale definizione funzionale dovrà assicurare, per ogni figura individuata, le competenze tecniche, i poteri necessari per la verifica, valutazione, gestione e controllo del rischio.

Inoltre, il modello organizzativo in materia di salute e sicurezza sul lavoro deve prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate (art. 30, comma 4).

Tale sistema di controllo deve essere in grado di:

- verificare l'adeguatezza del modello in ordine alla sua reale capacità di prevenire i reati in materia antinfortunistica;
- vigilare sull'effettività del modello (verifica della coerenza tra i comportamenti concreti ed il modello istituito);

- analizzare il mantenimento nel tempo delle condizioni di idoneità delle misure preventive adottate;
- aggiornare il modello quando *"siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico"* (art. 30, comma 4, secondo periodo).

Si fa ancora presente che il comma 5 del citato art. 30 stabilisce che: "*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 (SGSL) 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 (...)*".

Di particolare rilevanza risulta poi la modifica dell'art. 51 del d.lgs. 81/2008 da parte dell'art. 30, comma 1, lettera a), del d.lgs. 3 agosto 2009, n. 106, recante "*Disposizioni integrative e correttive del decreto legislativo 9 aprile 2008, n. 81, in materia di tutela della salute e della sicurezza nei luoghi di lavoro*", il quale, con l'introduzione del comma 3-*bis*, ha previsto la possibilità per le imprese di richiedere l'asseverazione dell'adozione e dell'efficace attuazione dei modelli di organizzazione e gestione della salute e sicurezza sul lavoro da parte di organismi paritetici costituiti a iniziativa di una o più associazioni dei datori e dei prestatori di lavoro comparativamente più rappresentative sul piano nazionale[66].

Infine, è appena il caso di segnalare che, a differenza di quanto verificatosi con riferimento ai reati in materia di tutela della salute e sicurezza sul lavoro, l'estensione della responsabilità amministrativa degli enti ai reati ambientali non è stata accompagnata da previsioni relative all'individuazione di un contenuto minimo dei modelli organizzativi ritenuti idonei a prevenire i reati ambientali né ha stabilito una presunzione di conformità legale per i modelli definiti conformemente a norme tecniche o standard internazionali piuttosto che alle certificazioni volontarie ambientali (ad esempio, ISO 14001 – EMAS)[67] già adottate da numerose imprese italiane.

Peraltro le predette certificazioni in materia ambientale rappresentano un elemento preventivo fondamentale da tenere in considerazione nell'ambito della definizione dei modelli organizzativi volti a prevenire i reati ambientali in questione.

1.9 Codici di comportamento predisposti dalle associazioni rappresentative degli enti

L'art. 6, comma 3, del d.lgs. 231/2001 prevede "*I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati"*.

[66] Per "organismi paritetici" si deve far riferimento alla definizione contenuta nell'art. 2, comma 1, lett. ee) del d.lgs. 81/2008, secondo la quale si tratta di "*organismi costituiti a iniziativa di una o più associazioni dei datori e dei prestatori di lavoro comparativamente più rappresentative sul piano nazionale, quali sedi privilegiate per: la programmazione di attività formative e l'elaborazione e la raccolta di buone prassi a fini prevenzionistici; lo sviluppo di azioni inerenti alla salute e alla sicurezza sul lavoro; l'assistenza alle imprese finalizzata all'attuazione degli adempimenti in materia; ogni altra attività o funzione assegnata loro dalla legge o dai contratti collettivi di riferimento*".

[67] Critica questa scelta Confindustria ("*Osservazioni di Confindustria allo Schema di decreto legislativo approvato in via preliminare nel corso del Consiglio dei Ministri del 7 aprile 2011*", pag. 7 e ss.), che rileva: "*in considerazione della complessità della disciplina ambientale e per evidenti esigenze di certezza degli operatori auspica la definizione di requisiti minimi ... sancendo la presunzione di idoneità dei modelli organizzativi definiti conformemente alla norma Uni ISO 14001 ovvero al Regolamento EMAS, o modelli equivalenti*".

In ottemperanza a quanto disposto dall'art. 6, comma 3, del d.lgs. 231/2001, Confindustria ha per prima emanato un codice di comportamento per la costruzione dei modelli di organizzazione, gestione e controllo (*Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001*) fornendo, tra l'altro, le indicazioni metodologiche per l'individuazione delle aree di rischio e la struttura del modello di organizzazione, gestione e controllo.

Sul punto le Linee guida di Confindustria suggeriscono di utilizzare i processi di *risk assessment* e *risk management* e prevedono le seguenti fasi per la definizione del modello di organizzazione, gestione e controllo:

- identificazione dei rischi;
- progettazione di un sistema di controllo preventivo;
- adozione di alcuni strumenti generali tra cui i principali sono un codice etico e un sistema disciplinare;
- individuazione dei criteri per la scelta dell'organismo di controllo.

1.10 Sindacato di idoneità

L'accertamento della responsabilità della società, attribuito al giudice penale, avviene mediante:

- la verifica della sussistenza del reato presupposto per la responsabilità della società; e
- il sindacato di idoneità sui modelli organizzativi adottati.

Il sindacato del giudice circa l'astratta idoneità del modello organizzativo a prevenire i reati di cui al d.lgs. 231/2001 è condotto secondo il criterio della c.d. "prognosi postuma".

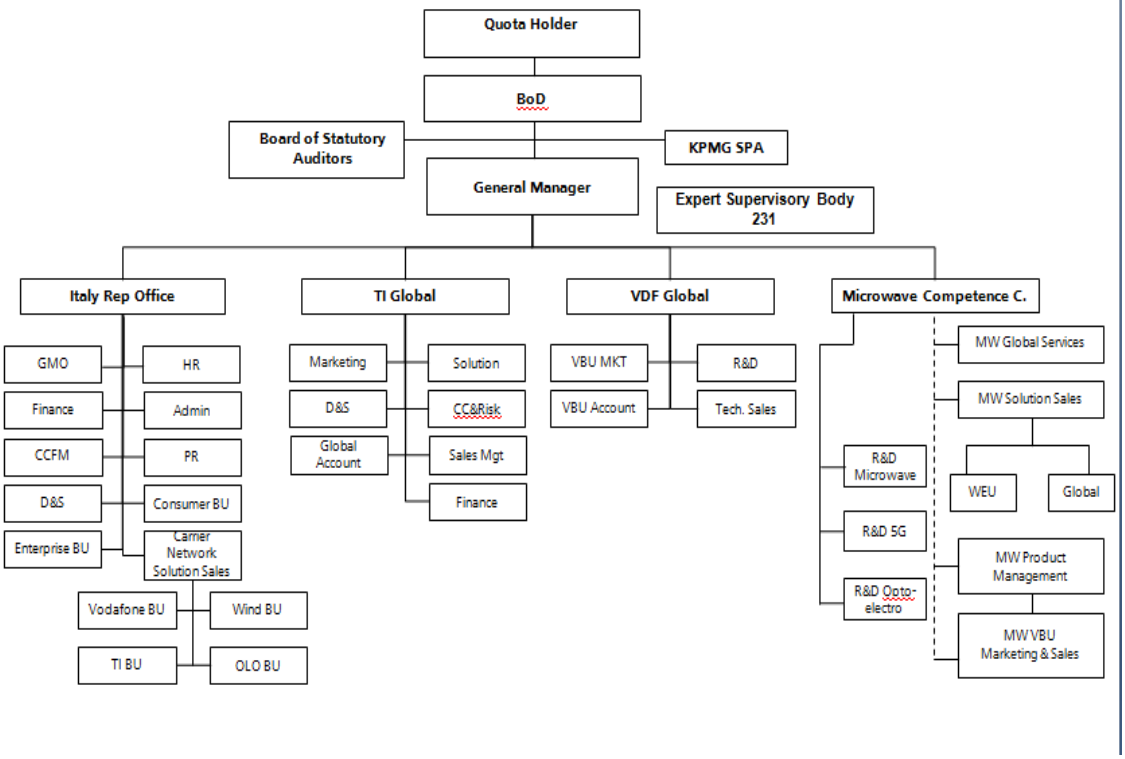
Il giudizio di idoneità va formulato secondo un criterio sostanzialmente *ex ante* per cui il giudice si colloca, idealmente, nella realtà aziendale nel momento in cui si è verificato l'illecito per saggiare la congruenza del modello adottato[68].

In altre parole, va giudicato "idoneo a prevenire i reati" il modello organizzativo che, prima della commissione del reato, potesse e dovesse essere ritenuto tale da azzerare o, almeno, minimizzare, con ragionevole certezza, il rischio della commissione del reato successivamente verificatosi[69].

[68] Paliero, *La responsabilità della persona giuridica per i reati commessi dai soggetti in posizione apicale*, Relazione tenuta al convegno Paradigma, Milano, 2002, p. 12 del dattiloscritto. Rordorf, *La normativa sui modelli di organizzazione dell'ente*, in *Responsabilità degli enti*, *cit.*, supplemento al n. 6/03 *Cassazione penale*, 88 s.

[69] In tal senso, Amato, nel commento all'ordinanza 4-14 aprile 2003 del GIP di Roma, in *Guida al diritto n. 31 del 9 agosto 2003*.

ALLEGATO 1
ORGANIGRAMMA



ALLEGATO 2
BUSINESS CODE OF CONDUCT

Business Code of Conduct

Objectives

This Business Code of Conduct outlines Huawei's approach to an individual's code in relation to business, together with an action plan which details how Huawei will achieve a professional and ethical working environment, which is inclusive and maximises the potential of all staff and clients.

Scope

This Business Code of Conduct applies to:

1) all local Italian officers and employees, including those local employees working for the EU Region, HQ, Vodafone Business Unit etc.; and

2) all expatriate employees with a work permit/visa working in the Italy including those expatriate employees working for the EU Region, HQ, Vodafone Business Unit etc; and

3) contractors, temporary workers, agency staff, agents and anyone retained, engaged or appointed to act on behalf of Huawei.

("Staff" or "You")

Statement of Trust

Huawei ethos since its early years can be summarised in one word – "Trust", a core value which Huawei advocates at all times.

Huawei promises to be honest and trustworthy to customers and its Staff in all aspects of its business interests and to encourage the promotion of harmony as part of the Company's growth and development. The Company believes that trust as the core value, whilst being invisible, is an asset which makes up Huawei competitive edge and trust culture will result in long-lasting efforts by all employees and continued commitment from its customers.

Basic Conduct Guidelines

It is essential that Staff should be seen to keep their promises, work in a professional and ethical manner.

- Comply with all applicable laws and regulations in each of the countries in which Huawei's business operations, including any laws, standards and principles relating to anti-bribery;
- Be honest, diligent and trustworthy in the treatment of all Huawei business activities and relationships;
- Protect and use Huawei assets in an appropriate manner and respect others' intellectual property rights;
- Uphold Huawei interests and ensure that personal interests do not take priority over the interests of the Company;

Guidelines for Ethical Behaviour

Business Activities and Relationships

Huawei Staff shall conduct their business in a lawful and ethical manner at all times while conducting business activities and dealing with business relationships.

Anti-bribery and Corruption

Huawei recognises that corruption can have a detrimental effect on society by undermining legal systems; damaging social and economic development; and free and fair competition. Huawei is committed to carrying out our business in an honest and ethical manner which is reflected within our business principles that form the foundation of our Company.

Huawei has a zero tolerance of bribery and corruption. Huawei will comply in all respects with all applicable domestic and international laws, standards and principles relating to anti-bribery in each of the countries in which Huawei trades, operates or has any other activity.

We are committed to the following:-

- To carry out our business fairly, honestly and transparently;
- To not make or receive bribes, or condone the offering of bribes on our behalf, so as to gain or retain a business advantage;
- Avoid doing business with others who do not accept our principles and who may harm our reputation;
- Keep transparent and updated records;
- Make sure that everyone in our business knows and adheres to our principles; and
- Keep our principles even when it becomes difficult.

Staff are referred to Huawei's Anti-bribery and Corruption Policy（which is published on W3 and available from HR upon request） for further guidance. Any Huawei Staff member who is found to be giving or taking bribes or any other acts of corruption, will be subject to disciplinary action which may lead to dismissal on the

grounds of Gross Misconduct (if not a Huawei employee, the procedure shall involve a review and the likely summary termination of the responsible individual's appointment to Huawei and/or contract) and, if appropriate, criminal proceedings.

Gifts and hospitality

Huawei Staff must not solicit gifts or hospitality in any circumstances. As a general principle, we discourage Staff from accepting gifts or hospitality from a business partner.

Notwithstanding this, Huawei recognises that the occasional acceptance or offer of modest gifts and hospitality may be a legitimate contribution to good business relationships. However, it is important that gifts or hospitality shall be suitable for the conduct of normal business relationships and shall never influence business decision-making processes, or cause others to perceive as an influence. The prohibitions against accepting or paying bribes and the avoidance of conflicts of interest should always be taken into consideration.

You shall make sure you get the right approvals before you either offer or accept gifts or hospitality and register any gifts or hospitality that are offered to or accepted by you.

You may never accept or offer the following with or without approval:

- Illegal gifts or hospitality;
- Gifts or hospitality that is of an inappropriate nature or in inappropriate venues or that might adversely affect Huawei's reputation;
- Gifts or hospitality that the giver knows are prohibited by the recipient's organisation;
- Cash or cash equivalents such as gift vouchers, stocks, loans or options;
- Travel arrangement for the purpose of tourism, flight upgrading;
- Job arrangement for a relative of a customer (except where the job offer is made via a fair, public and formal recruitment and selection procedure);
- Personal services;
- Gifts or hospitality during a tender exercise or during periods when important business decisions are being made.

Staff are referred to Huawei's Gifts and Hospitality Policy （which is published on W3 and available from HR upon request） for detailed guidance on the acceptance and offering of gifts and hospitality. It is the responsibility of each Huawei Staff member to familiarise themelf with Huawei's Gifts and Hospitality Policy and processes and to act in accordance and compliance with it. Huawei requires Staff abide by these rules not only to protect our reputation and efforts to reduce and eliminate bribery and corruption in business worldwide, but also to protect the individual Staff member against unfounded allegations of improper behaviour.

Promotion and Commitment

Staff who are involved with Advertising and Marketing should make sure that promotional literature is accurate and truthful in regards to the promotion of the Company's product and services.

The Selection of Suppliers

Huawei requires its Staff to maintain professional and lawful relationships with all its suppliers, including business partners such as agents, distributors, joint ventures or allies. Meanwhile, Huawei will require its business partners to accept and honor the Huawei Code of Business Conduct.

Selection of suppliers will be based on objective business criterion and where member of Staff does not have the expert knowledge of the professional area of the supplier, they must seek an advice from a member of Staff who does.

Ensuring Fair Transactions

Staff must not entrust business to a supplier owned or managed by his/her relative or close friend. If a member of Staff's relative has interests in one of Huawei suppliers, the Company will not enter into any form of business partnership with the supplier.

Business information of suppliers and other business partners must be kept confidential. Product conditions and quotations as well as Huawei assessment of suppliers are all trade secrets. No trade secret shall be disclosed to any other supplier.

Respecting Differences

Cultural differences and religious beliefs among customers, suppliers, business partners and their staff from all over the world must be respected at all times.

Complying with Local Country Laws and International Rules and Regulations

The Huawei business reaches many countries worldwide and its Staff consist or many different nationalities and ethnicities with many different beliefs. As a global operator we must ensure that our business operations are in compliance with the laws of local countries, regions, or regional economic communities, international practice and recognised standards. These laws or standards deal with a wide range of aspects, including investment, trade, foreign exchange, labor, environment, contract, consumer protection, bribery and corruption, intellectual property right, accounting and taxation.

- Staff will ensure that they understand and observe the laws and regulations relating to trade secret, proprietary information and other intellectual property rights, and respect others' effective intellectual property rights. Avoid improper economic or criminal practices relating to the use of others' intellectual property rights.
- Understand and comply with the regulations and conventions in relation to human rights recognised by the International Community.
- Ensure that fair employment opportunities are being offered and that recruitment, employment, and promotion of employees are based solely on

individual talents, qualifications and achievements.

- Private and/or personal information on Staff shall be properly used, stored and transferred in line with the company's related rules and the local country Data Protection laws. Privacy rights of all Staff must be respected.
- Understand and comply with the laws governing bribery and corruption in line with the company's related policy. Bribery in any form is strictly prohibited.
- Understand and comply with laws and regulations governing environmental protection, health and safety; create and maintain a safe working environment.
- In the event of any conflict between the laws applicable to two or more countries, be sure to consult the Huawei **Legal Department** and make sure how to deal with such conflict properly and lawfully.

Protecting Huawei Assets

It is prohibited to fraudulently prepare false contracts or relevant business documents, steal property from the Company, intentionally claim private, non-business related expenses, make double claims for a single expense or report false account. Technology and trade secrets are amongst Huawei's most important assets and it is the duty of all the Company's Staff to protect all the physical assets, financial assets, information assets and other invisible assets in the possession of Huawei. If You suspect that information is being disclosed by a third party, You have a duty to report the breach to the manager of the department in which you work, or Huawei's Compliance Officer.

Protecting Intellectual Property Rights (IPR)

Huawei's **Intellectual Property Rights include without limitation patents, trademarks, copyrights, trade secrets and other proprietary information. All Staff must observe Huawei's information security policies, protect and use Huawei intellectual property rights according to law.**

- **Intellectual property rights created by Staff during working hours are Huawei property. The Staff member shall provide the Intellectual Property Right Department with copies of any patent that he/she has applied for or obtained. The Staff member shall return the media and copies in his/her hands which contain Huawei proprietary information when he/she leaves the company. After the Staff member leaves the Company, these intellectual property rights shall remain the property of Huawei and the Staff member will continue to be bound by their ongoing obligations of confidentiality regarding the proprietary information.**
- Before applying for patents with the assistance of the Intellectual Property Right Department, an Staff member must not present or disclose any information relating to a new product or service without authorization. In the development or use of a new product or service name, make sure if any IPR-related issue persists.
- Every Staff member must use all due skill and diligence to avoid the inadvertent disclosure of **proprietary information such as intellectual property rights. You should never discuss with any unauthorised person including family members, friends, customers or suppliers about any proprietary information** Huawei has not

made public.

Staff must not disclose any inside information unless expressly instructed to do so by the manager of the department in which they work in order to fulfill a business need. Where the Staff member is unsure in the case of IPR disclosure, he/she shall consult the **Legal Department**. This inside information includes but not limited to any non-public information in connection with Huawei:

- Imminent acquisitions or combinations, transfer, establishment of a joint venture or associate; winning or terminating an important contract; winning or losing an important customer or supplier; major action or claim; change of profits or dividends distribution policy; and major product development projects.

Financial Control

All Staff shall observe the Company's finance systems and approval procedures at all times. Staff must make concerted efforts to create a safe and efficient financial environment through their commitments to financial control.

- Be sure to claim for actually incurred expenses lawfully within the specified limit, and avoid any improper expense claim. Staff must provide accurate financial records, claim expenses in line with Huawei's internal financial policies and approval procedures.
- Where a Staff member's financial submissions appear to be inconsistent, the issue will be raised with the manager of the department in which they work..
- Administrators in a new business department or an overseas organisation with only a small number of Staff members should establish appropriate financial procedures or control policies in time, to ensure the security of the Company's funds.

Protecting other Assets

Staff who are employees are not permitted to work for any other employer without the express written permission of the Company. Staff who are employees are not allowed to perform work which does not relate to the business of the Company during working hours or use the Company's office equipment such as computer, email box or telephone for non work-related purposes.

What would constitute as a conflict between Company and personal interests?

In respect of Staff who are employees, the following acts are considered violations of professional ethics: taking a second job (such as buying stocks, running a company or holding shares of another company, or work part time); participating in activities other than the company's business or receiving commissions or payments by taking advantage of one's position, especially any activity that would be considered as in competition with Huawei to the detriment of the Company's interest.

Where an Staff member holds shares in a Huawei competitor prior to joining Huawei, it will be the responsibility of that Staff Member to disclose this information – in writing- to the Company within 3 months from date of employment, engagement or appointment (as appropriate).

Without prior approval, Staff may not, in any form during the course of their employment, work or appointment to Huawei compete with Huawei or assist or work indirectly for Huawei competitors. If You are uncertain as to whether your behavior competes against Huawei, do consult your immediate supervisor or the **HR Department**.

- No Staff shall improperly or unlawfully use their position or influence within the Company, to promote or assist in other outside business or activity.
- Without prior authorisation and approval of the company, Staff shall not do any of the following:

  Conduct an inspection tour, carry out a negotiation, sign an agreement, invite or submit a tender, or make a competitive auction in the name of the company;

  Provide guarantee or proof in the name of the company;

  Publish opinions or information in any news media in the name of the company; or

  Attend public activities on behalf of the company.

Once employee Staff member has left the Company the Staff member will still be bound by their contractual post termination restrictions and their post termination duties and restrictions under law such as the duty of confidentiality.

Personal Investments

Personal investments made by a Huawei Staff member must not influence that person's independent judgment in performing duties on behalf of Huawei.

- Without approval of the Company, Staff shall not invest in any organisation associated with Huawei, including suppliers, competitors, customers, distributors and partners.
- Staff may not buy or sell stocks or securities using inside information or instruct or prompt others to do so.
- Staff must not disclose any such information to a third party either directly or indirect in order to make investments in order to seek profit from the Company.

Should employee Staff Member be found to undertake such an action the Company will take appropriate action which may include reporting the matter to the appropriate authorities.

Personal Behaviors

A Staff member's character and personal integrity will have direct influence on Huawei's image and reputation, therefore, any of the following behaviors are strictly prohibited:

- Behaviors that could be considered sexual harassment;

- Any form of verbal abuse
- Any violation of local criminal law.

Whistle Blowing

Any Huawei Staff Member who has a reasonable belief that a person has failed, is failing or is likely to fail to comply with a particular legal, obligatory or regulatory obligation – for the purposes of this Business Code of Conduct this include a breach of this Business Code of Conduct, the Anti-Bribery and Corruption Policy, or the Gifts and Hospitality Policy, should disclose the matter confidentially to the manager of the department in which they work.. If the matter is more serious or if You feel your concern has not been addressed, or if you prefer not to raise it with them for any reason, you should contact Huawei's Compliance Officer or the General Manager. You may also raise the matter anonymously to the following addresses:

NOTES: BCG complain/Huawei
Email: BCGcomplain@huawei.com

Huawei will always ensure that no Staff member will be subjected to any detriment or less favourable treatment for refusing to engage in or reporting in good faith any actual or suspected questionable conduct. Staff are referred to Huawei's Whistle Blowing Policy （which is published on W3 and available from HR upon request） for further guidance.

Review of Policy

Huawei is responsible for the interpretation and administration of the requirements set out in this Business Code of Conduct. The company reserves the right to amend this document and procedure from time to time or as may be required under the laws and regulations of Italy.

HUAWEI TECHNOLOGIES ITALIA S.R.L.

Modello di organizzazione, gestione e controllo ai sensi del d.lgs. 231/2001

PARTE SPECIALE

Approvato con delibera del Consiglio di Amministrazione del 9 Novembre 2014

INDICE

PREMESSA

I Protocolli di controllo

La struttura della presente Parte Speciale prevede l'illustrazione dei presidi finalizzati alla prevenzione del rischio di commissione delle violazioni rilevanti ai fini della responsabilità amministrativa degli enti *ex* d.lgs. 231/2001, ai quali si affiancano le previsioni del Business Code of Conduct.

Tali presidi si articolano su due livelli di controllo:

- protocolli generali delle attività, che sono sempre presenti in tutte le attività sensibili e strumentali prese in considerazione dal Modello;
- protocolli specifici, che prevedono disposizioni particolari volte a disciplinare gli aspetti peculiari delle attività sensibili e strumentali.

I protocolli prevedono sia disposizioni immediatamente precettive, sia disposizioni che trovano invece attuazione nella normativa aziendale (es. procedure, circolari, ecc.).

I protocolli generali di controllo delle attività sono:

a) Segregazione delle attività: l'esercizio delle attività sensibili e strumentali è realizzato in osservanza del principio di segregazione tra chi esegue, chi controlla e chi autorizza.

b) Norme: la Società adotta e applica disposizioni organizzative idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività sensibile/strumentale in conformità alle prescrizioni del Modello.

c) Poteri di firma e poteri autorizzativi: l'esercizio di poteri di firma e poteri autorizzativi interni avviene sulla base di regole formalizzate a tal fine introdotte.

d) Tracciabilità: i soggetti, le funzioni interessate e/o i sistemi informativi utilizzati assicurano l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati che supportano la formazione e l'attuazione delle decisioni della Società e le modalità di gestione delle risorse finanziarie.

e) Sicurezza informatica: il trattamento informatico dei dati è operato in osservanza di adeguate misure di sicurezza, quali quelle contenute nel d.lgs. 196/2003, negli standard internazionali in materia di sicurezza delle informazioni e nelle *best practice* di riferimento.

f) Obbligo di collaborazione: il soggetto che intrattiene rapporti o effettua negoziazioni con soggetti pubblici[1] è obbligato alla massima correttezza, collaborazione e trasparenza nei rapporti con tali soggetti. Tutte le azioni, le operazioni, le negoziazioni e, in genere, i comportamenti posti in essere nello svolgimento dell'attività sensibile, devono essere improntati ai principi di correttezza, integrità, legittimità e chiarezza. Qualsiasi informazione e/o comunicazione destinata a soggetti pubblici deve essere accurata, veritiera, corretta, completa, chiara, puntuale e sempre rigorosamente conforme a quanto previsto dalle disposizioni applicabili.

[1] Si precisa che per "soggetti pubblici" devono intendersi gli esponenti della P.A. o altri soggetti la cui qualificazione sia comunque riconducibile alla nozione di pubblico ufficiale o incaricato di pubblico servizio (si veda *infra* la premessa del Capitolo 1).

La presente Parte Speciale si compone di 5 capitoli ciascuno dedicato a una categoria di violazioni rilevanti ai fini della responsabilità amministrativa degli enti, che la Società ha stabilito di prendere in considerazione in ragione delle caratteristiche della propria attività.

La struttura di ogni capitolo è caratterizzata dall'associazione tra fattispecie di reato[2], attività sensibili (e strumentali) individuate dalla Società con riferimento alle predette fattispecie di reato e protocolli specifici.

Nell'Allegato 1 alla presente Parte Speciale, sono, inoltre, indicate le funzioni aziendali coinvolte nelle singole attività sensibili e strumentali individuate.

I protocolli generali e specifici sono stati definiti utilizzando come riferimento le Linee guida di Confindustria, quelle a oggi pubblicate dalle principali associazioni di categoria e le *best practice* internazionali.

Si rileva, infine, che nel caso in cui un'attività sensibile/strumentale individuata dalla Società sia, in tutto o in parte, svolta da soggetti terzi in nome e/o per conto della Società, trovano applicazione – in sostituzione e/o a complemento dei protocolli specifici previsti per le singole attività – i seguenti protocolli:

- Contratti: per ogni attività sensibile/strumentale affidata, in tutto o in parte, in *outsourcing* è stipulato uno specifico contratto che disciplina lo svolgimento di tale attività e definisce i livelli di servizio (SLA – *Service Level Agreement*) in modo dettagliato e analitico, in modo da delineare chiaramente le attività di competenza della Società e quelle di competenza dell'*outsourcer* e regolare le modalità secondo le quali, in conformità alle prescrizioni del Modello, l'attività deve essere eseguita da parte dell'*outsourcer*.
- Referente: con riferimento a ogni attività affidata, in tutto o in parte, in *outsourcing* è individuato, all'interno della Società, un soggetto/funzione responsabile del rispetto delle disposizioni contenute nel *Service Level Agreement* (norme contrattuali, livelli di servizio), a presidio delle responsabilità facenti capo alla Società con riferimento all'attività affidata all'esterno.
- Clausole *ad hoc*: nei contratti di servizio stipulati con soggetti terzi sono previsti richiami alla disciplina prevista dal Modello per lo svolgimento dell'attività sensibile e sono inserite clausole risolutive espresse volte a sanzionare comportamenti, da parte dei soggetti terzi, contrari alle previsioni contenute nel Modello.
- Presidi di controllo: nei contratti di servizio i soggetti terzi, cui è affidata da parte della Società – in tutto o in parte – la gestione dell'attività, si impegnano a dotarsi di misure idonee a prevenire il rischio di commissione delle violazioni rilevanti ai fini della responsabilità amministrativa *ex* d.lgs. 231/2001, che potrebbero essere ascritti alla Società.

II Sistema delle deleghe e dei poteri di firma

La Società è dotata di un sistema di poteri interni (c.d. deleghe) ed esterni (c.d. poteri di firma) illustrato nei documenti qui di seguito indicati, nelle versioni di volta in volta vigenti, disponibili agli atti della Società e accessibili da chiunque abbia legittimo interesse:

(i) statuto;

(ii) organigramma;

(iii) job descriptions;

[2] La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati *ex* art. 5 del d.lgs. 231/2001 è collegato il regime di responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

(iv) deleghe (a efficacia interna);

(v) poteri di firma (a efficacia esterna).

Il Consiglio di Amministrazione è l'organo competente a conferire e approvare qualsiasi delega o potere di firma, i quali vengono assegnati in coerenza con le responsabilità di ciascun soggetto, con indicazione delle soglie di approvazione delle spese, in coerenza con l'organigramma aziendale.

Le deleghe e le procure sono formalizzate per iscritto.

In particolare, le procure sono conferite mediante atti notarili, comunicate al destinatario e registrate presso il competente ufficio del registro delle imprese.

Il complesso della documentazione sopra indicata è tenuto e aggiornato a cura delle funzioni legale e HR.

Il sistema dei poteri di firma è in ogni momento caratterizzato dal conferimento di poteri di firma ai soggetti dotati delle necessarie competenze ed è coerente con il sistema delle deleghe interne.

III Gestione delle risorse finanziarie

Si rileva che il sistema di gestione delle risorse finanziarie, oltre a essere espresso dai protocolli che danno attuazione ai principi di "Tracciabilità" e "Segregazione delle attività" (quest'ultimo relativamente alla separazione dei compiti e alla contrapposizione di funzioni), trova manifestazione anche nell'ambito del sistema delle deleghe, istituito dalla Società in ossequio al protocollo "Poteri di firma e poteri autorizzativi**"**, che prevede differenziazione delle soglie di approvazione delle spese in capo a soggetti diversi e modalità di esercizio della firma sociale nell'autorizzazione di operazioni finanziarie.

La Società adotta procedure per autorizzare l'esecuzione di qualsiasi pagamento alla o da parte della Società ispirate al principio generale che la funzione che autorizza l'esecuzione del pagamento o dell'incasso, previa verifica della sussistenza di adeguata causa ed evidenza documentale, sia diversa da quella che decide la relativa operazione.

IV Operazioni a rischio e Procedure

Per operazione a rischio (di seguito, "**Operazione**") si intende qualsiasi operazione il cui compimento richiede l'esecuzione di un'attività sensibile o strumentale indicata nella presente Parte Speciale.

In attuazione dei protocolli di controllo indicati in ciascun capitolo della presente Parte Speciale con riferimento a ciascuna categoria di violazioni rilevanti ai fini del d.lgs. 231/2001, il compimento di ciascuna Operazione è regolato da procedure, che disciplinano i processi a rischio coinvolti in tale Operazione (le "**Procedure**").

Le Procedure sono approvate dalle competenti funzioni aziendali e sono autorizzate dal Consiglio di Amministrazione, in conformità alla procedura di volta in volta vigente per la disciplina della redazione e approvazione delle procedure della Società (c.d. "procedura delle procedure"). Ciascuna di tali procedure è soggetta a revisione e verifica da parte dell'Organismo di Vigilanza, su iniziativa di quest'ultimo in sede di esecuzione delle sue attività di vigilanza o su richiesta di qualsiasi delle funzioni coinvolte.

Le versioni vigenti delle Procedure sono disponibili presso le competenti funzioni aziendali, e una versione elettronica è disponibile sull'intranet aziendale e accessibile per la consultazione da parte di tutti i dipendenti, in particolare di quelli coinvolti in tali Procedure.

Gli elenchi delle Procedure adottate dalla Società per ciascuna categoria di fattispecie di reato-presupposto prese in considerazione in ciascun Capitolo della presente Parte Speciale sono riportati nei rispettivi allegati. Tali elenchi sono periodicamente aggiornati a cura della funzione legale, con la supervisione dell'Organismo di Vigilanza, in sede di adozione di nuove Procedure o modifica/integrazione di quelle esistenti.

La funzione HR, con il supporto o la supervisione dell'Organismo di Vigilanza, provvede ad assicurare adeguata conoscenza delle Procedure da parte dei Responsabili, come di seguito definiti, coinvolti nelle relative Operazioni.

Ciascuno dei Responsabili porta le Procedure relative alle Operazioni in cui è coinvolto a conoscenza del personale impiegato nelle funzioni aziendali cui è preposto, e ne esige il rispetto.

IV.1 Elementi essenziali di ciascuna Procedura

Le Procedure recepiscono i protocolli di controllo (generali e specifici) illustrati nel Modello, presentano l'elenco delle categorie omogenee di Operazioni interessate dalla singola procedura e indicano le funzioni aziendali coinvolte in dette Operazioni.

Le Procedure sono elaborate nel rispetto degli ulteriori criteri qui di seguito esposti.

a) <u>Responsabili</u>

Le Procedure individuano uno o più responsabili in persona dei preposti a ciascuna funzione aziendale coinvolta nell'Operazione (ciascuno un "**Responsabile**").

Per ciascuna categoria omogenea di Operazioni, il Responsabile costituisce il soggetto responsabile della conformità dell'Operazione al presente Modello, nei limiti delle attività di competenza della funzione aziendale cui è preposto. Le Procedure prevedono che ciascun Responsabile assuma formalmente tale responsabilità.

La sigla del Responsabile è imposta su ogni atto da sottoscriversi con efficacia verso terzi ovvero su ogni atto destinato a costituire il presupposto di un atto da sottoscriversi con efficacia verso terzi, in aggiunta alla firma del soggetto dotato di poteri operativi in relazione al compimento della relativa Operazione. Tale sigla attesta la correttezza procedurale dell'Operazione ai fini del presente Modello.

Nel caso in cui il Responsabile sia il soggetto dotato di poteri operativi in relazione al compimento di una Operazione, su ogni atto relativo a tale Operazione è comunque richiesta la firma del General Manager o altro soggetto munito dei necessari poteri di firma.

Nel caso in cui, con riferimento a una Operazione in cui è coinvolto, il Responsabile si trovi, o ritenga di trovarsi, in una situazione di conflitto di interessi con un altro dei soggetti coinvolti in tale Operazione (ivi inclusi altri Responsabili, Dipendenti, Clienti, Collaboratori, Consulenti, Partners), tale situazione deve essere immediatamente comunicata dal Responsabile all'Organismo di Vigilanza e al legal department e all'HR e determina, per il Responsabile in questione, l'obbligo di astenersi dal compiere atti connessi o relativi a tale Operazione; l'Organismo di Vigilanza e i manager delle funzioni HR e legal provvedono quindi a sollecitare la nomina di altro soggetto quale responsabile in sua sostituzione. Tale nomina è comunicata anche all'Organismo di Vigilanza e ai manager delle funzioni HR e legal. A titolo esemplificativo, costituisce situazione di conflitto di interessi in una data Operazione il fatto che il Responsabile sia legato a uno o più soggetti coinvolti nell'Operazione a causa di cariche sociali, rapporti di coniugio, parentela o affinità entro il quarto grado[3], lavoro, consulenza o

[3] Al fine di individuare la nozione di "parenti e affini entro il 4° grado" deve farsi riferimento alle disposizioni dell'art. 74 e ss. c.c.. Ai sensi di tali disposizioni, la parentela è il vincolo tra le persone che discendono da uno stesso stipite (ad es. due fratelli sono parenti in quanto discendono da uno stesso stipite, rappresentato dal genitore). I parenti possono essere in linea retta o collaterale: sono parenti in linea retta le persone di cui l'una discende dall'altra (ad es.

prestazione d'opera retribuita, ovvero di altri rapporti di natura patrimoniale che ne compromettano l'indipendenza.

b) Archiviazione

Di ogni Operazione è fatto obbligo di dare evidenza mediante documentazione di qualsiasi atto del procedimento interno relativo all'Operazione per iscritto o su supporto informatico o mediante registrazione nel sistema informatico della Società, in conformità alle procedure di autenticazione di volta in volta vigenti presso la Società.

In particolare, per ogni categoria omogenea di Operazioni deve essere tenuto da ciascun Responsabile un apposito sistema di archiviazione basato su uno o più archivi fisici o logici, da tenere costantemente aggiornati e da cui risulti, per ciascuna Operazione:

a) la descrizione dell'Operazione, con l'evidenziazione, sia pure a titolo indicativo, del suo valore economico;

b) se del caso, la Pubblica Amministrazione (incluso l'eventuale organo giudiziario) o l'ente pubblico coinvolti nell'Operazione, con indicazione della persona fisica che ne costituisce il referente ai fini dell'Operazione (in genere, il c.d. responsabile del procedimento);

c) copia di tutti i documenti e indicazione delle principali iniziative e dei principali atti o altri adempimenti svolti nell'espletamento dell'Operazione;

d) l'indicazione di eventuali consulenti incaricati di assistere la Società nell'Operazione;

e) l'indicazione di eventuali Partners ai fini della partecipazione congiunta all'Operazione;

f) l'indicazione di eventuali collaboratori esterni;

g) altri elementi e circostanze rilevanti, attinenti all'Operazione (quali movimenti di denaro effettuati nell'ambito della procedura stessa); in particolare, in caso di pagamenti effettuati dalla o alla Società, indicazione della causale e dei riferimenti ai documenti giustificativi.

Il Responsabile deve tenere ciascuno di tali archivi a disposizione dell'Organismo di Vigilanza. Gli archivi sono costituiti in formato cartaceo o elettronico.

Le Procedure indicano, in relazione a ciascuna Operazione, l'elenco degli archivi relativi a tale Operazione, i soggetti a cui compete la loro tenuta e i luoghi in cui tali archivi sono custoditi.

Per ogni Consulente o Partner, il Responsabile tiene a disposizione dell'Organismo di Vigilanza una scheda di evidenza da cui risulti (i) per ogni consulente, l'indicazione delle motivazioni che hanno portato alla scelta di tale soggetto, degli elementi di verifica assunti, del tipo di incarico conferito, del corrispettivo riconosciuto, di eventuali condizioni particolari applicate, e (ii) per ogni Partner, l'indicazione delle motivazioni che hanno portato alla scelta di tale Partner, della composizione del suo assetto azionario, del tipo di accordo associativo realizzato, delle condizioni economiche pattuite, di eventuali condizioni particolari applicate, con riferimento anche all'ipotesi di previsione di una maggior contribuzione da parte della Società a vantaggio dei Partners stessi.

---

nonno, padre e figlio), mentre sono parenti in linea collaterale quelle persone che, pur avendo uno stipite comune, non discendono l'un dall'altra (ad es. due fratelli tra loro oppure lo zio ed il nipote). Nella linea retta si computano tanti gradi quante sono le generazioni, escluso lo stipite (ad es. padre e figlio sono tra loro parenti di primo grado, nonno e nipote lo sono di secondo grado); nella linea collaterale i gradi si computano dalle generazioni, salendo da uno dei parenti fino allo stipite comune e da questo discendendo all'altro parente, sempre restando escluso lo stipite (ad es. due fratelli sono tra loro parenti di secondo grado). Quindi, i parenti entro il quarto grado sono a) in linea retta: genitori e figli nonché nonni, bisnonni, trisnonni e nipoti e b) in linea collaterale: fratelli tra loro, fratelli e figli di una stessa persona, figli e figli dei figli dei figli di una stessa persona, figli di due fratelli). Ai sensi delle stesse disposizioni, l'affinità è il vincolo tra un coniuge e i parenti dell'altro coniuge. Nella linea e nel grado in cui taluno è parente d'uno dei coniugi, egli è affine dell'altro coniuge (ad es. una persona è parente in linea retta entro il quarto grado dei propri cugini più prossimi, per tali intendendosi i figli dei fratelli dei suoi genitori, ed è affine in pari linea e grado dei coniugi di tali cugini).

c) Consulenti, Partners e collaboratori esterni

In relazione a ciascun Consulente, Partner o collaboratore esterno coinvolto in qualsiasi Operazione, l'Organismo di Vigilanza provvede a verificare l'inserimento nei relativi contratti di clausole volte a sanzionare la violazione da parte di tali soggetti delle disposizioni e delle regole di comportamento previste dal Modello a essi applicabili, ovvero l'eventuale commissione dei reati rilevanti ai fini della responsabilità amministrativa degli enti da parte degli stessi.

Tali clausole, facendo esplicito riferimento al rispetto delle disposizioni e delle regole di comportamento previste dal Modello, potranno prevedere, ad esempio, l'obbligo, da parte di questi soggetti terzi, di non adottare atti o intrattenere comportamenti tali da determinare una violazione del Modello da parte della Società. In caso di violazione di tale obbligo, dovrà essere prevista la risoluzione del contratto con eventuale applicazione di penali. Analoghe misure potranno essere previste con riferimento ai contratti di servizi infragruppo.

IV.2 Operazioni a rischio specifico: obblighi di segnalazione

Nell'ambito di una o più aree a rischio e con riferimento a una o più operazioni o categorie di operazioni a rischio, le Procedure possono individuare una o più categorie di operazioni a rischio specifico (ciascuna, di seguito, un'"**Operazione RS**"), in relazione alle quali, per loro natura, importo o altre caratteristiche soggettive od oggettive, il rischio di commissione di reati rilevanti ai fini del d.lgs. 231/2001 e di conseguente responsabilità amministrativa a carico della Società possa essere ritenuto particolarmente significativo.

A tal fine le Procedure prevedono che, per ogni singola Operazione RS, almeno uno dei Responsabili coinvolti nell'Operazione RS, o un soggetto a esso direttamente subordinato, trasmetta tempestivamente all'Organismo di Vigilanza apposita segnalazione iniziale di avvio di tale Operazione RS nonché, qualora nella segnalazione iniziale non sia già indicata la data prestabilita di conclusione, apposita segnalazione finale di conclusione di tale operazione. Da tali segnalazioni devono risultare almeno le seguenti informazioni:

a) la descrizione dell'Operazione RS, con l'evidenziazione, sia pure a titolo indicativo, del suo valore economico;

b) se del caso, la Pubblica Amministrazione (incluso l'eventuale organo giudiziario) o l'ente pubblico che è coinvolto o ha competenza nella procedura che forma oggetto dell'Operazione RS;

c) l'indicazione di eventuali consulenti incaricati di assistere la Società nell'Operazione RS;

d) l'indicazione di eventuali Partners ai fini della partecipazione congiunta all'Operazione RS;

e) altri elementi e circostanze rilevanti, attinenti all'Operazione RS (quali: movimenti di denaro effettuati nell'ambito della procedura stessa).

Ciascuna segnalazione può essere effettuata in forma di documento iscritto o informatico, secondo le modalità indicate nelle Procedure.

V Istruzioni e verifiche dell'Organismo di Vigilanza

L'Organismo di Vigilanza ha il compito di:

a) curare l'emanazione e l'aggiornamento di istruzioni standardizzate relative ai protocolli di cui alla Parte Speciale del presente Modello.

Tali istruzioni devono essere scritte e conservate su supporto cartaceo o informatico in luogo accessibile a tutti i soggetti a ciò legittimamente interessati con le stesse modalità con cui sono pubblicate le Procedure in conformità alla precedente sezione IV;

b) verificare periodicamente - con il supporto delle altre funzioni competenti - il sistema di deleghe in vigore, raccomandando delle modifiche nel caso in cui il potere di gestione e/o la qualifica non corrisponda ai poteri di rappresentanza conferiti ai soggetti indicati come responsabili di operazioni o procedimenti nella presente Parte Speciale;

c) verificare periodicamente, con il supporto delle altre funzioni competenti, l'effettiva adozione di clausole standard finalizzate:

   (i) all'osservanza da parte dei Destinatari delle disposizioni del d.lgs. 231/2001;

   (ii) alla possibilità della Società di effettuare efficaci azioni di controllo nei confronti dei Destinatari al fine di verificare il rispetto delle prescrizioni in esso contenute;

   (iii) all'attuazione di meccanismi sanzionatori (quali il recesso contrattuale nei riguardi di Partners o di Consulenti) qualora si accertino violazioni delle relative prescrizioni;

d) indicare alle competenti funzioni aziendali le opportune integrazioni ai sistemi gestionali delle risorse finanziarie (sia in entrata che in uscita), già presenti nella Società, con l'introduzione degli opportuni accorgimenti suscettibili di rilevare l'esistenza di eventuali flussi finanziari atipici e connotati da maggiori margini di discrezionalità rispetto a quanto ordinariamente previsto.

CAPITOLO 1
I REATI NEI CONFRONTI DELLA PUBBLICA AMMINISTRAZIONE

1 Le nozioni di Pubblica Amministrazione, pubblico ufficiale, incaricato di pubblico servizio

Qualsiasi riferimento alla Pubblica Amministrazione include, oltre lo Stato e le sue amministrazioni, anche enti pubblici economici o non, organismi di diritto pubblico (imprese a partecipazione pubblica o controllate dallo Stato o comunque esercenti attività di interesse pubblico o di pubblica utilità) o altri soggetti privati i cui rappresentanti, esponenti aziendali o dipendenti possano essere qualificati pubblici ufficiali o incaricati di pubblico servizio ai sensi della normativa vigente.

Ai fini del presente capitolo di Parte Speciale, è fondamentale esaminare in dettaglio le nozioni di Pubblica Amministrazione (di seguito anche "P.A."), di pubblico ufficiale (di seguito anche "PU") e di incaricato di pubblico servizio (di seguito anche "IPS").

Per P.A. si intende, in estrema sintesi, l'insieme di enti e soggetti pubblici (Stato, Ministeri, Regioni, Province, Comuni, ecc.) e talora privati (ad esempio concessionari, amministrazioni aggiudicatrici, S.p.A. miste, ecc.) e tutte le altre figure che svolgono in qualche modo la funzione pubblica, nell'interesse della collettività e quindi nell'interesse pubblico. Oggetto della tutela penale nei reati che rilevano in questa sede è il regolare funzionamento nonché il prestigio degli Enti Pubblici e, in generale, quel "buon andamento" dell'Amministrazione di cui all'art. 97 della Costituzione, ovvero, nel caso dei reati di truffa, il patrimonio pubblico.

La nozione di PU è fornita direttamente dal legislatore, all'art. 357 c.p., il quale indica il "*pubblico ufficiale*" in "*chiunque eserciti una pubblica funzione legislativa, giudiziaria o amministrativa*", specificandosi 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 e dal suo svolgersi per mezzo dei poteri autoritativi e certificativi*".

I "*pubblici poteri*" qui in rilievo sono: il potere legislativo, quello giudiziario e, da ultimo, quelli riconducibili alla pubblica funzione amministrativa.

Il potere legislativo trova la sua esplicazione nell'attività normativa vera e propria ovvero in tutte quelle accessorie e/o preparatorie di quest'ultima. E' un PU, in quanto svolge la "*pubblica funzione legislativa*", dunque, chiunque, al livello nazionale e comunitario, partecipi all'esplicazione di tale potere. I soggetti pubblici cui, normalmente, può ricondursi l'esercizio di tale tipo di funzione sono: il Parlamento, il Governo (limitatamente alle attività legislative di sua competenza, ad esempio decreti legge e decreti delegati), le Regioni e le Province (queste ultime per quanto attinenti alla loro attività normativa); le Istituzioni dell'Unione Europea aventi competenze legislative rilevanti nell'ambito dell'ordinamento nazionale.

Il potere giudiziario trova la sua esplicazione nell'attività dello *iusdicere*, inteso in senso lato. Si ritiene, dunque, che sia un PU, in quanto svolge la "*pubblica funzione giudiziaria*", non solo chiunque, al livello nazionale e comunitario, compia attività diretta esplicazione di tale potere, ma altresì tutta l'attività afferente l'amministrazione della giustizia, collegata e accessoria alla prima. Svolgono tale tipo di funzione, pertanto, tutti coloro che, al livello nazionale e comunitario, partecipano sia alla vera e propria attività dello *iusdicere*, sia a quella amministrativa collegata allo stesso, ovverosia i magistrati (ivi compresi i pubblici ministeri), i cancellieri, i segretari, i membri della Corte di Giustizia e della Corte dei Conti Comunitarie, i

funzionari e gli addetti a svolgere l'attività amministrativa collegata allo *iusdicere* della Corte di Giustizia e della Corte dei Conti Comunitarie, ecc..

I poteri riconducibili alla pubblica funzione amministrativa, da ultimo, sono il potere deliberativo, il potere autoritativo e il potere certificativo della Pubblica Amministrazione. Questi poteri, in nessun modo connessi a particolari qualifiche soggettive e/o mansioni dei soggetti agenti, possono essere qualificati nei termini che seguono:

- il potere deliberativo della P.A. è quello relativo alla "*formazione e manifestazione della volontà della Pubblica Amministrazione*". Questa formula è letta, in senso assai lato e, pertanto, comprensiva di qualsiasi attività che concorra in qualunque modo a estrinsecare il potere deliberativo della Pubblica Amministrazione; in tale prospettiva, sono stati qualificati come pubblici ufficiali, non solo le persone istituzionalmente preposte a esplicare tale potere ovvero i soggetti che svolgono le attività istruttorie o preparative all'iter deliberativo della Pubblica Amministrazione, ma anche i loro collaboratori, saltuari e occasionali;
- il potere autoritativo della P.A., diversamente, si concretizza in tutte quelle attività che permettono alla Pubblica Amministrazione di realizzare i suoi fini mediante veri e propri comandi. Questo ruolo di supremazia della P.A. è, ad esempio, facilmente individuabile nel potere della stessa di rilasciare "concessioni" ai privati. Alla luce di queste considerazioni, possono essere qualificati come pubblici ufficiali tutti i soggetti preposti a esplicare tale potere;
- il potere certificativo è normalmente riconosciuto in quello di rappresentare come certa una determinata situazione sottoposta alla cognizione di un "*pubblico agente*". Anche questa attività di certificazione pubblica è stata interpretata in senso assai lato, tanto da riconoscere nella stessa, non solo il potere certificativo fidefacente, ma una vera e propria dichiarazione di volontà della Pubblica Amministrazione.

Diversamente, l'art. 358 riconosce la qualifica di "*incaricato di un pubblico servizio*" a tutti "*coloro i quali, a qualunque titolo, prestano un pubblico servizio*", intendendosi per tale "*un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*".

E', pertanto, un IPS colui il quale svolge una "*pubblica attività*", non riconducibile ad alcuno dei poteri sopra rammentati e non concernente semplici mansioni d'ordine e/o la prestazione di opera meramente materiale e, in quanto tali, prive di alcun apporto intellettuale e discrezionale. Esempi di IPS sono i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati. L'effettiva ricorrenza dei su indicati requisiti deve essere verificata, caso per caso, in ragione della concreta ed effettiva possibilità di ricondurre l'attività di interesse alle richiamate definizioni, essendo certamente ipotizzabile anche che soggetti appartenenti alla medesima categoria, ma addetti a espletare differenti funzioni o servizi, possano essere diversamente qualificati proprio in ragione della non coincidenza dell'attività da loro in concreto svolta.

1.1 I reati nei confronti della Pubblica Amministrazione richiamati dagli articoli 24 e 25 del d.lgs. 231/2001

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

Questo delitto consiste nell'effettuare un mutamento di destinazione di contributi, sovvenzioni o finanziamenti ottenuti dallo Stato, da altri enti pubblici o dalle Comunità europee, e che

dovevano invece essere impiegati nella realizzazione di opere o nello svolgimento di attività di pubblico interesse.

Il delitto si consuma anche se solo una parte dei fondi è distratta e anche nel caso in cui la parte correttamente impiegata abbia esaurito l'opera o l'iniziativa cui l'intera somma era destinata.

La condotta criminosa prescinde dal modo in cui sono stati ottenuti i fondi e si realizza solo in un momento successivo all'ottenimento dei fondi stessi.

Il reato in esame può configurarsi sia quando le sovvenzioni sono erogate a favore della società, sia quando la società si fa tramite, nell'ambito di un rapporto trilaterale, della loro distribuzione ai privati destinatari dell'erogazione.

Nello specifico il reato in oggetto potrebbe, a titolo esemplificativo, essere realizzato destinando, in tutto o in parte, le somme concesse dallo Stato, da altri enti pubblici o dalle Comunità europee per l'assunzione e formazione del personale o per la ristrutturazione degli immobili o per le attività di adeguamento alla normativa in materia di tutela della salute e sicurezza sul lavoro ad altri scopi quali finanziamenti di progetti, acquisti di beni e servizi, ecc.

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

La fattispecie di delitto si realizza qualora l'ente - tramite chiunque (anche esterno all'ente stesso) - consegua per sé o per altri erogazioni dallo Stato, da altri enti pubblici o dalle Comunità europee, mediante una condotta consistente in qualsiasi tipo di utilizzo (ad es. presentazione) di dichiarazioni (scritte o orali), o di altra documentazione materialmente e/o ideologicamente falsa ovvero attraverso l'omissione di informazioni dovute.

La fattispecie si consuma con l'avvenuto ottenimento delle erogazioni (che costituisce l'evento tipico del reato).

Questa fattispecie costituisce una "ipotesi speciale" rispetto alla più ampia fattispecie di truffa aggravata per il conseguimento di erogazioni pubbliche di cui all'art. 640-*bis* c.p. Si applicherà la norma qui in esame (e cioè l'art. 316-*ter* c.p.) tutte le volte che ne ricorrano i requisiti specifici da essa contemplati; ricadendosi invece nell'ipotesi della fattispecie più generale (e più grave) solo qualora gli strumenti ingannevoli usati per ottenere le erogazioni pubbliche siano diversi da quelli considerati nell'art. 316-*ter* ma comunque riconducibili alla nozione di "artifici o raggiri" richiamata dall'art. 640-*bis*.

Il reato qui in esame (art. 316-*ter* c.p.) si configura come ipotesi speciale anche nei confronti dell'art. 640, comma 2, n. 1, c.p. (truffa aggravata in danno dello Stato), rispetto al quale l'elemento "specializzante" è dato non più dal tipo di artificio o raggiro impiegato, bensì dal tipo di profitto conseguito ai danni dell'ente pubblico ingannato. Profitto che nella fattispecie più generale, testé richiamata, non consiste nell'ottenimento di una erogazione, ma in un generico vantaggio di qualsiasi altra natura.

La società può essere chiamata a rispondere quando i suoi esponenti pongono in essere la condotta illecita prevista, assicurando alla società un finanziamento al quale non avrebbe diritto.

Nello specifico il reato in oggetto potrebbe, a titolo esemplificativo, essere realizzato rilasciando, allo scopo di ottenere un finanziamento pubblico (statale o comunitario), all'ente erogante informazioni/dichiarazioni non corrispondenti alla realtà o attestanti cose non vere ovvero omettendo informazioni dovute. Si pensi, in particolare, al caso in cui l'ente erogante richieda fra i requisiti di ammissibilità della richiesta del finanziamento che la società sia iscritta in albi specifici e la stessa società pur di ottenere il finanziamento produca una documentazione falsa che attesta l'iscrizione all'albo richiesto dall'ente.

1.1.3 Truffa in danno dello Stato o di altro ente pubblico (articolo 640, comma 2, n. 1 c.p.)

Si tratta della normale ipotesi di truffa (articolo 640 c.p.), aggravata dal fatto che il danno economico derivante dall'attività ingannatoria del reo ricade sullo Stato o su altro ente pubblico.

La condotta consiste, sostanzialmente, in qualsiasi tipo di menzogna (compreso l'indebito silenzio su circostanze che devono essere rese note) tramite la quale si ottiene che taluno cada in errore su qualcosa e compia, di conseguenza, un atto di disposizione che non avrebbe compiuto se avesse conosciuto la verità. Per la consumazione del reato occorre che sussista, oltre a tale condotta, il conseguente profitto di qualcuno (chiunque esso sia, anche diverso dall'ingannatore) e il danno dello Stato o dell'ente pubblico.

La responsabilità della società potrà sussistere, in via esemplificativa, quando un suo dipendente compia una truffa ai danni di un ente previdenziale o un'amministrazione locale attraverso dichiarazioni mendaci o fraudolente, purché agisca nell'interesse o a vantaggio della società.

Nello specifico il reato in oggetto potrebbe, a titolo esemplificativo, essere realizzato:

- alterando la documentazione trasmessa agli uffici della P.A. competenti al fine di indurre in errore circa l'esistenza di condizioni essenziali per ottenere licenze, autorizzazioni, concessioni, abilitazioni, ecc.;
- assumendo, nella fase preliminare e contestuale alla conclusione di accordi commerciali con la P.A., un comportamento fraudolento ovvero ponendo in essere artifizi e/o raggiri che inducano in errore la P.A. circa la situazione economica patrimoniale della società, il possesso dei requisiti tecnico-organizzativi richiesti, i requisiti quantitativi e qualitativi richiesti. Si pensi, in particolare, al caso in cui la P.A. sia intenzionata a contrattare esclusivamente con società che hanno un certo numero di dipendenti o che hanno sedi in luoghi specifici, e la società, interessata alla conclusione positiva del contratto, fornisca nelle dichiarazioni/informazioni da trasmettere all'ente dati diversi da quelli reali anche supportati da documentazione alterata (es. statistiche ufficiali);
- omettendo il versamento o alterando la documentazione relativa ai versamenti dei contributi INPS, INAIL dei dipendenti;
- alterando la documentazione da fornire alla P.A. all'atto dell'assunzione di personale appartenente alle categorie protette o agevolate al fine di ottenere sgravi contributivi indebiti e crediti d'imposta ovvero rendendo informazioni non veritiere in occasione della redazione del prospetto informativo annuale relativo alle assunzioni obbligatorie.

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

La fattispecie si realizza se il fatto previsto dall'art. 640 c.p. (ossia la truffa) riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.

Nello specifico il reato in oggetto potrebbe, a titolo esemplificativo, essere realizzato inducendo in errore, attraverso artifizi, raggiri o dichiarazioni mendaci, l'ente erogante allo scopo di ottenere erogazioni pubbliche (statali o comunitarie). Si pensi, in particolare, al caso in cui la società induca in errore l'ente erogante circa il possesso di specifici requisiti richiesti per ottenere il finanziamento producendo (o contribuendo a produrre, nel caso di concorso) documentazione falsa attestante il possesso dei predetti requisiti richiesti dall'ente erogante.

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

Questa fattispecie delittuosa si realizza quando un soggetto, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

Il reato presenta elementi costitutivi pressoché identici a quelli della truffa, salvo il fatto che l'attività fraudolenta non investe una persona, ma un sistema informatico attraverso la sua manipolazione.

Nello specifico il reato in oggetto potrebbe, a titolo esemplificativo, essere realizzato alterando i registri informatici della P.A. per far risultare esistenti condizioni essenziali per la partecipazione a gare (iscrizione in albi, ecc.) ovvero per la successiva produzione di documenti attestanti fatti e circostanze inesistenti o, ancora, per modificare dati fiscali/previdenziali di interesse della società (es. Mod. 770), già trasmessi all'amministrazione finanziaria.

1.1.6 Corruzione per un atto d'ufficio o contrario ai doveri di ufficio (articoli 318, 319 e 319-bis c.p.)

La fattispecie prevista dall'articolo 318 c.p. (corruzione per un atto d'ufficio) si realizza quando il pubblico ufficiale per compiere 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. La nozione di pubblico ufficiale è quella definita dall'art. 357 c.p.. Qui, come è chiaro, si tratta di atti che non contrastano con i doveri d'ufficio. Il reato può essere integrato anche quando il pubblico ufficiale riceve la retribuzione per un atto d'ufficio da lui già compiuto.

La fattispecie prevista dall'articolo 319 c.p. si realizza, invece, quando il pubblico ufficiale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro o altra utilità, o ne accetta la promessa.

Si ha circostanza aggravante se il fatto di cui all'articolo 319 c.p. ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene (articolo 319-*bis* c.p.).

L'attività delittuosa del funzionario pubblico può, dunque, estrinsecarsi sia in un atto conforme ai doveri d'ufficio (ad esempio velocizzare una pratica la cui evasione è di propria competenza), sia, e soprattutto, in un atto contrario ai suoi doveri (ad esempio il pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).

1.1.7 Corruzione in atti giudiziari (articolo 319-ter c.p.)

Tale fattispecie si realizza se i fatti indicati negli articoli 318 e 319 c.p. siano commessi dal pubblico ufficiale per favorire o danneggiare una parte in un processo civile, penale o amministrativo. La norma si applica, senza distinzione, a tutti i pubblici ufficiali e non soltanto ai magistrati.

In via esemplificativa potrà rispondere del reato in esame la società che, coinvolta in un processo il cui esito negativo potrebbe causarle un grave danno patrimoniale, decida di corrompere il giudice per ottenere un risultato favorevole.

1.1.8 Corruzione di persona incaricata di pubblico servizio (articolo 320 c.p.)

Le disposizioni dell'articolo 319 c.p. si applicano anche se il fatto è commesso da persona incaricata di un pubblico servizio; quelle di cui all'articolo 318 c.p. si applicano anche alla

persona incaricata di un pubblico servizio, quale definito dall'articolo 358 c.p., ma solo qualora rivesta la qualità di pubblico impiegato.

1.1.9 Pene per il corruttore (articolo 321 c.p.)

Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-*bis*, nell'articolo 319-*ter* e nell'articolo 320 c.p. in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche, per disposizione della norma qui in esame, a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro o altra utilità.

In altri termini, colui che corrompe commette una autonoma fattispecie di reato rispetto a quella compiuta dal pubblico ufficiale (o dall'incaricato di pubblico servizio) che si è lasciato corrompere nei modi e ponendo in essere le condotte contemplate negli articoli sopra richiamati.

1.1.10 Istigazione alla corruzione (articolo 322 c.p.)

Questa fattispecie delittuosa si configura allorché il privato tiene il comportamento incriminato dal sopra illustrato articolo 321 c.p. (e cioè svolge attività corruttiva), ma il pubblico ufficiale (o l'incaricato di pubblico servizio) rifiuta l'offerta illecitamente avanzatagli.

1.1.11 Concussione (articolo 317 c.p.)

Tale fattispecie si realizza quando "*il pubblico ufficiale o l'incaricato di un pubblico servizio* [...] *abusando della sua qualità o dei suoi poteri, costringe o induce taluno a dare o a promettere indebitamente, a lui o ad un terzo, denaro od altra utilità*".

La differenza tra la concussione e corruzione risiede nell'esistenza di una situazione idonea a determinare uno stato di soggezione del privato nei confronti del pubblico ufficiale.

1.1.12 Concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (articolo 322-bis c.p.)

Le disposizioni degli articoli da 317 a 320 e 322, terzo e quarto comma, c.p., si applicano anche a membri delle Istituzioni comunitarie europee, nonché ai funzionari delle stesse e dell'intera struttura amministrativa comunitaria, e alle persone comandate presso la Comunità con particolari funzioni o addette a enti previsti dai trattati. Le stesse disposizioni si applicano anche alle persone che nell'ambito degli Stati membri dell'Unione Europea svolgono attività corrispondenti a quelle che nel nostro ordinamento sono svolte da pubblici ufficiali o da incaricati di un pubblico servizio.

Ciò premesso, va detto che l'articolo 322-*bis* c.p. incrimina altresì – e questo è d'interesse per i privati che abbiano a che fare con i soggetti sopra elencati – tutti coloro che compiano le attività colpite dagli articoli 321 e 322 c.p. (cioè attività corruttive) nei confronti delle persone medesime, e non solo i soggetti passivi della corruzione. Inoltre, l'art. 322-*bis* c.p. incrimina anche l'offerta o promessa di denaro o altra utilità "*a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri* [diversi da quelli dell'Unione Europea, n.d.r.] *o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o altri un indebito vantaggio in operazioni economiche internazionali*" (art. 322-*bis*).

Nello specifico i reati di corruzione sopra richiamati potrebbero, a titolo esemplificativo, essere realizzati offrendo/promettendo denaro o altra utilità:

- al pubblico ufficiale o incaricato di pubblico servizio al fine di concludere accordi commerciali – mediante procedure negoziate o a evidenza pubblica – con la P.A. di appartenenza;
- al pubblico ufficiale o incaricato di pubblico servizio al fine di: ottenere l'accelerazione di pratiche di rilascio di autorizzazioni; non far rilevare elementi che impedirebbero il rilascio di autorizzazioni; garantire il sicuro rilascio di autorizzazioni;
- al pubblico ufficiale o incaricato di pubblico servizio al fine di non ricevere provvedimenti di natura sanzionatoria a seguito di accertate violazioni di adempimenti obbligatori (es. violazione delle norme sulla tutela della salute e sicurezza sul lavoro);
- a esponenti delle pubbliche autorità al fine di: omettere nel verbale di ispezione rilievi, anomalie emerse nel corso dell'ispezione; far ritardare o non effettuare l'ispezione stessa; far ignorare ritardi, o il mancato invio delle comunicazioni o risposte a richieste specifiche da parte delle autorità;
- al pubblico ufficiale o incaricato di pubblico servizio al fine di: non ricevere sanzioni per il mancato o ritardato inoltro di risposte alle richieste di informazioni inoltrate dall'Agenzia delle Entrate; non ricevere sanzioni per il mancato o ritardato pagamento delle imposte e tasse; evitare indagini di carattere fiscale; non far rilevare anomalie accertate in corso d'ispezione/indagine.

L'utilità promessa od offerta al pubblico ufficiale o incaricato di pubblico servizio al fine di ottenere un indebito vantaggio, potrebbe consistere a titolo esemplificativo:

- nell'assunzione di persone legate al pubblico ufficiale o incaricato di pubblico servizio da vincoli di parentela o simili;
- in regali o omaggi che non siano di modico valore e non direttamente ascrivibili a normali relazioni di cortesia;
- nella concessione di prodotti e servizi a condizioni economiche particolarmente vantaggiose;
- nella conclusione di contratti per la fornitura di beni e servizi con controparti segnalate dal pubblico ufficiale o incaricato di pubblico servizio;
- nella conclusione di contratti di sponsorizzazione con controparti segnalate dal pubblico ufficiale o incaricato di pubblico servizio.

1.2 Le sanzioni previste a carico dell'ente in relazione ai delitti contro la Pubblica Amministrazione

Gli artt. 24 e 25 del Decreto, in relazione alla commissione dei reati contro la Pubblica Amministrazione, recano le seguenti sanzioni:

(i) per i delitti di cui all'art. 316-*bis* ("*Malversazione a danno dello Stato*"), all'art. 316-*ter* ("*Indebita percezione di erogazioni a danno dello Stato*"), all'art. 640, comma 2, n. 1 ("*Truffa in danno dello Stato o di altro ente pubblico*"), all'art. 640-*bis* ("*Truffa aggravata per il conseguimento di erogazioni pubbliche*") ed all'art. 640-*ter* ("*Frode informatica in danno dello Stato o di altro ente pubblico*") se commesso in danno dello Stato o di altro ente pubblico, si applicano:

- la sanzione pecuniaria in misura pari a 500 quote (dove ciascuna quota corrisponde ad un importo variabile fra un minimo di € 258,22 ad un massimo di € 1.549,37) e, se l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità, la sanzione pecuniaria da 200 a 600 quote, nonché

- in caso di condanna, le sanzioni interdittive di cui all'art. 9, comma 2, lett. c) del Decreto (i.e. divieto di contrattare con la pubblica amministrazione salvo che per ottenere le prestazioni di un pubblico servizio), all'art. 9, comma 2, lett. d) del Decreto (i.e. esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi), e all'art. 9, comma 2, lett. e) del Decreto (i.e. divieto di pubblicizzare beni o servizi).

(ii) Per i delitti di cui all'art. 318 ("*Corruzione per un atto d'ufficio*"), all'art. 321 ("*Pene per il corruttore*") ed all'art. 322 ("*Istigazione alla corruzione*"), commi 1 e 3, c.p., si applicano:

- la sanzione pecuniaria fino a 200 quote, anche quando tali delitti sono stati commessi dalle persone indicate negli artt. 320 e 322-bis;
- in caso di condanna, le sanzioni interdittive in misura non inferiore ad 1 anno.

(iii) Per i delitti di cui all'art. 319 ("*Corruzione per un atto contrario ai doveri d'ufficio*"), all'art. 319-*ter* ("*Corruzione in atti giudiziari*"), comma 1, all'art. 321 ("*Pene per il corruttore*"), all'art. 322 ("*Istigazione alla corruzione*"), commi 2 e 4, c.p., si applica

- la sanzione pecuniaria da 200 a 600 quote.

(iv) Per i delitti di cui all'art. 317 ("*Concussione*"), 319 ("*Corruzione per un atto contrario ai doveri d'ufficio*"), aggravato ai sensi dell'art. 319-*bis* quando dal fatto l'ente ha conseguito un profitto di rilevante entità, all'art. 319-*ter* ("*Corruzione in atti giudiziari*"), comma 2, ed all'art. 321 ("*Pene per il corruttore*") c.p., si applicano:

- **la** sanzione pecuniaria da 300 a 800 quote, anche quando tali delitti sono stati commessi dalle persone indicate negli articoli 320 e 322-bis, c.p.;
- le sanzioni interdittive in misura non inferiore ad 1 anno.

1.3 Le attività individuate come sensibili o strumentali ai fini del d.lgs. 231/2001 con riferimento ai reati nei confronti della Pubblica Amministrazione

L'analisi dei processi aziendali della Società ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dagli articoli 24 e 25 del d.lgs. 231/2001.

È opportuno distinguere tra attività sensibili e attività strumentali a quelle sensibili.

Le attività sensibili sono quelle il cui compimento è correlato al rischio di commissione di un reato rilevante in considerazione della sussistenza di rapporti o contatti diretti tra la Società e la Pubblica Amministrazione.

Le attività strumentali sono quelle il cui compimento è di supporto alle attività sensibili, in via propedeutica o esecutiva.

Qui di seguito sono elencate le cosiddette attività sensibili e strumentali identificate con riferimento ai reati nei confronti della Pubblica Amministrazione.

1.3.1 Attività sensibili

1. Acquisizione (redazione e/o predisposizione delle domande/istanze) e/o gestione/destinazione di contributi/sovvenzioni/finanziamenti pubblici (nazionali e/o

internazionali ricevuti, ad esempio, per attività di formazione, assunzione di personale, ristrutturazione immobili, ecc.).

2. Gestione delle domande e dei rapporti con Pubbliche Amministrazioni, aziende di Stato, enti ed uffici pubblici per l'ottenimento di concessioni, autorizzazioni e licenze e altri provvedimenti amministrativi inerenti all'esercizio delle attività aziendali (es. autorizzazioni per la costruzione e fornitura di reti di telecomunicazione, autorizzazioni per l'istallazione di siti radiomobili).
3. Negoziazione, stipulazione ed esecuzione di contratti e/o convenzioni con la Pubblica Amministrazione anche attraverso la partecipazione a procedure ad evidenza pubblica (aperte, negoziate o ristrette) o affidamenti diretti da parte di enti pubblici (es. contratti di vendita di prodotti e servizi ICT forniti dalla Società, contratti di locazione relativi a terreni/siti per l'istallazione di siti radiomobili).
4. Gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici e collegamenti telematici (in entrata e in uscita) o trasmissione di dati su supporti informatici a soggetti pubblici – in particolare in materia societaria e fiscale.
5. Gestione dei contenziosi e controversie giudiziarie di qualsiasi genere, grado o giurisdizione nei quali sia coinvolta a qualsiasi titolo la Società.
6. Gestione rapporti con autorità e soggetti pubblici nel normale svolgimento di attività aziendali (es. Enti Pubblici Locali, Agenzia delle Entrate, Guardia di Finanza, INPS, INAIL, Ispettorato del Lavoro, autorità competenti in materia di tutela della salute e sicurezza sul lavoro, VVFF, Sportello Unico per l'Immigrazione, Prefetture, Questure, Dipartimento Provinciale del Lavoro, ASL, Camere di Commercio, Agenzia delle dogane, uffici catastali e conservatorie, istituti universitari, ecc.) e nell'ambito di collaborazione in caso di indagini basate su comunicazioni elettroniche. Adempimenti e ispezioni.
7. Gestione dei rapporti con altre Autorità pubbliche di vigilanza o regolamentari (es. Autorità Garante della Concorrenza e del Mercato, AGCOM, Autorità garante per la protezione dei dati personali, Ministeri, autorità governative, ecc.).

1.3.2 Attività strumentali

1. Gestione dei flussi finanziari in entrata ed in uscita.
2. Gestione dell'attività relativa ad azioni di recupero di crediti insoluti.
3. Selezione e gestione dei rapporti con fornitori di beni e servizi (ivi inclusi consulenti in materia tecnico-finanziaria, legale o altro tipo), agenti e distributori.
4. Gestione degli omaggi e delle spese di rappresentanza/gestione delle erogazioni liberali.
5. Selezione, assunzione e promozione di personale dipendente (ivi compreso personale appartenente alle categorie protette o la cui assunzione è agevolata).

1.4 Il sistema dei controlli

Per le attività sensibili e strumentali identificate con riferimento ai reati nei confronti della Pubblica Amministrazione, oltre ai sei protocolli generali indicati alla sezione I della Premessa della presente Parte Speciale, sono stati individuati, anche sulla scorta delle *best practice* internazionali in tema di rischi di frode e corruzione, i protocolli specifici elencati nei successivi paragrafi.

I protocolli generali e quelli specifici di seguito riportati sono stati recepiti dalla Società

nell'ambito delle procedure indicate nell'Allegato n. 2.

1.4.1 Protocolli specifici relativi alle attività sensibili

Relativamente a tutte le attività sensibili, la Società applica i protocolli specifici rappresentati dai seguenti divieti da applicare in relazione ai soggetti che intrattengono rapporti con la Pubblica Amministrazione.

I Divieto di intrattenere rapporti con la Pubblica Amministrazione in autonomia: nessun soggetto può intrattenere rapporti con la Pubblica Amministrazione da solo e liberamente.

II Divieto di accesso a risorse finanziarie in autonomia: il soggetto che intrattiene rapporti con la Pubblica Amministrazione non può da solo e liberamente accedere alle risorse finanziarie e autorizzare disposizioni di pagamento.

III Divieto di conferimento di contratti di consulenza o similari in autonomia: il soggetto che intrattiene rapporti con la Pubblica Amministrazione non può da solo e liberamente conferire incarichi di consulenza/prestazioni professionali né stipulare contratti di mediazione.

IV Divieto di concessione di utilità in autonomia: il soggetto che intrattiene rapporti con la Pubblica Amministrazione non può da solo e liberamente concedere qualsivoglia utilità.

V Divieto di assunzione di personale in autonomia: il soggetto che intrattiene rapporti con la Pubblica Amministrazione non può da solo e liberamente procedere ad assunzioni di personale.

VI Divieto di concedere in autonomia prodotti e servizi a condizioni diverse da quelle standard: il soggetto che intrattiene rapporti con la Pubblica Amministrazione non può da solo e liberamente concedere prodotti e servizi a condizioni diverse da quelle standard.

Oltre ai suddetti divieti, la Società adotta ulteriori protocolli specifici in relazione alle singole attività sensibili elencate nel precedente paragrafo 1.3.

Relativamente all'attività sensibile n. **1** "**acquisizione (redazione e/o predisposizione delle domande/istanze) e/o gestione/destinazione di contributi/sovvenzioni/finanziamenti pubblici (nazionali e/o internazionali ricevuti, ad esempio, per attività di formazione, assunzione di personale, ristrutturazione immobili, ecc.)**", i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura che preveda: i) il coinvolgimento di più funzioni aziendali nella predisposizione di domande inviate a soggetti pubblici; ii) poteri di firma congiunta per le richieste all'ente erogante; iii) modalità di gestione dei contributi/finanziamenti; iv) il coinvolgimento di più funzioni aziendali nella rendicontazione sull'utilizzo del finanziamento; v) modalità di gestione delle eventuali verifiche da parte degli enti erogatori.

2 Segregazione: segregazione di funzioni tra chi propone la richiesta di un finanziamento agevolato, chi effettua lo studio di fattibilità per valutare la possibilità di accedere al finanziamento, chi raccoglie e predispone la documentazione necessaria per la richiesta e chi approva e sottoscrive la richiesta.

3 Controlli preventivi: effettuazione di studi di fattibilità per la verifica del possesso dei requisiti richiesti dalla legge per l'ottenimento del finanziamento; controlli sulla documentazione allegata alla richiesta di finanziamento al fine di garantire la completezza, accuratezza e veridicità dei dati comunicati alla P.A.

4 Ruoli/Responsabilità: l'attribuzione formale di poteri interni/responsabilità (es. attraverso

deleghe di funzione e disposizioni/comunicazioni organizzative) avviene nei confronti dei soggetti che istituzionalmente intrattengono rapporti con soggetti pubblici.

5 Autorizzazione e poteri: solo soggetti dotati di apposita procura sono legittimati a intrattenere rapporti con gli enti pubblici eroganti.

6 Monitoraggio periodico: monitoraggio periodico dei progetti coperti da finanziamenti pubblici allo scopo di garantire il persistere delle condizioni in base alle quali è stato ottenuto il finanziamento.

Relativamente all'attività sensibile n. **2** "**gestione delle domande e dei rapporti con Pubbliche Amministrazioni, aziende di Stato, enti ed uffici pubblici per l'ottenimento di concessioni, autorizzazioni e licenze e altri provvedimenti amministrativi inerenti all'esercizio delle attività aziendali (es. autorizzazioni per la costruzione e fornitura di reti di telecomunicazione, autorizzazioni per l'istallazione di siti radiomobili)**", i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura per la gestione delle richieste di licenze /autorizzazioni che preveda: i) segregazione delle funzioni aziendali coinvolte; ii) definizione di ruoli e responsabilità dei soggetti coinvolti; iii) modalità di archiviazione della documentazione rilevante.

2 Documentazione: esistenza di adeguata documentazione delle attività e conservazione della stessa in apposito archivio con divieto di cancellare o distruggere arbitrariamente i documenti archiviati.

3 Poteri/Responsabilità: l'attribuzione formale di poteri interni/responsabilità (es. attraverso deleghe di funzione e disposizioni/comunicazioni organizzative) avviene solo nei confronti della funzione che istituzionalmente intrattiene rapporti con la P.A.

4 Attività preventiva: formalizzazione dei contatti avuti con la P.A., preliminarmente alla richiesta dell'autorizzazione (richiesta di chiarimenti, verifiche ispettive propedeutiche all'ottenimento dell'autorizzazione).

5 Segregazione: segregazione di funzioni tra chi predispone la documentazione necessaria per la richiesta di una autorizzazione/licenza, chi la controlla e chi sottoscrive la richiesta.

6 Controlli preventivi: controlli sulla documentazione allegata alla richiesta di licenza/autorizzazione al fine di garantire la completezza, accuratezza e veridicità dei dati comunicati alla P.A.

7 Monitoraggio periodico: monitoraggio periodico volto a garantire il persistere delle condizioni in base alle quali è stata ottenuta l'autorizzazione e la tempestiva comunicazione alla P.A. di eventuali cambiamenti.

8 Scadenziario: monitoraggio tramite appositi scadenzari delle autorizzazioni/licenze ottenute al fine di richiedere il rinnovo delle stesse nel rispetto dei termini di legge.

Relativamente all'attività sensibile n. **3** "**negoziazione, stipulazione ed esecuzione di contratti e/o convenzioni con la Pubblica Amministrazione anche attraverso la partecipazione a procedure ad evidenza pubblica (aperte, negoziate o ristrette) o affidamenti diretti da parte di enti pubblici (es. contratti di vendita di prodotti e servizi ICT forniti dalla Società, contratti di locazione relativi a terreni/siti per l'istallazione di siti radiomobili)**", i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura per la partecipazione a procedure a evidenza

pubblica e gestione di contratti pubblici: i) definizione dei poteri e delle responsabilità dei soggetti coinvolti nel processo di negoziazione, stipulazione ed esecuzione di contratti e/o convenzioni con la Pubblica Amministrazione nel rispetto del principio di segregazione delle funzioni; ii) poteri di firma congiunta per la firma dei contratti pubblici; iii) formalizzazione delle verifiche necessarie per determinare l'ammissibilità della Società alla gara; iv) accesso ristretto alla documentazione inerente a contratti pubblici alle sole persone che ne abbiano necessità in considerazione delle loro funzioni aziendali; v) controllo formale dei provvedimenti pubblici di affidamento con il contenuto delle offerte.

2 Autorizzazione: l'eventuale vendita di prodotti e servizi ICT a condizioni diverse da quelle standard può avvenire solo in base a una delega o autorizzazione o procura a tal fine formalizzate.

3 Poteri ruoli e responsabilità: l'attribuzione formale di poteri interni/responsabilità (es. attraverso deleghe di funzione e disposizioni/comunicazioni organizzative) ed esterni (es. procure) avviene nei confronti dei soggetti che istituzionalmente intrattengono rapporti con gli enti pubblici aggiudicatori. Le fasi del processo di vendita sono approvate secondo uno schema che definisce i livelli autorizzativi sulla base delle caratteristiche economiche/tecniche del progetto.

4 Controlli preventivi: i) effettuazione di una verifica del possesso dei requisiti richiesti per l'affidamento del contratto; ii) controlli sulla documentazione allegata alle offerte al fine di garantire la completezza, accuratezza e veridicità dei dati comunicati alla P.A.

5 Accesso ristretto: accesso ristretto a determinati soggetti aziendali, chiaramente identificati, al sistema informatico utilizzato per la predisposizione dell'offerta di gara, al fine di impedire manipolazioni dei dati da trasmettere all'ente appaltante.

6 Coerenza delle offerte: controllo formale di conformità delle condizioni e dei termini della delibera di aggiudicazione a quanto previsto in fase di approvazione delle offerte.

Relativamente all'attività sensibile n. **4** "**gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici e collegamenti telematici (in entrata e in uscita) o trasmissione di dati su supporti informatici a soggetti pubblici – in particolare in materia societaria e fiscale**", i protocolli specifici sono i seguenti:

1 Autenticazione ai sistemi: è richiesta l'autenticazione individuale degli utenti tramite log in e password o altro sistema di autenticazione sicura.

2 Sistema di autorizzazione alle operazioni eseguibili sui dati: è previsto un sistema di autorizzazione (profili di utilizzo) per l'esecuzione di operazioni sui dati o per limitare la visibilità a un sottoinsieme dei dati stessi.

3 Liste di controllo: sono disponibili liste di controllo del personale abilitato all'accesso ai sistemi, nonché le autorizzazioni specifiche dei diversi utenti o categorie di utenti, nel caso in cui sia previsto un sistema di autorizzazione.

4 Obblighi degli utenti: la Società adotta procedure che definiscono gli obblighi degli utenti nell'utilizzo dei sistemi informatici.

5 Poteri: la facoltà di cancellare dati, liste di controllo e archivi è attribuita esclusivamente al servizio competente. Il servizio assicura la tracciabilità delle relative operazioni.

6 Altre misure di protezione: le principali misure di protezione adottate ai sensi dell'Allegato B del d.lgs. 196/2003 (politica di aggiornamento dell'antivirus, misure di *back up*, *disaster recovery*, ecc.) sono opportunamente documentate.

Relativamente all'attività sensibile n. **5** "**gestione dei contenziosi e controversie giudiziarie di qualsiasi genere, grado o giurisdizione nei quali sia coinvolta a qualsiasi titolo la Società**", i protocolli specifici sono i seguenti:

1 Procedura: la Società adotta una procedura per la gestione dei contenziosi giudiziali e stragiudiziali che prevede: i) segregazione delle funzioni aziendali coinvolte; ii) definizione di ruoli e responsabilità dei soggetti coinvolti; iii) modalità di archiviazione della documentazione rilevante.

2 Autorizzazione e poteri: solo soggetti dotati di apposita procura sono legittimati a intrattenere rapporti con l'Autorità Giudiziaria (di qualsiasi genere, grado e giurisdizione).

3 Documentazione: esistenza di adeguata documentazione delle attività e conservazione della stessa in apposito archivio con divieto di cancellare o distruggere.

4 Tariffario: adozione e utilizzo di un tariffario standard per la definizione del compenso da corrispondere ai consulenti legali.

5 Reporting: è svolta un'attività di reporting periodico sull'andamento delle cause in corso da parte dei consulenti legali.

6 Monitoraggio: monitoraggio interno sullo status dei contenziosi e reporting al management aziendale, relativo anche alle spese sostenute e da sostenere.

7 Verifica della prestazione: evidenza documentale del controllo sulla prestazione ricevuta e sulle spese addebitate, prima del benestare al pagamento, al fine di verificare la conformità al contratto.

Relativamente all'attività sensibile n. **6** "**gestione rapporti con autorità e soggetti pubblici nel normale svolgimento di attività aziendali (es. Enti Pubblici Locali, Agenzia delle Entrate, Guardia di Finanza, INPS, INAIL, Ispettorato del Lavoro, autorità competenti in materia di tutela della salute e sicurezza sul lavoro, VVFF, Sportello Unico per l'Immigrazione, Prefetture, Questure, Dipartimento Provinciale del Lavoro, ASL, Camere di Commercio, Agenzia delle dogane, uffici catastali e conservatorie, istituti universitari, ecc.) e nell'ambito di collaborazione in caso di indagini basate su comunicazioni elettroniche. Adempimenti e ispezioni**", i protocolli specifici sono i seguenti:

1 Procedura: la Società adotta una procedura per la gestione dei rapporti con tali soggetti che prevede: i) segregazione delle funzioni aziendali coinvolte; ii) definizione di ruoli e responsabilità dei soggetti coinvolti; iii) modalità di archiviazione della documentazione rilevante.

2 Poteri/Responsabilità: l'attribuzione formale di poteri interni/responsabilità (es. attraverso deleghe di funzione e disposizioni/comunicazioni organizzative) ed esterni (es. procure) avviene nei confronti dei soggetti che istituzionalmente intrattengono rapporti con gli enti pubblici.

3 Documentazione: esistenza di adeguata documentazione delle attività e conservazione della stessa in apposito archivio con divieto di cancellare o distruggere arbitrariamente i documenti archiviati.

4 Verifica: verifica della documentazione inviata o fornita alla P.A. – anche nell'ambito di verifiche e ispezioni – al fine di garantire la completezza, accuratezza e veridicità dei dati comunicati.

5 Reporting: attività di reporting verso il superiore gerarchico su quanto emerso nel corso dei contatti/riunioni/ verifiche/ispezioni avuti e sulle informazioni rilevanti acquisite presso tali

soggetti.

6 Adeguamento: condivisione dei risultati delle verifiche ispettive con i responsabili aziendali coinvolti al fine di definire il piano d'azione per la tempestiva implementazione delle azioni correttive necessarie a fronte di eventuali carenze rilevate dalla P.A.

7 Scadenziario: monitoraggio, effettuato tramite scadenzari, degli adempimenti richiesti al fine di garantire il rispetto dei termini di legge.

Con particolare riferimento ai rapporti con le autorità fiscali, valgono i seguenti ulteriori protocolli specifici:

8 Monitoraggio dell'evoluzione del piano normativo di riferimento, effettuato con il supporto di consulenti esterni, al fine di garantire l'adeguamento alle nuove leggi in materia fiscale.

9 Sistemi di doppio controllo preventivo e successivo per verificare la correttezza del calcolo delle imposte e approvazione formale della documentazione a supporto.

10 Monitoraggio costante attraverso uno scadenzario degli adempimenti di legge, al fine di evitare ritardi e imprecisioni nella presentazione di dichiarazioni e/o documenti fiscali.

11 Clausola di rispetto: inserimento nel contratto con i consulenti che supportano la Società nell'espletamento degli adempimenti fiscali della previsione relativa all'impegno della controparte a non adottare atti o intrattenere comportamenti tali da determinare una violazione del Business Code of Conduct e del Modello della Società nei rapporti con la stessa, nonché, più in generale, comportamenti che possano determinare la commissione, ovvero il tentativo, delle violazioni rilevanti ai fini della responsabilità amministrativa *ex* d.lgs. 231/2001.

Relativamente alle attività sensibili n. **7** "**gestione dei rapporti con altre Autorità pubbliche di vigilanza o regolamentari (es. Autorità Garante della Concorrenza e del Mercato, AGCOM, Autorità garante per la protezione dei dati personali, Ministeri, autorità governative, ecc.)**", i protocolli specifici sono i seguenti:

1 Procedura: la Società adotta una procedura per la gestione dei rapporti con tali soggetti che prevede: i) segregazione delle funzioni aziendali coinvolte; ii) definizione di ruoli e responsabilità dei soggetti coinvolti; iii) modalità di archiviazione della documentazione rilevante.

2 Autorizzazione e poteri: solo soggetti dotati di apposita procura sono legittimati a intrattenere rapporti con Autorità di vigilanza.

3 Documentazione: esistenza di adeguata documentazione delle attività e conservazione della stessa in apposito archivio con divieto di cancellare o distruggere arbitrariamente i documenti archiviati.

4 Verifica: verifica della documentazione da inviare o fornire all'Autorità di vigilanza per conto della clientela al fine di garantire la completezza, accuratezza e veridicità dei dati comunicati.

5 Reporting: è svolta attività di reporting al superiore gerarchico su quanto emerso nel corso dei contatti/riunioni avuti e sulle informazioni rilevanti acquisite presso Autorità di vigilanza.

1.4.2 Protocolli specifici relativi alle attività strumentali.

Relativamente all'attività strumentale n. **1** "**gestione dei flussi finanziari in entrata e in uscita**", i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura per la gestione dei flussi finanziari che definisca, fra l'altro: i) ruoli e responsabilità dei soggetti coinvolti; ii) tipologie di transazioni eseguibili direttamente dalle varie funzioni aziendali; iii) controlli specifici e preventivi da applicarsi in casi, tassativamente previsti, in deroga alla normale procedura (es. pagamenti urgenti); iv) regole per la gestione dei flussi finanziari che non rientrino nei processi tipici aziendali e che presentino caratteri di estemporaneità e discrezionalità; v) controlli della documentazione aziendale e, in particolare, delle fatture passive.

2 Autorizzazione e poteri: solo soggetti dotati di apposita delega o autorizzazione o procura formalizzate sono legittimati alla gestione e movimentazione dei flussi finanziari.

3 Documentazione: esistenza di documenti giustificativi delle risorse finanziarie utilizzate, con motivazione e attestazione di inerenza e congruità approvati da adeguato livello gerarchico e archiviati.

4 Preventivi e consuntivi: programmazione dei flussi economico-finanziari su base annuale.

5 Spese rimborsabili: definizione delle spese rimborsabili (tipologia e limiti).

6 Note spese: gestione delle note spese con specifiche funzioni di approvazione gerarchica da parte del supervisore previo controllo di merito.

7 Campionamenti: controllo di adeguatezza procedurale, di completezza e accuratezza dei giustificativi su base campionaria.

8 Utilizzo di carte di credito aziendali regolate da specifiche procedure per il pagamento delle spese rimborsabili.

9 Segregazione: concorrenza di più soggetti responsabili alla definizione delle risorse disponibili e degli ambiti di spesa, con l'obiettivo di garantire la costante presenza di controlli e verifiche incrociate su un medesimo processo/attività, volta tra l'altro a garantire una adeguata segregazione delle funzioni.

10 Scostamenti: verifica mensile degli scostamenti tra i risultati effettivi e quelli fissati nel budget; analisi delle cause degli scostamenti e necessità di autorizzazione delle differenze da parte dell'adeguato livello gerarchico.

11 Poteri bancari: il sistema dei poteri di firma bancari è caratterizzato da meccanismi di doppia firma per quanto attiene alle operazioni di maggiore rilevanza, secondo quanto di volta in volta definito dai regolamenti interni.

12 Conti correnti: apertura di conti correnti solo mediante doppia firma in Paesi che non garantiscano trasparenza; mensilmente è effettuata, e adeguatamente verificata, la riconciliazione dei conti bancari.

13 Riconciliazione automatica di pagamenti e incassi: il pagamento dei debiti e gli incassi dei crediti, inviati dalle banche sui sistemi aziendali, sono abbinate automaticamente con i debiti e crediti. Le partite non abbinate sono indagate e riconciliate.

14 Report: sono predisposti report periodici sull'utilizzo di risorse finanziarie con motivazioni e beneficiari, inviati al livello gerarchico superiore e archiviati.

Relativamente all'attività strumentale n. **2** "**gestione dell'attività relativa ad azioni di recupero di crediti insoluti**", i protocolli specifici sono i seguenti:

1 Segregazione di funzioni e responsabilità tra chi è incaricato del monitoraggio dei crediti scaduti e del relativo recupero, chi si occupa della contabilità clienti e chi si occupa dell'attività di gestione e registrazione degli incassi.

2 Chiara identificazione dei soggetti autorizzati a rappresentare la Società nei rapporti con la P.A. nelle attività di contatto legate al recupero dei crediti.

3 Formalizzazione dei principali contatti con la P.A., in particolare di quelli che sfociano in piani di rientro del credito.

4 Autorizzazione formale delle operazioni di cancellazione del credito e di emissione di note di credito nei confronti della P.A. e archiviazione della documentazione a supporto.

Relativamente all'attività strumentale n. **3** "**selezione e gestione dei rapporti con fornitori di beni e servizi (ivi inclusi consulenti in materia tecnico-finanziaria, legale o altro tipo), agenti e distributori**", i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura per la gestione degli acquisti che preveda: i) segregazione delle funzioni coinvolte; ii) definizione di ruoli e responsabilità dei soggetti coinvolti; iii) modalità di archiviazione della documentazione rilevante.

2 Autorizzazione formale: esistenza di un'autorizzazione formalizzata per gli acquisti.

3 Lista fornitori: i fornitori sono scelti all'interno di una lista gestita dalla funzione competente; l'inserimento/eliminazione dei fornitori dalla lista è basato su criteri qualitativi oggettivi per categoria di bene o servizio; l'individuazione, all'interno della lista, del fornitore del singolo acquisto è motivata e documentata.

4 Budget le spese per gli acquisti sono fatte rientrare nell'ambito del budget approvato per l'attività con riferimento allo specifico settore di business.

5 Centralizzazione: gestione centralizzata degli acquisti.

6 Conflict check: richiesta al fornitore di una dichiarazione relativa a eventuali rapporti/conflitti di interesse con esponenti della P.A.

7 Monitoraggio periodico delle prestazioni e dei requisiti dei fornitori ai fini dell'aggiornamento della Lista fornitori.

8 Gara: necessario ricorso al processo di gara per la selezione del fornitore per acquisti superiori a determinati importi.

9 Selezione: evidenza documentale del processo di selezione del fornitore e dell'approvazione della scelta da parte dell'adeguato livello gerarchico (in relazione all'importo dell'acquisto).

10 Ordini di acquisto: approvazione degli ordini d'acquisto di servizi e beni all'interno del sistema informatico in base a definiti livelli autorizzativi.

11 Clausola di rispetto: inserimento nel contratto/convenzione con i fornitori della previsione relativa all'impegno della controparte a non adottare atti o intrattenere comportamenti tali da determinare una violazione del Business Code of Conduct e del Modello della Società nei rapporti con la stessa, nonché, più in generale, comportamenti che possano determinare la commissione, ovvero il tentativo, delle violazioni rilevanti ai fini della responsabilità amministrativa *ex* d.lgs. 231/2001.

12 Anagrafica: la gestione dell'anagrafica fornitori è adeguatamente segregata; le modifiche all'anagrafica fornitori sono formalizzate e supportate da adeguata documentazione; periodicamente è effettuato un controllo dei fornitori presenti in anagrafica al fine di verificare l'adeguatezza dei requisiti qualitativi e quantitativi. Tutte le modifiche e gli inserimenti sono verificati con cadenza regolare.

13 Three way match: le fatture sono registrate in accordo al principio del three way match: la fattura è registrata solamente in presenza di un ordine adeguatamente approvato in accordo

con i limiti di spesa attribuiti a ogni dipendente in funzione delle proprie responsabilità e dell'evidenza del bene/servizio ricevuto; tale flusso è automatizzato e gestito all'interno del sistema informatico; i pagamenti sono effettuati da una funzione segregata rispetto alla contabilità fornitori e sono effettuati a fronte di fatture registrate nel sistema informatico; in casi specifici possono essere effettuati pagamenti anche con richiesta senza ordine, adeguatamente autorizzata e registrata a sistema.

14 Monitoraggio: periodicamente sono effettuati controlli per monitorare le fatture da ricevere.

15 Anticipi a fornitori sono consentiti solo se riferiti a ordini adeguatamente approvati e previsti da contratto.

16 Predisposizione e revisione dei contratti: la predisposizione e revisione dei contratti da stipulare avviene all'interno del sistema informatico da parte delle diverse funzioni aziendali coinvolte per approvazioni di diversa natura (tecnico-economica, legale, fiscale); tali funzioni assicurano la tracciabilità dei commenti e delle proposte di modifiche da apportare alla bozza del contratto sottoposto ad approvazione.

17 Revenue recognition: è effettuato un controllo sulla corretta applicazione del principio della "revenue recognition": tutti i servizi fatturati entro il periodo contabile di riferimento devono essere stati effettuati.

18 Note di credito: il modulo di richiesta note di credito è verificato e approvato con criteri gerarchici; l'emissione periodica delle note di credito è approvata da adeguati livelli autorizzativi e in accordo con il principio della segregazione di funzioni.

19 Riconciliazione: mensilmente è effettuata adeguata riconciliazione tra i saldi a credito, i partitari e gli estratti conto.

Con riferimento ai rapporti con gli agenti, valgono i seguenti protocolli specifici:

1 Selezione della controparte: la selezione dell'agente avviene secondo modalità definite che includono, ad esempio, richiesta di requisiti soggettivi relativi alla professionalità e onorabilità dell'agente.

2 Pagamenti: la Società effettua i pagamenti esclusivamente tramite bonifico bancario su conto corrente indicato dall'agente nel relativo contratto. In nessun caso la Società effettua pagamenti in contanti o per mezzo di titoli al portatore ovvero nei confronti di soggetto diverso dalla controparte e in luogo/Paese diverso da quello in cui l'agente ha reso i propri servizi.

3 Riconoscimento dei compensi, delle provvigioni e dei rimborsi spese: il riconoscimento/determinazione dei compensi, delle provvigioni e dei rimborsi spese e l'entità degli stessi viene operato secondo modalità predefinite e ancorato a parametri il più uniformi possibile, eventualmente precisati in apposito allegato al contratto di agenzia. In particolare, i rimborsi spese vengono effettuati soltanto a fronte della presentazione dei relativi giustificativi. La Società non effettua pagamenti a titolo di rimborso spese in assenza di tali giustificativi.

4 Controlli su compensi, provvigioni e rimborsi spese: provvigioni, bonus, premi e rimborsi spese sono preventivamente ed espressamente approvati dalla Società e non pagati con meccanismi di corresponsione "automatica". La Società effettua verifiche periodiche per controllare la determinazione di compensi e rimborsi spese. I meccanismi di incentivazione non contengono obiettivi eccessivamente ambiziosi o irrealizzabili.

5 Clausola di rispetto: inserimento nel contratto di agenzia della previsione relativa all'impegno della controparte a non adottare atti o intrattenere comportamenti tali da determinare una violazione del Business Code of Conduct e del Modello della Società nei

rapporti con la stessa, nonché, più in generale, comportamenti che possano determinare la commissione, ovvero il tentativo, delle violazioni rilevanti ai fini della responsabilità amministrativa *ex* d.lgs. 231/2001.

6 Divieto di cessione del contratto: il contratto è sottoposto a divieto di cessione, anche parziale, senza preventivo consenso scritto da parte della Società.

7 Esclusione del potere della controparte di rappresentare o vincolare la Società: è escluso, anche mediante apposita previsione contrattuale, ogni potere dell'agente di vincolare la Società in assenza della preventiva approvazione di quest'ultima.

Con riferimento ai rapporti con ai distributori, valgono i seguenti protocolli specifici:

1 Selezione della controparte: la selezione della controparte avviene secondo modalità definite che includono, ad esempio, richiesta di requisiti soggettivi relativi alla professionalità e onorabilità.

2 Clausola di rispetto: inserimento nel contratto di distribuzione della previsione relativa all'impegno della controparte a non adottare atti o intrattenere comportamenti tali da determinare una violazione del Business Code of Conduct e del Modello della Società nei rapporti con la stessa, nonché, più in generale, comportamenti che possano determinare la commissione, ovvero il tentativo, delle violazioni rilevanti ai fini della responsabilità amministrativa *ex* d.lgs. 231/2001.

Relativamente all'attività sensibile n. **4** "**gestione degli omaggi e delle spese di rappresentanza/gestione delle erogazioni liberali**", i protocolli specifici sono i seguenti:

1 Richiesta della Pubblica Amministrazione a ricevere erogazioni liberali: esistenza di una richiesta scritta della Pubblica Amministrazione al ricevimento delle erogazioni.

2 Modico valore: gli omaggi sono di modico valore e comunque tali da non poter essere interpretati come finalizzati ad acquisire favori o vantaggi in modo improprio o indebito.

3 Report: relazione periodica sulle spese per la concessione di omaggi, con motivazioni e nominativi dei beneficiari, inviata al livello gerarchico superiore, comunicata all'Organismo di Vigilanza e archiviata.

4 Elenco degli omaggi: gli omaggi sono sempre selezionati/acquistati sulla base di un elenco gestito dalla funzione competente e, comunque, da soggetto diverso da quello che intrattiene rapporti con la Pubblica Amministrazione.

5 Budget: le spese per omaggi/spese di rappresentanza rientrano nell'ambito del budget annuale approvato per le attività promozionali con riferimento allo specifico settore di business.

6 Oggetto e destinatari: definizione dei limiti che le singole elargizioni devono rispettare per quanto riguarda l'oggetto e la natura degli enti che possono ricevere elargizioni.

7 Approvazione: la richiesta è approvata da almeno due funzioni aziendali della Società prima dell'esecuzione dell'erogazione, sulla base di limiti di valore e oggetto predeterminati.

Relativamente all'attività strumentale n. **5** "**selezione e assunzione di personale dipendente (ivi compreso personale appartenente alle categorie protette o la cui assunzione è agevolata)**", i protocolli specifici sono i seguenti:

1 Procedura: la Società adotta una procedura per l'assunzione del personale che prevede: i) criteri di selezione dei candidati oggettivi e trasparenti (es. voto di laurea/diploma,

conoscenza di lingue straniere, precedenti esperienze professionali, ecc.); ii) tracciabilità delle fonti di reperimento dei curricula; iii) segregazione delle funzioni coinvolte nel processo; iv) definizione di ruoli e responsabilità dei soggetti coinvolti; v) modalità di archiviazione della documentazione rilevante.

2 Valutazione, incentivi, bonus: la Società adotta disposizioni aziendali in base alle quali gli obiettivi posti ai dipendenti nell'esercizio della loro attività e i meccanismi di incentivazione previsti non siano basati su target di performance palesemente immotivati e così "sfidanti" da risultare, di fatto, irraggiungibili con mezzi leciti.

La Società definisce: un sistema formalizzato di valutazione del personale basato sull'uso di criteri e moduli standard volto a verificare il grado di raggiungimento degli obiettivi definiti; l'erogazione degli incentivi basata sul collegamento diretto con gli obiettivi raggiunti; un tetto massimo all'erogazione degli incentivi.

Gli obiettivi devono rappresentare risultati specifici, non generici e misurabili.

3 Documentazione: esistenza di adeguata documentazione del processo di selezione e obbligo di conservare la relativa documentazione in apposito archivio, con divieto di cancellare o distruggere i documenti archiviati.

4 Rapporti con enti pubblici in sede di assunzione (categorie protette, ecc.): chiara identificazione del soggetto responsabile di effettuare il controllo di accuratezza e completezza dei dati inviati alla P.A.; segregazione di funzioni tra chi predispone la documentazione da inviare alla P.A. e chi la controlla prima dell'invio.

5 Monitoraggio delle scadenze da rispettare per le comunicazioni/denunce/adempimenti nei confronti degli enti pubblici competenti, tramite scadenzari e timetable inviati alle funzioni aziendali coinvolte per la raccolta e consolidamento dei dati.

6 Autorizzazione formale: l'assunzione di personale avviene solo in base a una delega o autorizzazione o procura formalizzate.

7 Procura: sono autorizzati a intrattenere rapporti con soggetti appartenenti alla P.A. o, comunque, con soggetti qualificabili come "pubblici", solo i soggetti muniti di apposita procura.

8 Anagrafica: segregazione delle funzioni tra chi aggiorna l'anagrafica dipendenti, chi provvede al calcolo dei cedolini e chi gestisce il loro pagamento; formale autorizzazione delle modifiche apportate all'anagrafica dipendenti e ai dati retributivi e controllo volto a garantire che le modifiche apportate all'anagrafica del personale (inserimento di nuovo personale, cancellazioni, modifiche delle retribuzioni) siano dovutamente autorizzate.

9 Effettività: utilizzo di meccanismi operativi di controllo atti a garantire la coerenza tra ore retribuite e ore di lavoro effettuate ed evitare il pagamento di salari/stipendi non dovuti o dovuti solo parzialmente.

10 Benefit: definizione formale dei criteri di assegnazione dei benefit aziendali in base a un sistema di obiettivi qualitativi e quantitativi.

11 Riconciliazioni periodiche tra i dati del personale e la contabilità generale.

12 Selezione: formalizzazione dei requisiti richiesti per la posizione da ricoprire e delle valutazioni dei diversi candidati nelle diverse fasi del processo di selezione; archiviazione della documentazione relativa al processo di selezione, al fine di garantire la tracciabilità dello stesso; richiesta al candidato di una dichiarazione relativa a eventuali rapporti di parentela con esponenti della P.A. o altri dipendenti della Società o del Gruppo.

13 Proposta di assunzione: formulazione dell'offerta economica in base a linee guida aziendali relative alla retribuzione e necessaria autorizzazione per offerte economiche superiori al

limite definito per la posizione.

14 Richiami al Modello: il contratto di lavoro prevede specifici richiami al Business Code of Conduct e al Modello.

CAPITOLO 2
I REATI SOCIETARI

2.1 I reati societari richiamati dall'articolo 25-*ter* del d.lgs. 231/2001[4]

2.1.1 False comunicazioni sociali (articolo 2621 del codice civile) e false comunicazioni sociali in danno della società, dei soci o dei creditori (articolo 2622 del codice civile)

Questo reato si realizza tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene con l'intenzione di ingannare i soci o il pubblico; ovvero tramite l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.

Si precisa che:

- soggetti attivi del reato possono essere amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, sindaci e liquidatori (trattasi, quindi, di cd. "reato proprio"), nonché coloro che secondo l'articolo 110 c.p. concorrono nel reato da questi ultimi commesso[5];
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- la condotta deve essere idonea a indurre in errore i destinatari delle comunicazioni;
- la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi;
- 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% o una variazione del patrimonio netto non superiore all'1%;
- in ogni caso il fatto non è punibile se conseguenza di valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10% da quella corretta;
- in particolare, la fattispecie delittuosa di cui all'articolo 2622 del codice civile:
  - consta dell'ulteriore elemento del danno patrimoniale cagionato ai soci o creditori;
  - è punibile a querela della parte lesa, salvo che si tratti di società quotate.

In via esemplificativa, si evidenzia che il reato in esame sussisterà, in presenza di un danno per i soci o per i creditori, anche nell'ipotesi in cui gli amministratori della società espongano nel bilancio fatti non rispondenti al vero senza l'intenzione di ledere gli interessi della società o addirittura al fine di risollevarne le sorti, potendo comportare, in questo caso, anche una responsabilità dell'ente: tipico è, ad esempio, il caso della creazione di riserve occulte illiquide, ottenute attraverso la sottovalutazione di poste attive o la sopravvalutazione di quelle passive per favorire l'autofinanziamento dell'impresa sociale, sacrificando l'interesse degli azionisti alla percezione dei dividendi.

[4] La descrizione del reato di aggiotaggio (previsto dall'art. 2637 c.c.), unitamente alle attività sensibili a esso connesse e ai protocolli specifici relativi a tali attività, è contenuta nel successivo Capitolo 3.

[5] Tale osservazione (relativa al c.d. concorso dell'*extraneus*) si applica, in linea di principio, a tutti i reati propri.

Essenziale appare dunque il richiamo dei soggetti tenuti alla redazione del bilancio al rispetto dei principi di compilazione dei documenti che lo costituiscono.

Una particolare attenzione è richiesta in sede di stima delle poste contabili: i responsabili devono attenersi al rispetto del principio di ragionevolezza ed esporre con chiarezza i parametri di valutazione seguiti, fornendo ogni eventuale informazione complementare che sia necessaria a garantire la veridicità del documento.

Il bilancio deve inoltre essere completo sotto il profilo dell'informazione societaria e, in particolare, contenere tutti gli elementi richiesti dalla legge, quali ad esempio quelli previsti dagli articoli 2424, per lo stato patrimoniale, 2425, per il conto economico, 2427, per la nota integrativa, del codice civile.

Analoga correttezza deve essere richiesta agli amministratori, ai direttori generali, ai sindaci, ai liquidatori (nonché ai soggetti che esercitino di fatto tali funzioni) nella redazione delle altre comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico, affinché le stesse contengano informazioni chiare, precise, veritiere e complete.

2.1.2 Falso in prospetto (articolo 173-bis del T.U. della finanza)

L'art. 34 *(Falso in prospetto),* comma 2, della legge 262/2005 ha abrogato l'art. 2623 del codice civile, che puniva il reato in esame[6].

La fattispecie criminosa è, attualmente, prevista e sanzionata dall'articolo 173-*bis (Falso in prospetto)* del T.U. della finanza.

Si precisa, con riferimento ai reati presupposto della responsabilità amministrativa *ex* d.lgs. 231/2001, che l'art. 25-*ter* del citato decreto richiama, attualmente, la norma civilistica abrogata, mentre non fa riferimento alcuno al reato introdotto dalla legge 262/2005. Le novità legislative sembrerebbero, quindi, comportare il venir meno della responsabilità amministrativa della società ai sensi dell'art. 25-*ter* con riferimento al reato di falso in prospetto.

Si ritiene in ogni caso opportuno, sia pure in difetto di un esplicito richiamo normativo in tal senso, sottoporre a particolare attenzione la predisposizione dei prospetti e dei documenti richiamati dall'art. 173-*bis* del T.U. della finanza[7].

Tale condotta criminosa consiste nell'esporre, nei prospetti richiesti ai fini dell'offerta al pubblico di prodotti finanziari o dell'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, false informazioni idonee a indurre in errore od occultare dati o notizie con la medesima intenzione.

Si precisa che:

---

[6] L'abrogato art. 2623 c.c., in vigore prima della modifica disposta dalla legge 262/2005, era il seguente: "Falso in prospetto - *Chiunque, allo scopo di conseguire per sé o per altri un ingiusto profitto, nei prospetti richiesti ai fini della sollecitazione all'investimento o dell'ammissione alla quotazione nei mercati regolamentati, ovvero nei documenti da pubblicare in occasione delle offerte pubbliche di acquisto o di scambio, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari del prospetto, espone false informazioni od occulta dati o notizie in modo idoneo ad indurre in errore i suddetti destinatari è punito, se la condotta non ha loro cagionato un danno patrimoniale, con l'arresto fino ad un anno.*
Se la condotta di cui al primo comma ha cagionato un danno patrimoniale ai destinatari del prospetto, la pena è dalla reclusione da uno a tre anni".

[7] E' opportuno, altresì, ricordare che il prospetto di sollecitazione, rivolto al pubblico in generale, in considerazione della sua precipua rilevanza esterna è stato classificato dalla giurisprudenza come "*comunicazione sociale*" di cui all'art. 2621 c.c. (si veda Cass. 9 aprile 1991, n. 226 in *Banca, borsa, titoli di credito*, 1992, II, 129) e che, pertanto, un comportamento illecito relativo alla redazione di tale documento potrebbe integrare i reati previsti in tema di false comunicazioni sociali, laddove non sia applicabile la norma contenuta nel citato art. 173-*bis* del T.U. della finanza.

- deve sussistere l'intenzione di ingannare i destinatari del prospetto;
- la condotta deve essere idonea a indurre in errore i destinatari del prospetto;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto.

2.1.3 Falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale (art. 27 d.lgs. 39/2010)

L'art. 37 del d.lgs. 39/2010 ha abrogato l'art. 2624 c.c., che puniva il reato in esame[8].

La fattispecie criminosa è, attualmente, prevista e sanzionata dall'art. 27 (*Falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale*) del d.lgs. 39/2010.

Si precisa, con riferimento ai reati presupposto della responsabilità amministrativa *ex* d.lgs. 231/2001, che l'art. 25-*ter* del citato decreto richiama, attualmente, la norma civilistica abrogata, mentre non fa riferimento alcuno al reato introdotto dal d.lgs. 39/2010. La novità legislativa sembrerebbe, quindi, comportare il venir meno della responsabilità amministrativa della società ai sensi dell'art. 25-*ter* con riferimento al reato di falsità nelle relazioni o nelle comunicazioni dei responsabili della revisione legale.

Si ritiene in ogni caso opportuno, sia pure in difetto di un esplicito richiamo normativo in tal senso, sottoporre a particolare attenzione la gestione dei rapporti con la società di revisione legale.

Si tratta di un reato proprio, per la cui commissione è richiesta la qualifica di "responsabile della revisione legale".

La società di revisione legale incaricata di effettuare la revisione legale dei conti (art. 14 d.lgs. 39/2010):

a) esprime con apposita relazione un giudizio sul bilancio di esercizio e sul bilancio consolidato, ove redatto;
b) verifica nel corso dell'esercizio la regolare tenuta della contabilità sociale e la corretta rilevazione dei fatti di gestione nelle scritture contabili.

Per l'esercizio dei suoi compiti, la società di revisione legale ha diritto di ottenere dagli amministratori della società sottoposta a controllo documenti e notizie utili all'attività di revisione legale e può procedere ad accertamenti, controlli ed esame di atti e documentazione.

Il reato può essere posto in essere mediante due condotte, alternative ed equivalenti:

a) mediante l'attestazione del falso, ovvero
b) mediante l'occultamento di informazioni concernenti la situazione economica, patrimoniale o finanziaria della società sottoposta a revisione.

In entrambi i casi la condotta deve essere idonea a indurre in errore i destinatari delle comunicazioni sulla situazione economica, patrimoniale o finanziaria della società soggetta a revisione.

[8] L'abrogato art. 2624 c.c., in vigore prima della modifica disposta dal d.lgs. 39/2010, era il seguente: "*I responsabili della revisione i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nelle relazioni o in altre comunicazioni, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni, attestano il falso od occultano informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, ente o soggetto sottoposto a revisione, in modo idoneo ad indurre in errore i destinatari delle comunicazioni sulla predetta situazione, sono puniti, se la condotta non ha loro cagionato un danno patrimoniale, con l'arresto fino a un anno.*
Se la condotta di cui al primo comma ha cagionato un danno patrimoniale ai destinatari delle comunicazioni, la pena è della reclusione da uno a quattro anni".

La condotta è sanzionata sia ove abbia cagionato un danno patrimoniale ai destinatari della comunicazione (delitto, punito con la reclusione da uno a quattro anni); sia ove tale danno non sia stato cagionato (contravvenzione, punita con l'arresto fino a un anno).

Il bene giuridico tutelato è dunque l'interesse patrimoniale dei destinatari delle relazioni o comunicazioni.

Quanto all'elemento soggettivo del reato, sono richiesti da un lato la generica consapevolezza della falsità e di ingannare i destinatari delle comunicazioni; dall'altro l'intenzione di conseguire per sé o per altri un ingiusto profitto.

Sanzioni più elevate sono previste se il reato è commesso:

- dal responsabile della revisione legale di un ente di interesse pubblico[9];
- dal responsabile della revisione legale di un ente di interesse pubblico per denaro o altra utilità data o promessa, ovvero in concorso con gli amministratori, i direttori generali o i sindaci della società assoggettata a revisione.

La pena si applica a chi dà o promette l'utilità nonché ai direttori generali e ai componenti dell'organo di amministrazione e dell'organo di controllo dell'ente di interesse pubblico assoggettato a revisione legale, che abbiano concorso a commettere il fatto.

2.1.4 Impedito controllo (articolo 2625 del codice civile)

Il reato consiste nell'impedire od ostacolare, mediante occultamento di documenti o altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali.

Si precisa che:

- soggetti attivi sono gli amministratori;
- si configura illecito penale, procedibile a querela di parte, se la condotta ha cagionato un danno ai soci.

Nello specifico il reato in oggetto potrebbe, a titolo esemplificativo, essere realizzato impedendo lo svolgimento di controlli da parte dei soggetti legittimati/organo di controllo mediante azioni (ad es. messa a disposizione di documentazione o informazioni non veritiere) od omissioni relative a informazioni, dati, documenti, ecc..

2.1.5 Formazione fittizia del capitale (articolo 2632 del codice civile)

Tale reato può consumarsi quando: è formato o aumentato fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali in misura complessivamente superiore all'ammontare del capitale sociale; sono sottoscritte reciprocamente azioni o quote; sono

[9] Ai sensi dell'art. 16 del d.lgs. 39/2010, sono enti di interesse pubblico: a) le società italiane emittenti valori mobiliari ammessi alla negoziazione su mercati regolamentati italiani e dell'Unione europea e quelle che hanno richiesto tale ammissione alla negoziazione; b) le banche; c) le imprese di assicurazione di cui all'articolo 1, comma 1, lettera u), del codice delle assicurazioni private; d) le imprese di riassicurazione di cui all'articolo 1, comma 1, lettera cc), del codice delle assicurazioni private, con sede legale in Italia, e le sedi secondarie in Italia delle imprese di riassicurazione extracomunitarie di cui all'articolo 1, comma 1, lettera cc-ter), del codice delle assicurazioni private; e) le società emittenti strumenti finanziari, che, ancorché non quotati su mercati regolamentati, sono diffusi tra il pubblico in maniera rilevante; f) le società di gestione dei mercati regolamentati; g) le società che gestiscono i sistemi di compensazione e di garanzia; h) le società di gestione accentrata di strumenti finanziari; i) le società di intermediazione mobiliare; l) le società di gestione del risparmio; m) le società di investimento a capitale variabile; n) gli istituti di pagamento di cui alla direttiva 2009/64/CE; o) gli istituti di moneta elettronica; p) gli intermediari finanziari di cui all'articolo 107 del TUB.

sopravvalutati in modo rilevante i conferimenti dei beni in natura, i crediti ovvero il patrimonio della società, nel caso di trasformazione.

Si precisa che soggetti attivi sono gli amministratori e i soci conferenti.

Con riferimento a eventuali profili di rischio, le operazioni idonee a integrare l'elemento oggettivo del reato in esame possono essere compiute per una pluralità di fini, molti dei quali realizzabili nell'interesse o a vantaggio dell'ente. Si pensi, in particolare, all'aumento fittizio del capitale sociale operato tramite una sopravvalutazione dei beni posseduti al fine di fornire all'esterno la rappresentazione - evidentemente fallace - di una solida situazione patrimoniale della società.

2.1.6 Indebita restituzione dei conferimenti (articolo 2626 del codice civile)

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

Si precisa che soggetti attivi sono gli amministratori.

La fattispecie in esame, così come quella successiva prevista dall'art. 2627, sanziona una condotta idonea a determinare un pregiudizio per la società, risolvendosi in una forma di aggressione al capitale sociale, a vantaggio dei soci.

Sotto un profilo astratto, pare invero difficile che il reato in esame possa essere commesso dagli amministratori nell'interesse o a vantaggio della società, implicando in tal modo una responsabilità dell'ente. Più delicato si presenta il problema in relazione ai rapporti intragruppo, essendo possibile che una società, avendo urgente bisogno di disponibilità finanziarie, si faccia indebitamente restituire i conferimenti effettuati ai danni di un'altra società del gruppo. In tale ipotesi, in considerazione della posizione assunta dalla prevalente giurisprudenza che disconosce l'autonomia del gruppo societario inteso come concetto unitario, è ben possibile che, sussistendone tutti i presupposti, possa configurarsi una responsabilità dell'ente per il reato di indebita restituzione dei conferimenti commesso dai suoi amministratori.

Nello specifico il reato in oggetto potrebbe, a titolo esemplificativo, essere realizzato facendosi restituire indebitamente i conferimenti, effettuati in una società del gruppo, in modo simulato attraverso il pagamento di servizi non resi o erogati a condizioni più onerose di quelle di mercato.

2.1.7 Illegale ripartizione degli utili e delle riserve (articolo 2627 del codice civile)

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

Si fa presente che:

- soggetti attivi sono gli amministratori;
- configura una modalità di estinzione del reato la restituzione degli utili o la ricostituzione delle riserve prima del termine previsto per l'approvazione del bilancio.

Con riferimento a eventuali profili di rischio valgono, al riguardo, le osservazioni compiute con riferimento alla disposizione precedente, risultando anche in tale caso particolarmente problematici i profili di rilevanza della fattispecie in esame in relazione alle operazioni intragruppo.

2.1.8 Illecite operazioni sulle azioni o quote sociali o della società controllante (articolo 2628 del codice civile)

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

Si fa presente che:

- soggetti attivi sono gli amministratori;
- configura una modalità di estinzione del reato la ricostituzione del capitale sociale o delle riserve prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta.

Con riferimento ai profili di rischio, va rilevato che, benché non vi sia un divieto assoluto in merito alle operazioni di *buy back*, la normativa vigente - nel prevedere una disciplina capillare della materia – lascia trasparire la diffidenza da parte del legislatore in merito a tali pratiche.

In realtà, le operazioni sulle azioni proprie appartengono alla fisiologia della gestione delle società e possono assolvere a varie funzioni sotto il profilo economico-aziendalistico, molte delle quali perseguite nell'interesse o a vantaggio dell'ente, e dunque idonee, ove sussistano gli estremi del reato di cui all'art. 2628, a dar luogo a una concorrente responsabilità dell'ente medesimo.

Si pensi, ad esempio, a operazioni di investimento di fondi sociali compiute a fini di speculazione finanziaria; ovvero al rastrellamento delle azioni per fronteggiare la prospettiva di scalate ostili mediante offerte pubbliche di acquisto; ovvero ancora, per le società quotate in borsa, a operazioni volte a regolarizzare i propri corsi azionari, evitando le oscillazioni del titolo in caso di assenza di domanda delle azioni della società.

Più problematica la configurabilità di una concorrente responsabilità dell'ente nell'ipotesi in cui l'operazione di *buy back* sia indirizzata più specificamente a fini interni alla compagine sociale, non direttamente riconducibili a un interesse generale dell'ente: così, ad esempio, nel caso di acquisto di azioni realizzato al fine di rafforzare il potere di una maggioranza rispetto alle minoranze, oppure di modificare degli assetti di potere esistenti.

Un'ultima considerazione riguarda le operazioni finanziarie di c.d. *leveraged buy out*, finalizzate all'acquisto di attività di un'azienda, o di partecipazioni di società (azioni o quote), finanziate da un consistente ammontare di debiti e da un limitato o nullo ammontare di mezzi propri, consentiti dall'utilizzo delle attività oggetto dell'acquisizione e dal flusso di cassa che l'investimento genererà in futuro. La rilevanza penale di tali operazioni - che era stata oggetto di dibattito in passato - è oggi espressamente esclusa dal legislatore.

Si rileva infine che ai sensi dell'art. 2474 c.c. le società a responsabilità limitata non possono in nessun caso acquistare o accettare in garanzia partecipazioni proprie, ovvero accordare prestiti o fornire garanzia per il loro acquisto o la loro sottoscrizione.

2.1.9 Operazioni in pregiudizio dei creditori (articolo 2629 del codice civile)

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

Si fa presente che:

- soggetti attivi sono gli amministratori;

- configura una modalità di estinzione del reato il risarcimento del danno ai creditori prima del giudizio.

Con riferimento a eventuali profili di rischio, trattandosi di un reato che è di regola commesso al fine di preservare l'interesse sociale, a scapito dei diritti dei creditori, evidente è il rischio che alla sua commissione da parte degli amministratori consegua un coinvolgimento della persona giuridica nel relativo procedimento penale.

Tipico è, ad esempio, il caso di una fusione tra una società in floride condizioni economiche e un'altra in stato di forte sofferenza, realizzata senza rispettare la procedura prevista dall'art. 2503 c.c. a garanzia dei creditori della prima società, che potrebbero vedere seriamente lesa la garanzia per essi rappresentata dal capitale sociale.

Essenziale appare dunque il richiamo - indirizzato in particolare agli amministratori - al rispetto delle norme civili poste a tutela dei creditori in fasi tanto delicate della vita della società.

2.1.10 Omessa comunicazione del conflitto d'interessi (articolo 2629-*bis del codice civile)*

Il reato è stato introdotto dall'articolo 31 della legge 262/2005.

La condotta criminosa consiste nella violazione degli obblighi di comunicazione imposti dall'art. 2391, comma 1, del codice civile[10], il quale prevede che si dia notizia agli amministratori e al collegio sindacale di ogni interesse, per conto proprio o di terzi, si abbia in una determinata operazione della società.

Si precisa che sono soggetti attivi del delitto l'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'art. 116 del T.U. della finanza, ovvero di un soggetto sottoposto a vigilanza ai sensi del T.U. bancario, del T.U. della finanza, del d.lgs. 209/2005 (*Codice delle assicurazioni private*), del d.lgs. 124/1993 (*Disciplina delle forme pensionistiche complementari*)[11].

2.1.11 Indebita ripartizione dei beni sociali da parte dei liquidatori (articolo 2633 del codice civile)

[10] Art. 2391 c.c.: "Interessi degli amministratori.- *L'amministratore deve dare notizia agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata; se si tratta di amministratore delegato, deve altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale, se si tratta di amministratore unico, deve darne notizia anche alla prima assemblea utile.*
Nei casi previsti dal precedente comma la deliberazione del consiglio di amministrazione deve adeguatamente motivare le ragioni e la convenienza per la società dell'operazione.
Nei casi di inosservanza a quanto disposto nei due precedenti commi del presente articolo ovvero nel caso di deliberazioni del consiglio o del comitato esecutivo adottate con il voto determinante dell'amministratore interessato, le deliberazioni medesime, qualora possano recare danno alla società, possono essere impugnate dagli amministratori e dal collegio sindacale entro novanta giorni dalla loro data; l'impugnazione non può essere proposta da chi ha consentito con il proprio voto alla deliberazione se sono stati adempiuti gli obblighi di informazione previsti dal primo comma. In ogni caso sono salvi i diritti acquistati in buona fede dai terzi in base ad atti compiuti in esecuzione della deliberazione.
L'amministratore risponde dei danni derivati alla società dalla sua azione od omissione.
L'amministratore risponde altresì dei danni che siano derivati alla società dalla utilizzazione a vantaggio proprio o di terzi di dati, notizie o opportunità di affari appresi nell'esercizio del suo incarico".
[11] Il d.lgs. 124/1993 è stato abrogato dall'art. 21 del d.lgs. 252/2005.

Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori.

Si fa presente che:

- soggetti attivi sono i liquidatori;
- costituisce una modalità di estinzione del reato il risarcimento del danno ai creditori prima del giudizio.

2.1.12 Illecita influenza sull'assemblea (articolo 2636 del codice civile)

La "condotta tipica" prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Con riferimento a eventuali profili di rischio, sono in particolare in considerazione le fraudolente manovre degli amministratori o di soci idonee a influenzare il costituirsi delle maggioranze assembleari, allo scopo di far assumere deliberazioni conformi all'interesse della società, ma che pure appaiono assunte in spregio dei diritti delle minoranze, nonché attraverso mezzi illeciti e tali da determinare un pregiudizio al corretto funzionamento degli organi sociali.

2.1.13 Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (articolo 2638 del codice civile)

La condotta criminosa si realizza attraverso l'esposizione nelle comunicazioni alle Autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza; ovvero attraverso l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

La condotta criminosa si realizza, altresì, quando siano, in qualsiasi forma, anche mediante omissione delle comunicazioni dovute, intenzionalmente ostacolate le funzioni delle Autorità di vigilanza.

Si precisa che:

- soggetti attivi sono gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti a obblighi nei loro confronti;
- la responsabilità si ravvisa anche nell'ipotesi in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto terzi.

2.1.14 Aggiotaggio (articolo 2637 c.c.)

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

2.2 Le sanzioni previste a carico dell'ente in relazione ai delitti societari

Ai sensi dell'art. 25-*ter* del Decreto, in relazione ai reati in materia societaria previsti dal codice civile, se commessi nell'interesse della società, da amministratori, direttori generali o liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica, si applicano le seguenti sanzioni pecuniarie:

(i) per la contravvenzione di false comunicazioni sociali, prevista dall'art. 2621 c.c., la sanzione pecuniaria da 100 a 150 quote (dove ciascuna quota corrisponde ad un importo variabile fra un minimo di € 258,22 ad un massimo di € 1.549,37);

(ii) per il delitto di false comunicazioni sociali in danno dei soci o dei creditori, previsto dall'art. 2622, comma 1, c.c., la sanzione pecuniaria da 150 a 330 quote;

(iii) per il delitto di false comunicazioni sociali in danno dei soci o dei creditori, previsto dall'art. 2622, comma 3, c.c., la sanzione pecuniaria da 200 a 400 quote;

(iv) per la contravvenzione di falso in prospetto, prevista dall'art. 2623, comma 1, c.c., la sanzione pecuniaria da 100 a 130 quote;

(v) per il delitto di falso in prospetto, previsto dall'art. 2623, comma 2, c.c., la sanzione pecuniaria da 200 a 330 quote;

(vi) per la contravvenzione di falsità nelle relazioni o nelle comunicazioni delle società di revisione, prevista dall'art. 2624, comma 1, c.c., la sanzione pecuniaria da 100 a 130 quote;

(vii) per il delitto di falsità nelle relazioni o nelle comunicazioni delle società di revisione, previsto dall'art. 2624, comma 2, c.c., la sanzione pecuniaria da 200 a 400 quote;

(viii) per il delitto di impedito controllo, previsto dall'art. 2625, comma 2, c.c., la sanzione pecuniaria da 100 a 180 quote;

(ix) per il delitto di formazione fittizia del capitale, previsto dall'art. 2632 c.c., la sanzione pecuniaria da 100 a 180 quote;

(x) per il delitto di indebita restituzione dei conferimenti, previsto dall'art. 2626 c.c., la sanzione pecuniaria da 100 a 180 quote;

(xi) per la contravvenzione di illegale ripartizione degli utili e delle riserve, prevista dall'art. 2627 c.c., la sanzione pecuniaria da 100 a 130 quote;

(xii) per il delitto di illecite operazioni sulle azioni o quote sociali o della società controllante, previsto dall'art. 2628 c.c., la sanzione pecuniaria da 100 a 180 quote;

(xiii) per il delitto di operazioni in pregiudizio dei creditori, previsto dall'art. 2629 c.c., la sanzione pecuniaria da 150 a 330 quote;

(xiv) per il delitto di indebita ripartizione dei beni sociali da parte dei liquidatori, previsto dall'art. 2633 c.c., la sanzione pecuniaria da 150 a 330 quote;

(xv) per il delitto di illecita influenza sull'assemblea, previsto dall'art. 2636 c.c., la sanzione pecuniaria da 150 a 330 quote;

(xvi) per il delitto di aggiotaggio, previsto dall'art. 2637 c.c. e per il delitto di omessa comunicazione del conflitto d'interessi previsto dall'art. 2629-*bis* c.c., la sanzione pecuniaria da 200 a 500 quote;

(xvii) per i delitti di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, previsti dall'art. 2638, commi 1 e 2, c.c., la sanzione pecuniaria da 200 a 400 quote.

Le sanzioni pecuniarie sopra richiamate sono aumentate di un terzo ciascuna se, in seguito alla commissione dei relativi reati, l'ente ha conseguito un profitto di rilevante entità.

2.3 Le attività individuate come sensibili ai fini del d.lgs. 231/2001 con riferimento ai reati societari

L'analisi dei processi aziendali della Società ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 25-*ter* del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai reati societari:

1. Tenuta della contabilità, redazione del bilancio d'esercizio, delle situazioni economiche infrannuali, delle relazioni e delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico.
2. Rapporti con il Collegio Sindacale, società di revisione legale e soci.
3. Operazioni sul capitale e destinazione degli utili.
4. Attività di preparazione delle riunioni assembleari, svolgimento e verbalizzazione delle assemblee.
5. Comunicazioni alle Autorità di vigilanza e gestione dei rapporti con le stesse.
6. Comunicazione del conflitto di interessi ai sensi dell'art. 2391, comma 1, c.c.
7. Liquidazione di società.
8. Emissione di comunicati tramite media (ad es.: stampa, sito internet, ecc.)
9. Gestione delle transazioni infragruppo.

2.4 Il sistema dei controlli

Per ognuna delle attività sensibili identificate, oltre ai sei protocolli generali indicati alla sezione I della Premessa della presente Parte Speciale, sono stati individuati i protocolli specifici di seguito elencati.

I protocolli generali e quelli specifici di seguito riportati sono stati recepiti dalla Società nell'ambito delle procedure indicate nell'Allegato n. 3.

2.4.1 Protocolli specifici relativi alle attività sensibili

Relativamente all'attività sensibile n. **1** "**tenuta della contabilità, redazione del bilancio d'esercizio, delle situazioni economiche infrannuali, delle relazioni e delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico**", i protocolli specifici sono i seguenti:

1 Norme: la Società adotta, e diffonde al personale coinvolto in attività di predisposizione del bilancio, norme che definiscano con chiarezza i principi contabili da adottare per la definizione delle poste del bilancio civilistico (e situazioni infrannuali) e le modalità operative per la loro contabilizzazione. Tali norme sono tempestivamente aggiornate dall'ufficio competente alla luce delle novità della normativa civilistica e diffuse ai destinatari sopra indicati.

2 Istruzioni di chiusura contabile: le chiusure annuali e infrannuali (per i relativi documenti contabili societari) nonché le relative modalità e la tempistica sono regolate da istruzioni rivolte alle funzioni/unità organizzative, che indicano dati e notizie che è necessario fornire alla funzione preposta alla predisposizione dei documenti di cui sopra.

3 Tracciabilità: il sistema informatico utilizzato per la trasmissione di dati e informazioni garantisce la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il responsabile di ciascuna funzione/unità coinvolta nel processo deve garantire la tracciabilità di tutti i dati e le informazioni finanziarie.

4 Riunioni tra società di revisione legale (ove esistente) e Collegio Sindacale: sono effettuate una o più riunioni tra la società di revisione legale (ove esistente) e il Collegio Sindacale, prima delle riunioni del Consiglio di Amministrazione e della relativa Assemblea indette per l'approvazione del bilancio, che abbiano per oggetto la valutazione di eventuali criticità emerse nello svolgimento delle attività di revisione legale dei conti.

5 Informazione pre-consiliare: circolazione con congruo anticipo, rispetto alla riunione di approvazione del bilancio, della bozza e, ove presente, del giudizio sul bilancio rilasciato dalla società di revisione legale, al Consiglio di Amministrazione.

6 Sottoscrizione da parte del massimo vertice esecutivo della c.d. lettera di attestazione o di manleva richiesta dalla società di revisione legale, ove esistente. La lettera è altresì siglata dal responsabile della funzione Finance e messa a disposizione dei membri del Consiglio di Amministrazione. Occorre precisare che tuttavia tale lettera non elimina di per sé la responsabilità della società di revisione.

7 Attività di formazione: sono svolte attività di formazione di base, rivolte alle funzioni/unità coinvolte nella redazione del bilancio e degli altri documenti connessi, in merito alle principali nozioni e problematiche giuridiche e contabili sul bilancio e alle relative norme di Gruppo.

8 Conservazione del fascicolo di bilancio: la Società adotta regole formalizzate che identificano ruoli e responsabilità relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall'approvazione del Consiglio di Amministrazione e dell'Assemblea, al deposito e pubblicazione (anche informatica) dello stesso fino alla relativa archiviazione.

9 Modifiche ai dati contabili: ogni modifica ai dati contabili di funzione/unità può essere effettuata solo dalla funzione/unità che li ha generati.

10 Regole di comportamento: regole di comportamento sono rivolte agli amministratori, ai direttori generali, ai sindaci e ai liquidatori al fine di richiedere la massima correttezza nella redazione delle altre comunicazioni imposte o comunque previste dalla legge e dirette ai soci o al pubblico. Tali regole prevedono che nelle comunicazioni siano inserite informazioni chiare, precise, veritiere e complete.

Relativamente all'attività sensibile n. **2** "**rapporti con il Collegio Sindacale, società di revisione legale e soci**", i protocolli specifici sono i seguenti:

1 Regole di comportamento: la Società prevede obblighi di massima collaborazione e trasparenza nei rapporti con il Collegio Sindacale e in occasione di richieste da parte dei soci.

2 Archiviazione: l'archiviazione di fonti e informazioni nei rapporti con soci e Collegio Sindacale è costantemente assicurata.

3 Obbligo di informativa verso l'Organismo di Vigilanza: le richieste di informazioni o documentazione ricevute dall'organo amministrativo o dai suoi delegati e provenienti dai soci o dal Collegio Sindacale sono comunicate all'Organismo di Vigilanza.

In caso di affidamento dell'incarico relativo alla revisione legale dei conti a una società di revisione legale, oltre all'estensione delle previsioni dei protocolli di cui ai precedenti punti 1, 2

e 3 nei confronti dei responsabili della revisione legale, troveranno applicazione i seguenti protocolli specifici:

4 Selezione della società di revisione legale e sua indipendenza nel mandato: le fasi di selezione della società di revisione legale e le regole per mantenere l'indipendenza della società di revisione legale, nel periodo del mandato, aderenti alle disposizioni normative emanate al fine di evitare che l'incarico sia affidato o permanga in capo a società di revisione legale che si trovano in una situazione di incompatibilità con la Società, sono regolamentate mediante apposite disposizioni aziendali.

5 Verifiche: il Collegio Sindacale verifica il grado di indipendenza della società di revisione legale alla luce delle regole e criteri fissati per la selezione e valutazione della società di revisione legale.

6 Obbligo di trasmettere alla società di revisione legale con congruo anticipo tutti i documenti relativi agli argomenti posti all'ordine del giorno delle riunioni dell'Assemblea o del Consiglio di Amministrazione sui quali debba esprimere un parere ai sensi di legge o in base a regolamenti interni.

7 Report: il Collegio Sindacale e il vertice aziendale sono periodicamente informati sullo stato dei rapporti con la società di revisione legale da parte delle funzioni istituzionalmente deputate ai rapporti con la stessa.

Relativamente all'attività sensibile n. **3** "**operazioni sul capitale e destinazione degli utili**", i protocolli specifici sono i seguenti:

1 Utili e riserve: il Consiglio di Amministrazione elabora adeguata motivazione al fine di giustificare la proposta di distribuzione di utili e riserve nel rispetto di quanto previsto dalla legge.

2 Documentazione: adeguata documentazione relativa al processo di elaborazione e approvazione della bozza di bilancio/situazioni infrannuali è predisposta e mantenuta da parte del Consiglio di Amministrazione con particolare riferimento alla formazione di utili e riserve.

3 Procedure: la Società adotta una procedura per la valutazione, autorizzazione e gestione delle operazioni sul capitale.

4 Operazioni straordinarie: le operazioni di riduzione del capitale sociale, fusione e scissione societaria sono disciplinate mediante apposite procedure.

Relativamente all'attività sensibile n. **4** "**attività di preparazione delle riunioni assembleari, svolgimento e verbalizzazione delle assemblee**", i protocolli specifici sono i seguenti[12]:

1 Procedure autorizzative**:** un flusso autorizzativo strutturato disciplina la predisposizione di progetti, prospetti e documentazione da sottoporre all'approvazione dell'Assemblea.

2 Regolamento assembleare: la Società approva, mantiene e applica un regolamento assembleare adeguatamente diffuso ai soci.

3 Regole per l'esercizio: la Società definisce le regole per il controllo dell'esercizio del diritto di voto e il controllo della raccolta ed esercizio delle deleghe di voto.

4 Gestione del verbale d'Assemblea: la Società definisce ruoli e responsabilità relativamente

[12] Attualmente Huawei è interamente partecipata da Huawei Technologies Cooperatief U.A. e pertanto allo stato non risultano applicabili i protocolli specifici che presuppongo la presenza di una pluralità di soci.

alla trascrizione, pubblicazione e archiviazione del verbale dell'Assemblea.

Relativamente all'attività sensibile n. **5** "**comunicazioni alle Autorità di vigilanza e gestione dei rapporti con le stesse**", i protocolli specifici sono i seguenti:

1 Archiviazione e segnalazioni nelle ispezioni: la Società identifica un soggetto/funzione responsabile per la gestione dei rapporti con l'Autorità di vigilanza in caso di ispezioni, appositamente delegato dai vertici aziendali. Tale disposizione aziendale disciplina anche le modalità di archiviazione, la tracciabilità delle informazioni fornite, nonché l'obbligo di segnalazione iniziale e di relazione sulla chiusura delle attività.

2 Archiviazione nelle comunicazioni scritte: il soggetto/funzione che redige le comunicazioni scritte alle Autorità di vigilanza assicura la tracciabilità delle relative fonti e degli elementi informativi, nonché l'archiviazione delle relative richieste pervenute.

3 Report: è prevista un'attività di reporting periodico al vertice aziendale sullo stato dei rapporti con le Autorità di vigilanza da parte dei soggetti/funzioni deputati ai rapporti con tali soggetti.

4 Obbligo di collaborazione e trasparenza: la Società adotta regole che sanciscano l'obbligo alla massima collaborazione e trasparenza nei confronti delle Autorità di vigilanza.

Relativamente all'attività sensibile n. **6** "**comunicazione del conflitto di interessi ai sensi dell'art. 2391, comma 1, c.c.**", il protocollo specifico è il seguente:

1 Comunicazione del conflitto di interessi: è previsto l'obbligo, per ciascun esponente di Huawei che assuma il ruolo di amministratore o di componente del consiglio di gestione in altra società, di comunicare, all'apertura della riunione del consiglio di amministrazione o del consiglio di gestione di tale società, agli altri amministratori o componenti del consiglio di gestione e al collegio sindacale o al consiglio di sorveglianza, l'eventuale presenza di interessi che – per conto di Huawei – abbia in una determinata operazione della società, precisando, ove presente, l'interesse, la natura, l'origine o la portata.

Relativamente all'attività sensibile n. **7** "**liquidazione di società"**, il protocollo specifico è il seguente:

1 Regole di comportamento: tutti coloro che svolgono attività di liquidatori (anche di fatto) di società del Gruppo sono chiamati, anche mediante l'emanazione di specifiche regole di comportamento, a comportarsi con la massima lealtà e correttezza nello svolgimento delle operazioni di liquidazione. La Società sottolinea in particolare il dovere di non procedere alla distribuzione ai soci dei beni sociali prima di aver soddisfatto le pretese dei creditori sociali o di aver accantonato le risorse a tal fine necessarie.

Relativamente all'attività sensibile n. **8** "**emissione di comunicati tramite *media* (ad es.: stampa, sito internet, ecc.)"**, i protocolli specifici sono i seguenti:

1 Processo di comunicazione all'esterno e archiviazione delle evidenze: la Società adotta una procedura in materia di informazione societaria che prevede: i) l'identificazione di ruoli e responsabilità per la comunicazione all'esterno; ii) che il soggetto/l'unità responsabile dell'emissione dei comunicati stampa e di elementi informativi similari, incluso l'inserimento di tali informazioni in *internet*, assicuri l'archiviazione delle relative fonti e delle informazioni; iii) che i soggetti/le unità che forniscono informazioni per la definizione

dei comunicati stampa e di elementi informativi similari ricevano gli stessi in bozza prima della loro diffusione al fine di verificare il corretto inserimento dei dati loro forniti; iv) l'archiviazione dei documenti.

2 Informazioni: i rapporti con i *media* concernenti informazioni che riguardino la Società sono gestiti d'intesa con la Capogruppo.

3 Regole di comportamento: i singoli esponenti della Società che siano contattati personalmente dalla stampa e/o dai *media* in generale osservano principi comportamentali stabiliti dalla Società. Tutti coloro che operano nell'interesse della Società sono tenuti a osservare il divieto di diffusione all'interno o all'esterno della Società, se non tramite il canale istituzionalmente previsto, di documenti ed informazioni acquisiti nello svolgimento dell'attività lavorativa.

4 Divieti: tutti coloro che operano nell'interesse della Società sono sottoposti al divieto di: i) diffondere notizie false o di porre in essere operazioni simulate o altri artifici volti a provocare una sensibile alterazione del prezzo di strumenti finanziari, quotati o non quotati; ii) porre in essere comportamenti fraudolenti diretti a danneggiare l'immagine presso il pubblico di una banca o di un gruppo bancario.

5 Operazioni su strumenti finanziari: la Società adotta procedure per l'autorizzazione, il controllo e la limitazione/divieto delle operazioni su strumenti finanziari che ciascuno degli Esponenti Aziendali e dei Dipendenti può porre in essere.

Relativamente all'attività sensibile n. **9** "**gestione delle transazioni infragruppo**", il protocollo specifico è il seguente:

1 Gli addebiti/accrediti a carico o in favore della Società per prestazioni ricevute/rese nei rapporti con altre società del Gruppo o riconducibili al Gruppo sono sottoposti a controllo periodico al fine di verificare l'effettiva esecuzione della prestazione, la coerenza delle modalità di esecuzione adottate con le prescrizioni normative di volta in volta applicabili e la compatibilità delle condizioni praticate con i criteri generalmente accettati per la determinazione del valore normale delle transazioni. Tale controllo si estende altresì a una verifica periodica dell'allineamento degli accordi infragruppo di *cost sharing*, *royalty*, *cash pooling* e similari, ove esistenti, ai principi vigenti in materia di prezzi di trasferimento.

CAPITOLO 3
I DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

3.1 I delitti informatici e trattamento illecito di dati richiamati dall'articolo 24-*bis* del d.lgs. 231/2001

3.1.1 Falsità riguardanti documenti informatici (art. 491-bis c.p.)

La norma, attraverso un rinvio alle disposizioni sulle falsità concernenti atti pubblici e scritture private, previste dal Codice Penale, ne dispone l'applicazione anche alle ipotesi in cui le rispettive previsioni riguardino un documento informatico.

In particolare, le norme del Codice Penale cui l'articolo in commento fa rinvio sono quelle contenute nel Capo III, Titolo VII, Libro II. Tra queste si segnalano:

- art. 476 c.p. ("*falsità materiale commessa dal pubblico ufficiale in atti pubblici*");
- art. 477 c.p. ("*falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative*");
- art. 478 c.p. ("*falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti*");
- art. 479 c.p. ("*falsità ideologica commessa dal pubblico ufficiale in atti pubblici*");
- art. 480 c.p. ("*falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative*");
- art. 482 c.p. ("*falsità materiale commessa dal privato*");
- art. 483 c.p. ("*falsità ideologica commessa dal privato in atto pubblico*");
- art. 484 c.p. ("*falsità in registri e notificazioni*");
- art. 485 c.p. ("*falsità in scrittura privata*");
- art. 486 c.p. ("*falsità in foglio firmato in bianco. Atto privato*");
- art. 487 c.p. ("*falsità in foglio firmato in bianco. Atto pubblico*");
- art. 488 c.p. ("*altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali*");
- art. 489 c.p. ("*uso di atto falso*");
- art. 490 c.p. ("*soppressione, distruzione e occultamento di atti veri*").

3.1.2 Accesso abusivo ad un sistema informatico[13] o telematico[14] (art. 615-ter. c.p.)

[13] Si rileva che l'art. 1 della Convenzione di Budapest individua come sistema informatico "*qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per l'elaboratore, compiono elaborazione automatica di dati*". "*Rientrano, dunque nella definizione tutti i dispositivi hardware che gestiscono dei dati attraverso uno o più programmi (software): si tratterà degli strumenti elettronici, informatici o telematici, sia che essi lavorino in rete, sia che lavorino in assoluta autonomia (telefoni cellulari, palmari) . Peraltro, sul punto era già intervenuta la Suprema Corte, affermando che per sistema informatico "deve intendersi un complesso di apparecchiature destinate a compiere una funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche, che sono caratterizzate dalla registrazione o memorizzazione*

L'art. 615-*ter* punisce chiunque 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 il diritto di escluderlo.

Il legislatore prevede sanzioni più elevate 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;
- il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- 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.

E', inoltre, previsto un aggravamento della sanzione qualora i fatti sopra descritti riguardino 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 norma non si limita alla tutela della *privacy* informatica e telematica, ovvero alla riservatezza dei dati memorizzati nei sistemi informatici o trasmessi con sistemi telematici, ma offre un'ampia tutela che si concreta nello *ius excludendi alios*.

3.1.3 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)

L'art. 615-*quater* sanziona chiunque, 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 ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Sanzioni più gravi sono previste se il fatto è commesso:

- 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;
- 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.

---

per mezzo di impulsi elettrici, su supporti adeguati di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazioni diverse, nonché costituito dalla elaborazione automatica di tali dati, in modo da generare informazioni costituite da un insieme, più o meno vasto, dei dati stessi, organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente" (Giordanengo, *op. cit.*). Quanto al concetto di "dati informatici", lo stesso è individuato dall'art, 1, comma I, lett. b), della medesima Convenzione che lo definisce come "*qualunque presentazione di fatti, informazioni o concetti in forma suscettibili di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione*". "*Rientrano, dunque in tale definizione tanto i programmi software, quanto i dati personali che mediante gli stessi vengono elaborati*" (Giordanengo, *I reati informatici: le intrusioni illecite*, in atti del convegno *I reati informatici e la responsabilità amministrativa degli enti*, Milano, 15 e 16 ottobre 2008).

[14] Per sistema telematico si intende, secondo un primo orientamento espresso in dottrina, ogni forma di telecomunicazione che si giovi dell'apporto informatico per la sua gestione, indipendentemente dal fatto che la comunicazione avvenga via cavo, via etere o con altri sistemi (cfr. Borruso, in AA.VV., *Profili penali dell'informatica*, Milano, 1994, 7 ss.). Altri riducono invece il significato del termine alle forme di comunicazione via cavo, ed essenzialmente alle comunicazioni via linea telefonica tra *computers* (cfr. Buonuomo, in AA.VV., *Profili penali dell'informatica*, Milano, 1994, 148 ss.).

Il bene giuridico tutelato dalla norma in oggetto sarebbe da individuarsi nella riservatezza delle chiavi d'accesso, considerate dal legislatore alla stregua di qualità personali riservate, in quanto identificatrici della persona[15]. Con questa previsione il legislatore ha voluto fornire una tutela anticipata dal momento che sanziona tutta una serie di condotte che sono preparatorie rispetto alla condotta descritta dal disposto di cui all'art. 615-*ter* (*Accesso abusivo ad un sistema informatico o telematico*).

3.1.4 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

L'art. 615-*quinquies* considera il fenomeno della diffusione dei c.d. virus.

La norma punisce chiunque, 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.

La norma intende preservare il corretto funzionamento delle tecnologie informatiche, punendo comportamenti prodromici al danneggiamento di un sistema informatico o telematico, delle informazioni, dati o programmi in esso contenuti sanzionato dall'art. 635-*bis* c.p. e ss.

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

L'art. 617-*quater* (così come il successivo art. 617-*quinquies*) è una norma volta a tutelare la sicurezza e la genuinità delle comunicazioni informatiche e telematiche.

La fattispecie punisce:

- chiunque fraudolentemente intercetta, impedisce o interrompe comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni informatiche o telematiche intercettate.

Sanzioni più elevate sono previste se il fatto è commesso:

- 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;
- 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;
- da chi esercita anche abusivamente la professione di investigatore privato.

3.1.6 Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

L'art. 617-*quinquies* punisce l'installazione, fuori dai casi consentiti dalla legge, di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

[15] Si veda Pica, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 80 ss.

Sanzioni più elevate sono previste se il fatto è commesso:

- 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;
- 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;
- da chi esercita anche abusivamente la professione di investigatore privato.

La norma tutela in forma anticipata il bene giuridico della riservatezza delle informazioni o notizie trasmesse per via telematica o elaborate da singoli sistemi informatici. Il legislatore ha ritenuto opportuno ricorrere allo schema del reato di pericolo per realizzare la più ampia tutela dell'interesse protetto.

3.1.7 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.)

L'art. 640-*quinquies* punisce la condotta posta in essere dal soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

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

La fattispecie si realizza quando chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Sanzioni più gravi sono previste se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

L'art. 5 della legge 48/2008 ha operato un complessivo riordino delle fattispecie di danneggiamento, riunendo sotto le norme dall'articolo 635-*bis* al 635-*quinquies* c.p., le varie figure di danneggiamento informatico e abrogando i commi 2 e 3 dell'art. 420 c.p. (*Attentato a impianti di pubblica utilità*). In particolare, il legislatore ha disposto lo scorporo tra le fattispecie di danneggiamento di sistemi informatici o telematici e quella di danneggiamento di informazioni, dati o programmi informatici.

Inoltre, è stata introdotta una distinzione tra i casi di danneggiamento di dati o sistemi con rilevanza meramente privatistica e i casi in cui sono poste in essere condotte volte a danneggiare dati o sistemi di pubblica utilità[16].

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

La fattispecie si realizza quando chiunque 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.

Sanzioni più elevate sono previste se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

[16] Si veda Giordanengo, *op. cit.*

È, inoltre, previsto un aumento della pena se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

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

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

È previsto un aumento della pena se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

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

La norma prevede sanzioni nel caso in cui il fatto previsto dal precedente articolo 635-*quater* 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.

Sanzioni più gravi sono previste se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile.

È, inoltre, previsto un aumento della pena se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

3.2 Le sanzioni previste a carico dell'ente in relazione ai delitti informatici e trattamento illecito di dati

L'art. 24-*bis* del Decreto prevede che per i reati sopra analizzati siano inflitte all'ente le seguenti sanzioni:

(i) in relazione alla commissione dei delitti di cui all'art. 615-*ter* ("*Accesso abusivo ad un sistema informatico o telematico* "), all'art. 617-*quater* ("*Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche*"), all'art. 617-*quinquies* ("*Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche*"), all'art. 635-*bis* ("*Danneggiamento di informazioni, dati e programmi informatici*"), all'art. 635-*ter* ("*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità*"), all'art. 635-*quater* ("*Danneggiamento di sistemi informatici o telematici*"), all'art. 635-*quinquies* ("*Danneggiamento di sistemi informatici o telematici di pubblica utilità*") c.p., si applicano:

- la sanzione pecuniaria in misura compresa tra 100 e 500 quote (dove ciascuna quota corrisponde ad un importo variabile fra un minimo di € 258,22 ad un massimo di € 1.549,37), nonché
- in caso di condanna, le sanzioni interdittive di cui all'art. 9, comma 2, lett. a) del Decreto (i.e. interdizione dall'esercizio dell'attività), all'art. 9, comma 2, lett. b) del Decreto (i.e. sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito) ed all'art. 9, comma 2, lett. e) del Decreto (i.e. divieto di pubblicizzare beni o servizi).

(ii) In relazione alla commissione dei delitti di cui all'art. 615-*quater* ("*Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici*") ed all'art. 615-*quinquies* ("*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico*") c.p. si applicano:

- la sanzione pecuniaria fino a 300 quote, nonché
- in caso di condanna, le sanzioni interdittive di cui all'art. 9, comma 2, lett. b) del Decreto (i.e. sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito) ed all'art. 9, comma 2, lett. e) del Decreto (i.e. divieto di pubblicizzare beni o servizi).

(iii) In relazione alla commissione dei delitti di cui all'art. 491-*bis* ("*Falsità riguardanti documenti informatici* ") ed all'art. 640-*quinquies* ("*Frode informatica del soggetto che presta servizi di certificazione di firma elettronica*") c.p., salvo quanto previsto dall'art. 24 del Decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applicano:

- la sanzione pecuniaria fino a 400 quote, nonché
- in caso di condanna, le sanzioni interdittive di cui all'art. 9, comma 2, lett. c) del Decreto (i.e. divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio), all'art. 9, comma 2, lett. d) del Decreto (i.e. esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi) ed all'art. 9, comma 2, lett. e) del Decreto (i.e. divieto di pubblicizzare beni o servizi).

3.3 Le attività individuate come sensibili ai fini del d.lgs. 231/2001 con riferimento ai delitti informatici e trattamento illecito di dati

L'analisi dei processi aziendali della Società ha consentito di individuare le attività nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'articolo 24-*bis* del d.lgs. 231/2001. Qui di seguito sono elencate le cosiddette attività sensibili o a rischio identificate con riferimento ai delitti informatici e trattamento illecito di dati:

1. Definizione delle regole da adottare in materia di sicurezza del sistema informatico e telematico.
2. Gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione.
3. Gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni.
4. Gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni, ecc.) e delle attività di inventariazione dei beni.
5. Acquisizione e gestione di apparecchiature, di dispositivi (anche di rilevazione) connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione).
6. Monitoraggio/verifica periodica del sistema informatico e gestione degli incidenti e dei problemi di sicurezza informatica.

3.4 Il sistema dei controlli.

Per ognuna delle attività sensibili identificate, oltre ai sei protocolli generali indicati alla sezione I della Premessa della presente Parte Speciale, sono stati individuati i protocolli specifici di seguito elencati.

I protocolli specifici riportati sono da applicarsi in base alla tipologia e caratteristiche dell'apparato/applicazione informatica nonché alla classe di appartenenza nella catena tecnologica (come in seguito evidenziato):

- applicazioni;
- *database*;
- sistema operativo;
- apparato di sicurezza/accesso perimetrale (IDS, *firewall*, *proxy*, VPN);
- apparato di connettività (*router*, *switch*, centrale di comunicazione);
- altro *device* (centralina di misurazione e comunicazione).

I protocolli generali e quelli specifici di seguito riportati sono stati recepiti dalla Società nell'ambito delle procedure indicate nell'Allegato n. 4.

3.4.1 Protocolli specifici relativi alle attività sensibili

Relativamente all'attività sensibile n. **1** "**definizione delle regole da adottare in materia di sicurezza del sistema informatico e telematico**", i protocolli specifici sono i seguenti:

1 Disposizioni sulla sicurezza: le regole in materia di sicurezza del sistema informatico e telematico adottate dalla Società includono:

   a) la definizione della metodologia nell'analisi e valutazione dei rischi, degli obiettivi della sicurezza, delle linee guida, degli strumenti normativi e delle modalità di aggiornamento, anche a seguito di cambiamenti significativi;

   b) l'identificazione dei ruoli e delle responsabilità dei soggetti coinvolti;

   c) i rapporti con gli *outsourcer* informatici;

   d) la definizione di clausole contrattuali relative alla gestione delle misure di sicurezza da parte degli *outsourcer*;

   e) la definizione di ruoli e responsabilità nel trattamento dei dati e delle informazioni e i relativi principi di classificazione (confidenzialità, autenticità e integrità).

2 Risorse umane e sicurezza: nell'ambito della gestione delle risorse umane la Società provvede all'applicazione delle seguenti misure:

   a) una valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza del sistema informatico;

   b) l'attuazione di specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza del sistema informatico per tutti i dipendenti e, dove rilevante, per i terzi;

   c) l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, *token* di autenticazione, ecc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto.

3 Amministratori di sistema: la Società adempie alle prescrizioni del Garante per la protezione dei dati personali in tema di attribuzione delle funzioni di amministratore di sistema[17], con riferimento, in particolare, a quanto segue:

a) la valutazione delle caratteristiche soggettive;

b) le designazioni individuali;

c) l'elenco degli amministratori di sistema;

d) i servizi in *outsourcing* (servizi forniti da terze parti anche interne al Gruppo);

e) la verifica delle attività;

f) la registrazione degli accessi.

Relativamente all'attività sensibile n. **2** "**gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione**", i protocolli specifici sono i seguenti:

1 Organizzazione della sicurezza per gli utenti interni ed esterni o operatori di sistema: la Società definisce ruoli e responsabilità degli utenti interni ed esterni all'azienda o operatori di sistema ai fini della sicurezza del sistema, e i connessi obblighi nell'utilizzo del sistema informatico e delle risorse informatiche e telematiche (anche con riferimento all'accesso a risorse telematiche in possesso di enti terzi la cui gestione del sistema di sicurezza ricade sulla parte terza stessa).

2 Controllo degli accessi: l'accesso alle informazioni, al sistema informatico, alla rete, ai sistemi operativi e alle applicazioni viene sottoposto a controllo da parte della Società attraverso l'adozione di misure selezionate in base alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:

a) l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e *password* o altro sistema di autenticazione sicura (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);

b) le autorizzazioni specifiche dei diversi utenti o categorie di utenti (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);

c) procedimenti di registrazione e deregistrazione per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati, l'accesso a tutti i sistemi e servizi informativi, anche di terzi (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);

d) la rivisitazione periodica dei diritti d'accesso degli utenti (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);

e) l'accesso ai servizi di rete esclusivamente da parte degli utenti specificamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete (anche se tali diritti permettono di connettersi a reti e dispositivi di terze parti, la cui gestione del sistema di sicurezza ricade sulla parte terza stessa);

f) la chiusura di sessioni inattive dopo un limitato periodo di tempo (valido per le postazioni di lavoro e per le connessioni ad applicazioni, come ad esempio *screen saver*).

[17] Provvedimento emesso in data 27 novembre 2008.

Relativamente all'attività sensibile n. **3** "**gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni**", i protocolli specifici sono i seguenti:

1 Crittografia: la Società utilizza controlli crittografici per la protezione delle informazioni e regolamenta la gestione delle chiavi crittografiche al fine di evitare un uso non appropriato della firma digitale.

2 Gestione delle comunicazioni e dell'operatività: la sicurezza del sistema informatico e telematico viene garantita da parte della Società attraverso l'adozione di misure selezionate in base alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:

   a) le misure volte a garantire e monitorare la disponibilità degli elaboratori di informazioni (valido per tutte le applicazioni sulla base delle funzionalità di sicurezza disponibili e per i *database* e i sistemi operativi da esse sottese);

   b) la protezione da *software* pericoloso (es. *worm* e virus) (valido, sotto forma di antivirus per gli ambienti *microsoft* sia *client* che *server* e di *patch management* per gli altri sistemi e apparati di comunicazione come *router*, *switch* e per apparati *firewall*);

   c) il *backup* di informazioni di uso centralizzato e del *software* applicativo ritenuto critico (valido per le applicazioni e *database* da esse sottese) nonché delle informazioni salvate nelle aree condivise centralizzate;

   d) la previsione e la disponibilità, anche per gli utenti finali, di strumenti di protezione volti a garantire la sicurezza nello scambio di informazioni critiche per il *business* aziendale e di carattere confidenziale anche con terzi;

   e) gli strumenti per effettuare:

      i. la registrazione delle attività eseguite sulle applicazioni, sui sistemi e sulle reti che abbiano diretto impatto sulla sicurezza o relative agli accessi alle risorse informatiche e telematiche;

      ii. la registrazione delle attività effettuate dagli utenti verso l'esterno della rete aziendale (es. traffico *http*);

      iii. la protezione delle informazioni registrate (*log*) contro accessi non autorizzati;

   f) una verifica periodica/a evento dei *log* che registrano, per quanto rilevante ai fini della sicurezza, gli eventi, le attività degli utilizzatori e le eccezioni (valido per applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (*proxy*, *firewall*, IDS, *router*);

   g) il controllo che i cambiamenti effettuati agli elaboratori e ai sistemi (valido per le applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (*proxy*, *firewall*, IDS, *router*) non alterino i livelli di sicurezza;

   h) le regole per la corretta gestione e custodia dei dispostivi di memorizzazione (ad es. PC, telefoni, chiavi USB, CD, *hard disk* esterni, ecc.).

Relativamente all'attività sensibile n. **4** "**gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni, ecc.) e delle attività di inventariazione dei beni**", il protocollo specifico è il seguente:

1 Sicurezza fisica e ambientale: la Società:

   a) dispone l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature con particolare attenzione ai locali dedicati ai centri di

elaborazione dati gestiti direttamente;

b) dispone l'adozione di controlli al fine di prevenire danni e interferenze alle apparecchiature gestite direttamente che garantiscono la connettività e le comunicazioni;

c) assicura l'inventariazione degli *asset* aziendali (inclusi i *database* in essi contenuti) utilizzati ai fini dell'operatività del sistema informatico e telematico.

Relativamente all'attività sensibile n. **5** "**acquisizione e gestione di apparecchiature, di dispositivi (anche di rilevazione) connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione)**", il protocollo specifico è il seguente:

1 Sicurezza nell'acquisizione, sviluppo e manutenzione del sistema informatico (o della componente informatica presente nel servizio) e/o delle componenti tecniche connesse con il sistema: la Società identifica i requisiti di sicurezza e di conformità tecnica (ove applicabile) in fase di acquisizione, sviluppo, fornitura e manutenzione del sistema informatico (inclusivo di componente *hardware*, *software* e delle componenti tecniche connesse).

Relativamente all'attività sensibile n. **6** "**monitoraggio/verifica periodica del sistema informatico e gestione degli incidenti e dei problemi di sicurezza informatica**", i protocolli specifici sono i seguenti:

1 Gestione degli incidenti e dei problemi di sicurezza informatica: il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica include:

a) l'adozione di canali gestionali per la comunicazione degli incidenti e problemi (relativamente a tutta la catena tecnologica);

b) la registrazione, conservazione e analisi periodica degli incidenti e problemi, singoli e ricorrenti e l'individuazione della *root cause* e delle azioni preventive (relativamente a tutta la catena tecnologica);

c) la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva (relativamente a tutta la catena tecnologica).

2 Audit/Monitoraggio: la Società assicura lo svolgimento di attività di monitoraggio/verifica periodica dell'efficacia e operatività del sistema di gestione della sicurezza informatica sia in ambito applicativo che in ambito infrastrutturale, adottando le misure di verifica definite in base alle diverse categorie tecnologiche.

3 Amministratori di sistema: la Società adempie alle prescrizioni del Garante per la protezione dei dati personali in tema di attribuzione delle funzioni di amministratore di sistema, con riferimento, in particolare, a quanto segue:

a) la valutazione delle caratteristiche soggettive;

b) le designazioni individuali;

c) l'elenco degli amministratori di sistema;

d) i servizi in *outsourcing* (servizi forniti da terze parti anche interne al Gruppo);

e) la verifica delle attività;

f) la registrazione degli accessi.

CAPITOLO 4
I REATI IN MATERIA DI TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

4.1 Le caratteristiche specifiche dei modelli organizzativi ai sensi dell'art. 30 del d.lgs. 81/2008 (c.d. "Testo Unico sulla Sicurezza")

Huawei ha considerato rilevanti per la Società le fattispecie di reato richiamate dall'art. 25-*septies* del Decreto ovvero i reati commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro ed, in particolare, come sarà più ampiamente illustrato *infra*:

- l'omicidio colposo (art. 589, comma 2, c.p.);
- le lesioni personali colpose gravi o gravissime (art. 590, comma 3, c.p.).

Huawei ha quindi proceduto alla elaborazione e costruzione del Modello in applicazione sia dell'art. 6, comma 2, d.lgs. 231/2001 sia dell'art. 30 del d.lgs. 9 aprile 2008 n. 81 ("TUS" o "d.lgs. 81/2008").

Come già esposto nella Parte Generale, l'art. 6 del d.lgs. 231/2001 individua i criteri, i contenuti e requisiti generali propri dei modelli di organizzazione, i quali devono:

- individuare le attività "*a rischio-reato*";
- prevedere specifici protocolli di formazione-attuazione delle decisioni concernenti i reati da prevenire;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
- prevedere obblighi di informazione nei confronti dell'organismo di vigilanza sul funzionamento e l'osservanza del modello;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Inoltre, lo stesso art. 6 stabilisce che il modello può essere efficacemente attuato solo qualora siano posti in essere:

- una verifica periodica e eventuale modifica dello stesso, quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

A fronte di tali requisiti generali, e quindi validi per la costruzione di un Modello volto alla prevenzione di tutti i c.d. reati presupposto, l'art. 30 del d.lgs. 81/2008 stabilisce in via esplicita e specifica quali sono le caratteristiche che il Modello deve presentare per avere efficacia esimente della responsabilità amministrativa delle persone giuridiche in relazione ai reati compiuti in violazione delle norme in materia di salute e sicurezza sul lavoro[18], individuando, in particolare, le seguenti:

[18] In via preliminare, è interessante notare come l'art. 30 si collochi all'interno della Sezione II del Capo III del d.lgs. 81/2008, in cui viene disciplinata la specifica fase della valutazione dei rischi, a dimostrazione dello stretto rapporto esistente tra la fase di risk assessment e i modelli di organizzazione e gestione, confermando che solamente sulla base di un approfondito risk assessment può essere costruito un idoneo sistema di governo del rischio.

- attitudine ad assicurare il rispetto della normativa in materia prevenzionale e la registrazione delle attività relative, con specifico riferimento:

  "a) al rispetto degli standard tecnico-strutturali di legge relative ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

  b) alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;

  c) alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazione dei rappresentanti per la sicurezza;

  d) alle attività di sorveglianza sanitaria;

  e) alle attività di informazione e formazione dei lavoratori;

  f) alle attività di vigilanza con riferimenti al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;

  g) alla acquisizione di documentazioni e certificazioni obbligatorie di legge;

  h) alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate".

  (comma 1);
- previsione di una articolazione di funzioni atta ad assicurare la salvaguardia degli interessi protetti (comma 3);
- predisposizione di idoneo sistema di controllo sull'attuazione del medesimo Modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate (comma 4).

Ne consegue che l'efficacia esimente del Modello in relazione ai reati commessi in violazione della normativa antinfortunistica sarà subordinata e non potrà prescindere dalla efficace previsione e adozione di

- protocolli e procedure idonee a garantire la conformità dei propri comportamenti al rispetto della legislazione vigente, in ogni prevedibile circostanza (ivi comprese le potenziali situazioni di emergenza) tracciandone, con apposita registrazione, l'avvenuta effettuazione dell'attività di controllo (art. 30, comma 2);
- una organizzazione funzionale, dovutamente formalizzata, adeguata alla gestione delle problematiche inerenti la salute e sicurezza sul lavoro, che individui quali compiti devono essere svolti da parte di ogni attore che partecipa ai processi decisionali (art. 30, comma 3), a partire dal datore di lavoro fino a raggiungere ogni singolo lavoratore riservando particolare attenzione alle figure specifiche previste dalla normativa di riferimento (es. responsabile del servizio di prevenzione e protezione, medico competente, addetto al primo soccorso, etc.);
- un sistema di controllo in grado di:
  - verificare l'adeguatezza del Modello in ordine alla sua reale capacità di prevenire i reati in materia antinfortunistica;
  - vigilare sull'effettività del Modello (verifica della coerenza tra i comportamenti concreti ed il Modello istituito);
  - analizzare il mantenimento nel tempo delle condizioni di idoneità delle misure preventive adottate;
  - aggiornare il Modello quando "*siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico*".

4.2 I reati in materia di tutela della salute e della sicurezza sul lavoro richiamati dall'art. 25-*septies* del d.lgs. 231/2001

L'art. 9 della legge 3 agosto 2007 n. 123, così come sostituito dall'art. 300 del d.lgs. 81/2008, ha esteso l'ambito applicativo della responsabilità da reato degli enti ai delitti "*di cui agli articoli 589 e 590, terzo comma, c.p. commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*" ossia alle ipotesi di omicidio colposo (aggravato) e di lesioni gravi o gravissime (aggravate), prevedendo altresì le sanzioni (pecuniarie e interdittive) a carico dell'ente.

4.2.1 Omicidio colposo aggravato

L' art. 589, comma 2, c.p. recita : "*Chiunque cagiona per colpa la morte di una persona (...) se il fatto è commesso con violazione delle norme per la prevenzione degli infortuni sul lavoro, è punito con la pena della reclusione da due a sette anni*".

Le principali caratteristiche della fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: la norma tutela la vita umana sanzionando i comportamenti che provochino la morte per colpa del reo con condotte che violino le regole dettate a tutela dell'incolumità del lavoratore (siano esse previste da norme specifiche e sia dalla norma di "*chiusura*" del sistema, l'art. 2087 c.c.);
- *soggetto attivo*: malgrado il soggetto attivo del reato possa essere "*chiunque*", il rimprovero per non aver tenuto la condotta assunta come causa dell'evento è mosso a colui o coloro che, per il ruolo nell'organizzazione e nel luogo di lavoro interessato all'evento, si ritiene avrebbero dovuto adottare o imporre l'osservanza di una data misura protettiva[19];
- *nesso di causalità*: ai sensi dell'art. 40, comma 1, c.p. "*nessuno può essere punito per un fatto preveduto dalla legge come reato, se l'evento dannoso o pericoloso, da cui dipendente l'esistenza del reato, non è conseguenza della sua azione od omissione*". Per poter stabilire che un determinato evento è conseguenza di una azione od omissione si deve ricorrere alla c.d. "condicio sine qua non", per cui, se si elimina la detta azione od omissione, viene meno anche l'evento. Ovviamente per poter affermare che una azione (od omissione) costituisce condizione necessaria di un evento bisogna ricorrere a nozioni scientifiche o anche statistiche che dimostrino che v'è consequenzialità tra quella condotta e quell'evento. Poiché è impossibile conoscere tutti gli aspetti dei fatti e tutti i profili della situazione storica, il giudizio sul nesso di causalità è, in fondo, un giudizio di "alta probabilità" o di probabilità logica o razionale credibilità circa la consequenzialità di un evento ad una condotta. In caso di omicidio colposo, in particolare, il rapporto di causalità tra la condotta dell'imputato e l'evento non resta escluso per il solo fatto che tale condotta non sarebbe stata idonea a produrre l'evento stesso senza il concorso della condotta antigiuridica altrui (del lavoratore o di terzi), se non quando questi abbia posto in essere una condotta dolosa ovvero sia andato incontro ad un rischio elettivo generato da un'attività non avente rapporto con lo svolgimento del lavoro o esorbitante dai limiti di esso[20];

[19] Quindi, il chiunque si "*trasforma*" di volta in volta in questo o quel soggetto, la cui posizione in quel determinato luogo di lavoro lo colloca tra quelle figure alle quali le fonti normative prevenzionali assegnano una funzione - con i correlati obblighi - di scelta, programmazione, attuazione, controllo delle diverse misure prevenzionali, legislativamente predefinite e presuntivamente ritenute idonee a prevenire l'evento infortunistico in questa o quella delle attività lavorative. La Società al fine di rendere concretamente applicabili le regole prevenzionali ha individuato, all'interno della propria organizzazione imprenditoriale, i diversi ruoli e la ripartizione organizzativa degli stessi: solo così le "posizioni di garanzia" sono nelle condizioni di adempiere agli obblighi che tale posizione aggrega a sé, e la funzione di tutela dei terzi è sostanziale, e non già un mero "parametro" di valutazione dell'eventuale responsabilità

[20] Si veda, ad esempio, Cassazione Penale, Sez. IV, sentenza n. 5005 del 10 febbraio 2010 : "*Secondo un principio assolutamente consolidato della giurisprudenza di legittimità, il datore di lavoro è responsabile anche degli*

- *elemento soggettivo*: il soggetto attivo del reato deve aver realizzato involontariamente, cioè per colpa, la morte del lavoratore. Il soggetto attivo versa in colpa quando la sua condotta violi le regole cautelari, cioè le regole che impongono comportamenti, non realizzando i quali è prevedibile che si realizzi l'evento dannoso, mentre, realizzandoli, tale evento non è prevedibile ed è evitabile. E' importante rilevare che, mentre i comportamenti doverosi sono valutati sulla base della migliore scienza per essere adeguati al progresso tecnologico (art. 18, comma 1° lett. z) del d.lgs. 81/2008), la prevedibilità dell'evento (o, per converso, la sua evitabilità) vanno valutate tenendo presente il modello di agente formato per quella stessa condizione o professione del caso di specie. Le norme cautelari scritte non esauriscono tutta la prudenza, diligenza o perizia necessarie, cosicché il giudizio negativo circa l'atteggiamento psicologico del soggetto agente può trovare fondamento anche in valutazioni generiche del dovere di sicurezza; può infatti sussistere la colpa del soggetto attivo sulla base delle comuni nozioni generali di prudenza, diligenza e perizia.

4.2.2 Lesioni gravi o gravissime aggravate

L'art. 590, comma 3, c.p. dispone: "*Chiunque cagiona ad altri, per colpa, una lesione personale (...) se il fatto è commesso con la violazione delle norme per la prevenzione degli infortuni sul lavoro è punito, per le lesioni gravi, con la reclusione da tre mesi ad un anno o con la multa ad euro 500 a euro 2.000 e per le lesioni gravissime, con la reclusione da uno a tre anni*".

Il reato in discorso si caratterizza per i seguenti elementi:

- *oggetto*: la norma tutela l'integrità fisica e fisico-psichica della persona sanzionando i comportamenti che provochino una malattia o una situazione patologica penalmente rilevante[21].
- *soggetto attivo*: il reato può essere commesso da *"chiunque"*; tuttavia, valgono anche per le lesioni colpose gravi o gravissime le considerazioni già esposte in relazione al soggetto attivo del reato di omicidio colposo (v. *supra 4.2.1)*;
- *nesso di causalità*: nessuna peculiarità presenta la causalità rispetto a quella relativa al reato di omicidio colposo delineata al precedente punto 4.2.1; anche in questa ipotesi, peraltro, il rapporto di causalità tra la condotta dell'imputato e l'evento non resta escluso per il solo fatto che tale condotta non sarebbe stata idonea a produrre l'evento stesso senza il concorso della condotta antigiuridica altrui, e in particolare del lavoratore, se non quando questi abbia posto in essere una condotta dolosa ovvero sia andato incontro ad un rischio elettivo generato da un'attività non avente rapporto con lo svolgimento del lavoro o esorbitante dai limiti di esso;
- *elemento soggettivo*: anche in questo caso nessuna peculiarità rispetto a quanto già descritto nel reato di omicidio colposo aggravato. Il soggetto attivo versa quindi in colpa quando la sua condotta violi le regole cautelari, cioè le regole che impongono comportamenti, non realizzando i quali è prevedibile che si realizzi l'evento dannoso, mentre, realizzandoli, tale evento non è prevedibile ed evitabile.

---

infortuni ascrivibili a imperizia, negligenza ed imprudenza del lavoratore, salvi i casi di assoluta abnormità del comportamento di quest'ultimo".

[21] Il Codice Penale distingue a tale proposito tra lesione personale grave e lesione personale gravissima. Si ha lesione personale grave se dal fatto deriva (i) una malattia che metta in pericolo la vita della persona offesa ovvero una malattia o una incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni oppure (ii) l'indebolimento permanente di un senso o di un organo. La lesione personale è definita gravissima se dal fatto deriva: (i) una malattia certamente o probabilmente insanabile; (ii) la perdita di un senso, o 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; oppure (iii) la deformazione, ovvero lo sfregio permanente del viso

4.3 Le sanzioni previste a carico dell'ente in materia di tutela della salute e della sicurezza sui luoghi di lavoro

L'art. 25-*septies* del Decreto prevede che per i delitti di omicidio colposo e lesioni personali colpose gravi o gravissime (*ex* artt. 589, comma 2 e 590, comma 3, c.p.) commessi in violazione delle norme sulla tutela della salute e sicurezza sul lavoro siano inflitte all'ente le seguenti sanzioni:

(i) in relazione al delitto di omicidio colposo commesso con violazione dell'art. 55, comma 2, del d.lgs. 81/2008 (ovvero in caso di omessa valutazione dei rischi ed omessa elaborazione del relativo documento nelle aziende che presentano "indici di pericolosità" importanti come, ad esempio, le aziende soggette alla normativa cosiddetta *"Seveso"*), si applicano
   - una sanzione pecuniaria in misura pari a 1000 quote (dove ciascuna quota corrisponde ad un importo variabile fra un minimo di € 258,22 ad un massimo di € 1.549,37) nonché
   - in caso di condanna, la sanzione interdittiva per una durata non inferiore a 3 mesi e non superiore ad 1 anno;

(ii) in relazione al delitto di omicidio colposo commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro (al di fuori dei casi di cui al punto (i)), si applicano
   - una sanzione pecuniaria in misura non inferiore a 250 quote e non superiore a 500 quote e
   - in caso di condanna, la sanzione interdittiva per una durata non inferiore a 3 mesi e non superiore ad 1 anno;

(iii) in relazione al delitto di lesione personale colposa grave o gravissima (art. 590, comma 3, c.p.) commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, si applicano
   - una sanzione pecuniaria in misura non superiore a 250 quote e
   - in caso di condanna, la sanzione interdittiva per una durata non superiore ad 6 mesi.

4.4 Le attività individuate come sensibili ai fini del d.lgs. 231/2001 con riferimento ai reati in materia di tutela della salute e sicurezza sul lavoro

Come già illustrato, Huawei ha considerato in concreto rilevanti le fattispecie di reato richiamate dall'art. 25-*septies* del Decreto ovvero i reati di omicidio e di lesioni personali gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro. Entrambi i reati sopra richiamati rilevano, ai fini del Decreto, unicamente nel caso in cui sia ascrivibile al soggetto agente la violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene ed alla salute sul lavoro.

Atteso che, in forza di quanto precede, assume rilevanza la legislazione prevenzionistica vigente, ai fini del presente Modello è stata considerata, in particolare, la normativa di cui al d.lgs. n. 81/2008. Ne consegue che i reati oggetto del presente Capitolo 4 possono essere commessi in tutti i casi in cui vi sia, in seno all'azienda, una violazione degli obblighi e delle prescrizioni normative in relazione ai rischi per la salute e la sicurezza dei lavoratori[22]; e che,

[22] Correttamente, quindi, per quanto attiene l'individuazione e l'analisi dei rischi potenziali, la quale dovrebbe considerare le possibili modalità attuative dei reati in discorso in seno all'azienda, le Linee Guida rilevano che l'analisi delle possibili modalità attuative non può aprioristicamente escludere alcuna delle attività e dei luoghi di lavoro in cui esse vengono ad espletarsi.

d'altro canto, ai fini della individuazione di tali rischi sono da considerarsi -in particolare ma non esaustivamente- i fattori di rischio riportati nel Documento di Valutazione Rischi (di seguito, anche "DVR"), intesi come "*attività sensibili*", e cioè come operazione il cui compimento richiede l'esecuzione di una attività nell'ambito della quale si può verificare una "*occasione di reato*".

Su tali basi, ed attenendosi, in primo luogo, alle prescrizioni fornite dall'art. 30 del d.lgs. n. 81/2008, Huawei ha proceduto a istituire, rivedere o aggiornare, a seconda della necessità:

- un sistema aziendale per l'adempimento di tutti gli obblighi giuridici in materia antinfortunistica (art. 30, comma 1) nonché per la tracciabilità degli stessi (art. 30, comma 2);
- una articolazione di funzioni volta ad assicurare le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio (art. 30, comma 3);
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello (art. 30, comma 3);
- un idoneo sistema di controllo sull'attuazione del Modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate (art. 30, comma 4).

Nel presente paragrafo saranno illustrate le attività poste in essere dalla Società della adozione di un sistema aziendale volto ad assicurare l'adempimento degli obblighi giuridici previsti dall'art. 30, comma 1, d.lgs. n. 81/2008 (paragrafo 4.5) e dell'articolazione delle funzioni adottata dalla Società ai fini della valutazione e del controllo del rischio (paragrafo 4.6). Per quanto attiene al sistema disciplinare nonché alle modalità con cui la Società ha inteso assicurare la continuità delle condizioni di idoneità del Modello si rinvia a quanto già previsto nella Parte Generale del Modello come integrato, per quanto attiene alle attività di verifica da parte dell'Organismo di Vigilanza, da quanto indicato nella premessa alla presente Parte Speciale (sezione V).

In coerenza con quanto esposto, la Società ha assunto quali "*attività sensibili*" (nel cui ambito potrebbero astrattamente essere realizzate o aver comunque causa le fattispecie di reato richiamate dall'art. 25-*septies* del Decreto), tutte le attività richiamate dall'art. 30, comma 1, del d.lgs. n. 81/2008 e così, in particolare:

1. Individuazione, valutazione e mitigazione dei rischi: si tratta dell'attività di periodica valutazione dei rischi al fine di: i) individuare i pericoli e valutare i rischi per la salute e la sicurezza dei lavoratori sui luoghi di lavoro; ii) identificare le misure in atto per la prevenzione e il controllo dei rischi e per la protezione dei lavoratori; iii) definire il piano di attuazione di eventuali nuove misure di prevenzione e protezione ritenute necessarie.
2. Rispetto degli standard tecnico – strutturali di legge: si tratta delle attività volte a garantire la conformità alla normativa tecnica propria delle attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici presenti ed utilizzati in azienda.
3. Gestione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori: si tratta delle attività relative alla attuazione e alla gestione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori, comprensiva delle attività di natura organizzativa quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza.
4. Attività di sorveglianza sanitaria: si tratta dell'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 professionale e alle modalità di svolgimento dell'attività lavorativa.
5. Attività di informazione e formazione dei lavoratori: si tratta i) della gestione di un sistema interno di diffusione delle informazioni tale da garantire a tutti i livelli aziendali un corretto approccio alle tematiche riguardanti la sicurezza e la salute dei lavoratori; nonché ii) della

gestione ed attuazione di piani sistematici di formazione e sensibilizzazione con la partecipazione periodica di tutti i dipendenti, con particolare riferimento a quei soggetti che ricoprono ruoli particolari in azienda.

6. Attività di vigilanza sull'applicazione e sul rispetto da parte dei lavoratori delle procedure e delle istruzioni operative adottate da Huawei*:* si tratta della gestione delle attività volte a verificare: i) la corretta applicazione di politiche, programmi e procedure; ii) la chiara definizione, la comprensione, la condivisione e l'operatività delle responsabilità organizzative; iii) la conformità dei prodotti e delle attività industriali alle leggi e alle norme interne; iv) l'identificazione degli eventuali scostamenti e la regolare attuazione delle relative azioni correttive; v) l'identificazione e il controllo di tutte le situazioni di rischio conoscibili.
7. Attività di acquisizione di documentazione e certificazioni obbligatorie: si tratta della gestione dell'attività volta a garantire la richiesta e raccolta della documentazione e/o delle certificazioni connesse all'esercizio dell'attività ed obbligatorie per legge.
8. Attività di periodica verifica dell'applicazione e dell'efficacia delle procedure adottate: si tratta della verifica sistematica e continua dei dati e/o indicatori che rappresentano le caratteristiche principali delle varie attività costituenti il Sistema di Gestione della Società e, conseguentemente, della verifica dell'applicazione ed efficacia delle procedure adottate.
9. Organizzazione della struttura aziendale con riferimento alle attività in tema di salute e sicurezza sul lavoro: si tratta delle attività volte a garantire una struttura organizzativa aziendale che preveda una articolazione di funzioni in grado di assicurare le competenze tecniche ed i poteri necessari per la verifica, la valutazione, la gestione ed il controllo dei rischi per la salute e la sicurezza dei lavoratori.

4.5 Il sistema dei controlli per l'adempimento degli obblighi in materia antinfortunistica

Il sistema dei controlli adottati dalla Società a presidio delle attività sensibili in materia di salute e sicurezza sui luoghi di lavoro prevede un articolato insieme di protocolli generali e protocolli specifici di seguito descritti.

Tali protocolli sono stati recepiti dalla Società nell'ambito delle procedure indicate nell'Allegato n. 5.

4.5.1 Il Sistema di Gestione HSE per la salute e sicurezza dei lavoratori

La Società è dotata del Sistema di Gestione HSE che, peraltro è stato adottato anche da diverse altre società del gruppo Huawei a livello europeo, al fine di assicurare i più elevati standard di tutela nelle aree considerate.

Tale sistema, per quanto concerne specificamente l'area della salute e della sicurezza sui luoghi di lavoro, è stato certificato in conformità ai requisiti di cui al British Standard OHSAS 18001:2007 *"Occupational Health & Safety Management System"*.

Come noto, lo standard OHSAS stabilisce i criteri per un sistema di gestione della salute e della sicurezza sul lavoro, al fine di consentire all'Organizzazione aziendale di controllare i propri rischi di igiene e sicurezza e migliorare le proprie prestazioni (OHSAS specification *"given requirements for an occupational health and safety – OH&S – management system, to enable an organization to control its OH&S risks and improve its performances"*).

Il Sistema di Gestione HSE comprende, in primo luogo, il Manuale del Sistema di Gestione HSE ("*Huawei Europe EHS Management Manual*"), il quale, oltre ad una descrizione generale dell'organizzazione aziendale e della politica interna in materia di salute e sicurezza nonché di

ambiente, dedica specifica attenzione agli argomenti della pianificazione, realizzazione e verifica del Sistema stesso, ivi compreso il riesame della direzione.

Oltre al Manuale del Sistema di Gestione HSE, la Società è dotata di un articolato insieme di procedure volte a presidiare lo svolgimento delle attività aventi un impatto, anche solo potenziale, sulla salute e la sicurezza nei luoghi di lavoro. Ulteriori documenti ed elaborati sono di volta in volta richiamati nelle procedure cui afferiscono.

Tutti i documenti che compongono il Sistema di Gestione HSE della Società sono resi disponibili, in formato cartaceo, presso la funzione Quality ed altresì, in formato elettronico, all'interno della rete intranet aziendale così da essere facilmente accessibili a tutti gli interessati.

Le procedure sono inoltre caratterizzate dall'individuazione della data di prima emissione e dalla traccia delle revisioni apportate.

Il Sistema di Gestione HSE (così come di volta in volta integrato da altri sistemi di gestione, quali ad esempio, il sistema della qualità) reca inoltre i protocolli di controllo generali e specifici utili per assicurare e, quindi, verificare che le attività sensibili ritenute rilevanti, singolarmente ed unitariamente considerate, si svolgano nel rispetto di quanto previsto dalla normativa applicabile.

4.5.2 Protocolli di controllo generali relativi alle attività sensibili

I protocolli di controllo di carattere generale da considerare e applicare con riferimento a tutte le attività sensibili relative ai reati in materia di tutela della salute e sicurezza sul lavoro sopra individuate sono:

- ***Norme/Circolari/Procedure a carattere generale o catch-all***: tali protocolli indicano i principi di comportamento e le modalità da osservare nello svolgimento delle attività aziendali, ivi comprese quelle sensibili, al fine di assicurare il rispetto della politica aziendale. Tra esse si segnala, oltre al Business Code of Conduct di Huawei, il Huawei Europe EHS Management Manual e la Politica HSE ivi richiamata (par. 02).
- ***Procedure di Registrazione ed archiviazione***: la Società assicura la trascrizione, la tracciabilità e l'archiviazione della documentazione aziendale relativa alla salute e alla sicurezza dei lavoratori, secondo il principio per cui ogni operazione deve, ove possibile, essere adeguatamente registrata. Inoltre, il processo di decisione, autorizzazione e svolgimento delle attività sensibili viene gestito in modo tale che lo stesso sia verificabile *ex post*, anche tramite appositi supporti documentali la cui compilazione, approvazione, identificazione, distribuzione, conservazione ed eliminazione viene debitamente controllata all'interno del Sistema di Gestione HSE.

4.5.3 Protocolli di controllo specifici relativi alle attività sensibili

Relativamente all'attività sensibile **n. 1 "individuazione, valutazione e mitigazione dei rischi"** (art. 30, comma 1, lett. b, d.lgs. 81/2008), con particolare riferimento all'attività di **redazione del Documento di Valutazione dei Rischi – DVR**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura che disciplini l'attività di predisposizione del Documento di Valutazione dei Rischi (di seguito anche "DVR") e preveda, fra l'altro: i) l'identificazione dei soggetti preposti; ii) le responsabilità per la verifica e l'approvazione dei contenuti dello stesso; iii) le modalità operative per la redazione del DVR (Fase preliminare - raccolta dati ed informazioni; Fase di avvio dell'analisi ed individuazione dei pericoli/rischi - verifica della conformità legislativa, individuazione dei pericoli e dei rischi ed analisi delle mansioni; Fase di valutazione dei rischi - scelta dei criteri per la valutazione

e la stima del rischio, identificazione dei lavoratori esposti e stima dell'entità delle esposizioni; Fase di pianificazione e programmazione delle misure di prevenzione e protezione); iv) le scadenze di aggiornamento del DVR.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. DVR e relativi allegati). Ai sensi di legge, il DVR può essere tenuto anche informaticamente, purché accessibile ai lavoratori e agli organi di controllo.

Relativamente all'attività sensibile **n. 2 "rispetto degli standard tecnico – strutturali di legge"** (art. 30, comma 1, lett. a, d.lgs. 81/2008), con particolare riferimento all'attività di **individuazione delle prescrizioni legali e valutazione del loro contenuto**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta ad individuare, gestire, divulgare ed archiviare le prescrizioni legislative ed i riferimenti normativi che interessano le attività svolte nell'azienda, con conseguente valutazione della conformità normativa della Società alle stesse.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. registro della normativa applicabile; check-list degli adempimenti) anche con particolare riferimento: i) alla pubblicità delle procure/deleghe (su cui vds. par. 4.6); ii) alla opportunità di messa a disposizione del pubblico dell'Opuscolo informativo; iii) alla necessità di esposizione al pubblico di alcuni documenti (ad es: planimetrie) o schede (ad es.: schede di sicurezza sostanze pericolose) secondo quanto indicato specificamente.

Relativamente all'attività sensibile **n. 2 "rispetto degli standard tecnico – strutturali di legge"** (art. 30, comma 1, lett. a, d.lgs. 81/2008), con particolare riferimento all'attività di **sorveglianza e misurazione in materia di salute e sicurezza**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta ad attuare la sorveglianza e misurare le caratteristiche di base delle attività e delle operazioni aziendali che possono avere un significativo impatto sulla sicurezza per i lavoratori, al fine di verificare e tenere monitorata la conformità al dettato normativo.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. piano di sorveglianza e misurazione).

Relativamente all'attività sensibile **n. 2 "rispetto degli standard tecnico – strutturali di legge"** (art. 30, comma 1, lett. a, d.lgs. 81/2008), con particolare riferimento all'attività di **acquisizione di impianti, attrezzature e materiali**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta ad individuare necessità e le caratteristiche degli impianti, delle attrezzature e del materiali, al fine di assicurarne l'approvvigionamento in maniera controllata e la conformità a legge e alle norme tecniche di riferimento.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata anche con particolare riferimento per quanto attiene alla documentazione a valle dell'attività di acquisto.

Relativamente all'attività sensibile **n. 2 "rispetto degli standard tecnico – strutturali di legge"** (art. 30, comma 1, lett. a, d.lgs. 81/2008), con particolare riferimento all'attività di **appalti di opere**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta ad individuare le responsabilità, le verifiche da effettuare, i documenti da richiedere ed i comportamenti da tenere allorquando vengono affidati dei lavori a ditte esterne appaltatrici o a lavoratori autonomi.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. informativa circa i rischi esistenti all'interno dei luoghi di lavoro; permesso di lavoro per le imprese esterne; modulo per la supervisione dei lavori; DUVRI; planimetria uffici).

Relativamente all'attività sensibile **n. 2 "rispetto degli standard tecnico – strutturali di legge"** (art. 30, comma 1, lett. a, d.lgs. 81/2008), con particolare riferimento all'attività di **gestione delle manutenzioni**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a definire le modalità di predisposizione ed attuazione delle attività di manutenzione e di verifica periodica degli impianti in azienda.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. libretto manutenzione impianti, strumenti e apparecchiature; libretto interventi di manutenzione ordinaria; libretto interventi manutenzione straordinaria; piano delle manutenzioni).

Relativamente all'attività sensibile **n. 2 "rispetto degli standard tecnico – strutturali di legge"** (art. 30, comma 1, lett. a, d.lgs. 81/2008), con particolare riferimento all'attività di **utilizzo DPI**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a definire gli obblighi, le competenze, le responsabilità e le modalità operative nella gestione interna nonché l'utilizzo da parte dei lavoratori dei dispositivi di protezione individuale (DPI) appropriati ai rischi inerenti alle lavorazioni ed alle operazioni effettuate.

2 Documentazione : è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. modulo di consegna DPI; istruzioni utilizzo DPI).

Relativamente all'attività sensibile **n. 2 "rispetto degli standard tecnico – strutturali di legge"** (art. 30, comma 1, lett. a, d.lgs. 81/2008), con particolare riferimento all'attività di **requisiti e controlli di accesso ai locali aziendali**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a definire le modalità operative e le annesse responsabilità per l'accoglienza dei visitatori all'interno dei locali della società.

2 Documentazione : è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. modulo informativa visitatori - emergenza).

Relativamente all'attività sensibile **n. 2 "rispetto degli standard tecnico – strutturali di legge"** (art. 30, comma 1, lett. a, d.lgs. 81/2008), con particolare riferimento all'attività di **gestione delle sostanze nocive per la salute e l'ambiente**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a regolamentare le modalità di acquisizione, redazione, verifica, aggiornamento, autorizzazione e consultazione delle schede di sicurezza relative alle sostanze pericolose, al fine di eliminare o, comunque, ridurre al minimo il rischio da esse rappresentato per le persone e per l'ambiente.

2 Documentazione : è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata con particolare riferimento per quanto attiene alle schede di sicurezza dei prodotti, che sono conservate in prossimità degli armadi o cassette ove le stesse vengono riposte.

Relativamente all'attività sensibile **n. 3 "gestione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori"** (art. 30, comma 1, lett. c, d.lgs. 81/2008), con particolare riferimento all'attività di **individuazione, preparazione e risposta alle emergenze**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a individuare le possibili emergenze ambientali e/o riguardanti la salute e sicurezza sul lavoro, predisponendo piani specifici ovvero istruzioni operative.

2 Documentazione : è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. Piano di Emergenza; programma annuale delle esercitazioni ambientali e di sicurezza; elenco delle persone addette al primo soccorso; elenco delle persone addette all'emergenza incendio; numeri telefonici di emergenza; opuscolo informativo; modulo verbale prova di evacuazione; contenuto minimo della cassetta di pronto soccorso; controllo degli impianti e delle attrezzature antincendio nonché l'Opuscolo Informativo che è messo a disposizione anche dei visitatori).

Relativamente all'attività sensibile **n. 3 "gestione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori"** (art. 30, comma 1, lett. c, d.lgs. 81/2008), con particolare riferimento all'attività di **redazione e implementazione Piano di Emergenza,** i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a stabilire i comportamenti che debbono tenere tutte le persone che svolgono attività lavorativa di qualsiasi genere, per quanto di loro competenza, in caso di situazioni di emergenza o di pericolo, che possono verificarsi all'interno dei locali aziendali. In particolare, tale protocollo di controllo specifico mira a perseguire i seguenti obiettivi: i) affrontare l'emergenza fin dal primo insorgere per contenere gli effetti e riportare rapidamente la situazione in condizioni di normale esercizio; ii) pianificare le azioni necessarie per proteggere le persone sia all'interno che all'esterno; iii) prevenire o limitare i danni all'ambiente; iv) coordinare i servizi di emergenza, lo staff tecnico e la direzione aziendale.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (Piano di Emergenza, e, eventualmente in allegato allo stesso: i) addetti squadre di emergenza; ii) planimetria; iii) numeri telefonici di emergenza; iv) piano di evacuazione; v) planimetrie degli estintori; vi) opuscolo informativo in caso di emergenza).

Relativamente all'attività sensibile **n. 3 "gestione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori"** (art. 30, comma 1, lett. c, d.lgs. 81/2008), con particolare riferimento all'attività di **gestione comunicazioni ambientali e sulla sicurezza**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a definire come debbono essere gestite le comunicazioni, sia interne che esterne, in materia ambientale e di salute e sicurezza sul lavoro, in ordine a: i) attività; ii) prodotti e servizi; iii) politiche; iv) obiettivi e traguardi; v) programmi ambientali e di sicurezza; vi) performance.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. verbale di consultazione ed informazione RLS; verbale delle riunioni periodiche).

Relativamente all'attività sensibile **n. 4 "attività di sorveglianza sanitaria"** (art. 30, comma 1, lett. d, d.lgs. 81/2008), con particolare riferimento all'attività di **sorveglianza sanitaria**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a definire compiti e responsabilità dei soggetti coinvolti nello svolgimento dell'attività di sorveglianza sanitaria.

2 Documentazione : è assicurata la puntuale ed integrale registrazione nonché l'archiviazione della documentazione sanitaria inerente i lavoratori (ad es. atto di nomina del medico competente; verbale della visita annuale degli ambienti di lavoro; protocollo sorveglianza sanitaria; comunicazione dei risultati anonimi e collettivi della sorveglianza sanitaria effettuata al datore di lavoro, al RSPP e al rappresentante dei lavoratori per la sicurezza in occasione della riunione annuale ex art. 35; verbali di consegna della documentazione sanitaria e della copia della cartella sanitaria e di rischio. Eventualmente: accordo con centro per l'effettuazione delle analisi e delle visite specialistiche identificate dal medico competente nell'ambito delle attività di sorveglianza sanitari; documentazione distribuita ai lavoratori per renderli edotti dei rischi). Tali attività devono avvenire nel rispetto delle modalità previste dall'art. 25, comma 1, lett. e) del d.lgs. 81/08 e dal d.lgs. 196/03.

Relativamente all'attività sensibile n. **5** "**attività di informazione e formazione dei lavoratori**" (art. 30, comma 1, lett. e, d.lgs. 81/2008), con particolare riferimento all'attività di **formazione ed informazione**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a garantire una razionalizzazione ed uniformità della formazione e dell'addestramento del personale nonché una metodologia per: a) definire le competenze delle funzioni del Sistema di Gestione e delle mansioni il cui svolgimento possa determinare un impatto significativo sulla salute e sicurezza; b) fornire agli addetti una adeguata formazione, informazione e sensibilizzazione; c) valutare l'apprendimento e l'efficacia della formazione erogata. La procedura deve tra l'altro prevedere: i) l'individuazione dei profili professionali di riferimento; ii) l'individuazione delle necessità formative degli addetti a tali funzioni e mansioni (es.: assunzione, trasferimento o cambiamento di mansioni, insorgenza di nuovi rischi etc.); iii) la progettazione e l'attuazione di corsi di formazione che soddisfino tali necessità formative; iv) la verifica dell'efficacia dei corsi di formazione e l'individuazione delle necessità di mantenimento; v) la registrazione e l'archiviazione dell'attività formativa.

2 Documentazione : è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. manuale informativo norme e comportamenti; manuale "training on the job"; matrice addetti/corsi; modulo formazione dirigenti/preposti interno; modulo presenze corsi di formazione interni; modulo verifica apprendimento; questionario gradimento corso interno; modulo informativa corsi esterni; modulo richiesta corsi esterni).

Relativamente all'attività sensibile n. **6 "attività di vigilanza sull'applicazione e sul rispetto da parte dei lavoratori delle procedure e delle istruzioni operative adottate da Huawei"** (art. 30, comma 1, lett. f, d.lgs. 81/2008) , con particolare riferimento all'attività di **rilevazione e gestione delle non conformità, azioni correttive e preventive**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta ad indicare in modo dettagliato quali sono le modalità con cui debbono essere gestite le azioni correttive e/o preventive adottate per sanare eventuali carenze reali o potenziali, anche a livello di Sistema di Gestione HSE, individuando ruoli e responsabilità.

2 Documentazione : è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. rilevazione non conformità; indicazione azioni correttive).

Relativamente all'attività sensibile n. **6 "attività di vigilanza sull'applicazione e sul rispetto da parte dei lavoratori delle procedure e delle istruzioni operative adottate da Huawei"** (art. 30, comma 1, lett. f, d.lgs. 81/2008), con particolare riferimento all'attività di **indagine sugli infortuni**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta ad individuare una metodologia volta ad: i) analizzare le cause di un infortunio o quasi infortunio; ii) raccogliere gli elementi necessari alla ricostruzione della dinamica dell'evento; iii) individuare ed attuare le azioni correttive atte ad impedire il ripetersi di tali eventi.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. rapporto di infortunio; rapportino di medicazione). In particolare, si richiama l'attenzione sul fatto che la documentazione interna può avere rilevanza nell'ambito delle indagini condotte dall'autorità e necessita quindi di particolare attenzione sia in sede di compilazione e sia di archiviazione.

Relativamente all'attività sensibile all'attività sensibile n. **7 "attività di acquisizione di documentazione e certificazioni obbligatorie"** (art. 30, comma 1, lett. g, d.lgs. 81/2008), con particolare riferimento all'attività di **documentazione e certificazione**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta a stabilire le modalità di individuazione, gestione, aggiornamento, divulgazione ed archiviazione della documentazione relativa alle materie della salute e della sicurezza sui luoghi di lavoro nonché alle certificazioni obbligatorie ai sensi della legge vigente, ivi incluse le prescrizioni legislative applicabili.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. informativa circa i rischi esistenti all'interno dei luoghi di lavoro; permesso di lavoro per le imprese esterne; modulo per la

supervisione dei lavori; DUVRI; planimetria uffici).

Relativamente all'attività sensibile n. **8 "attività di periodica verifica dell'applicazione e dell'efficacia delle procedure adottate"** (art. 30, comma 1, lett. h, d.lgs. 81/2008), con particolare riferimento all'attività di **riesame della qualità**, i protocolli specifici sono i seguenti:

1 Procedura: formalizzazione di una procedura volta ad individuare i soggetti responsabili oltre che le modalità di esecuzione del Riesame della direzione aziendale, in particolare modo per quanto concerne l'elaborazione di un documento nel quale la Società prende in considerazione i seguenti elementi: i) i risultati della valutazione dei rischi; ii) le opzioni tecnologiche possibili; iii) le esigenze finanziarie; iv) le esigenze operative; v) i punti di vista delle parti interessate e dei dipendenti; vi) i risultati del riesame della direzione in materia di salute e sicurezza nei luoghi di lavoro. Il programma di miglioramento che ne consegue, oltre a definire le attività attraverso le quali raggiungere gli obiettivi ed i traguardi previsti, viene a definire anche chi sono i soggetti responsabili e quali le tempistiche.

2 Documentazione: è assicurata la puntuale ed integrale registrazione nonché l'archiviazione dei documenti relativi alla procedura indicata (ad es. rapporto e programma di miglioramento della sicurezza).

Relativamente all'attività sensibile n. **9 "organizzazione della struttura aziendale con riferimento alle attività in tema di salute e sicurezza sul lavoro"** (art. 30, comma 1, lett. h, d.lgs. 81/2008), le scelte organizzative di Huawei, ivi compresa la definizione del c.d. "*organigramma della sicurezza*", attesa la loro particolare importanza e complessità, sono descritte separatamente al successivo paragrafo 4.6.

4.6 L'Assetto Organizzativo e la delega di funzioni

L'assetto organizzativo di Huawei ha consentito l'accentramento dei poteri e dei correlativi doveri in materia di salute e sicurezza sul lavoro in capo al datore di lavoro.

Al momento non sono dunque state formalizzate specifiche deleghe di funzioni[23].

Nell'ambito delle attività sensibili, un ruolo preminente è svolto da quelle che sono le funzioni aziendali di cui si riporta di seguito la definizione normativa.

- **Datore di lavoro**: definito dall'art. 2 comma 1 lett. b) del d.lgs. 81/2008 come *"il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il*

[23] La delega di funzioni è quell'istituto normativamente previsto dalla normativa prevenzionistica che ricorre allorquando, mediante un atto di incarico o delega, viene costituita in capo al delegato una nuova posizione di garanzia, con il conseguente ritrarsi della sfera di competenza del delegante (datore di lavoro).
In linea con la costante giurisprudenza sull'argomento e con l'art. 16 sopra richiamato, la Società conferisce delega di funzioni in materia di salute e sicurezza nei luoghi di lavoro nel rispetto dei seguenti limiti e condizioni:
a) che essa risulti da atto scritto, recante data certa (lett. a);
b) che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate (lett. b);
c) che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate (lett. c);
d) che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate (lett. d);
e) che la delega sia accettata dal delegato per iscritto (lett. e).
Rimane - comunque - fermo il dovere di vigilanza sull'attività del delegato da parte del delegante, che viene esercitato attraverso la predisposizione ed efficace attuazione dei sistemi di verifica e controllo (art. 16, comma 3, d.lgs. 81/2008).

tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unità produttiva in quanto esercita i poteri decisionali e di spesa";

- **Delegato funzionale in materia di salute e sicurezza sul lavoro**: è il soggetto che, per i suoi requisiti di professionalità ed esperienza, viene delegato dal datore di lavoro – con apposito atto scritto recante data certa - a svolgere gli obblighi su di lui ricadenti in materia di salute e sicurezza nei luoghi di lavoro, ad eccezione di quelle che sono le funzioni indelegabili di cui all'art. 17 del d.lgs. 81/2008 (valutazione del rischio ed elaborazione del relativo documento nonché nomina del Responsabile del Servizio di Prevenzione e Protezione);
- **Dirigente**: definito dall'art. 2, comma 1 lett. d) del d.lgs. 81/2008 come la *"persona che, in ragione delle competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, attua le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando su di essa"*;
- **Preposto**: definito dall'art. 2, comma 1 lett. e) del d.lgs. 81/2008 come la *"persona che, in ragione delle competenze professionali e nei limiti dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende alla attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa"*;
- **Lavoratore**: definito dall'art. 2, comma 1, lett. a) del d.lgs. 81/2008 come la *"persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione di un datore di lavoro pubblico o privato, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione"*;
- **Responsabile del Servizio di Prevenzione e protezione (di seguito anche *"RSPP"*)**: definito dall'art. 2, comma 1 lett. f) del d.lgs. 81/2008 come la *"persona in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 del d.lgs. 81/2008, designata dal datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi della Società"*;
- **Addetto al Servizio di Prevenzione e protezione (di seguito anche *"ASPP"*)**: definito dall'art. 2, comma 1, lett. g) del d.lgs. 81/2008 come la *"persona in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 del d.lgs. 81/2008, facente parte del servizio di prevenzione e protezione dai rischi della Società"*;
- **Addetto alla gestione delle emergenze**: lavoratore designato dal datore di lavoro con apposito atto scritto, da lui accettato, e chiamato a gestire le situazioni di emergenza reali e potenziali in azienda;
- **Medico competente**: definito dall'art. 2, comma 1, lett. h) del d.lgs. 81/2008 come quel medico che è *"in possesso di uno dei titoli e dei requisiti formativi e professionali di cui all'articolo 38 del d.lgs. 81/2008, che collabora con il datore di lavoro ai fini della valutazione dei rischi ed è nominato dallo stesso per effettuare la sorveglianza sanitaria e per tutti gli altri compiti previsti dal d.lgs. 81/2008"*;
- **Rappresentante dei lavoratori per la sicurezza (di seguito anche *"RLS"*)**: definito dall'art. 2, comma 1, lett. l) del d.lgs. 81/2008 come la *"persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro"*;
- **Responsabile del Sistema di Gestione HSE**: è la persona che è stata nominata quale Responsabile per il Sistema di Gestione HSE della Società, con il compito di assicurare che lo stesso venga introdotto ed applicato, secondo i requisiti previsti, in tutti i luoghi ed in tutti gli ambiti operativi all'interno dell'organizzazione stessa, riferendone alla direzione ed

al datore di lavoro.

L'attuale assetto organizzativo di Huawei è strutturato secondo lo schema dell'organigramma allegato alla Parte Generale del Modello. Il complesso della documentazione sopra indicata è tenuto e aggiornato a cura della funzione HR.

I ruoli, i compiti e le responsabilità in materia prevenzionistica delle diverse funzioni aziendali sono comunicati ai soggetti responsabili mediante apposita formalizzazione dei rispettivi incarichi e documentati.

4.7 Gli obblighi di informativa all'Organismo di Vigilanza in materia di salute e sicurezza sul lavoro

Tutti i Destinatari del Modello, ivi incluse le funzioni aziendali di cui al precedente paragrafo 4.6 e i terzi destinatari di cui al successivo paragrafo 4.8, sono tenuti a rispettare gli obblighi di informazione all'Organismo di Vigilanza di Huawei secondo quanto indicato nel Capitolo 3 della Parte Generale di questo Modello con riferimento a qualsiasi non conformità, potenziale o attuale, in materia di salute e sicurezza sul lavoro.

Il datore di lavoro e gli eventuali delegati funzionali che dovessero essere nominati, per quanto di competenza, anche con il supporto dell'RSPP, assicurano l'adempimento di tali obblighi presso l'Organismo di Huawei.

4.8 I Terzi Destinatari

Occorre da ultimo precisare che in materia di salute e sicurezza sul lavoro assume particolare rilevanza la posizione di quei soggetti che, pur essendo esterni rispetto alla struttura organizzativa della Società, svolgono un'attività potenzialmente incidente sulla salute e la sicurezza dei lavoratori.

In questo ambito, devono pertanto considerarsi Terzi Destinatari:

a) i soggetti cui è affidato un lavoro in virtù di contratto d'appalto o d'opera o di somministrazione;

b) i fabbricanti ed i fornitori;

c) i progettisti dei luoghi, posti di lavoro ed impianti;

d) gli installatori ed i montatori di impianti, attrezzature di lavoro o altri mezzi tecnici.

In particolare, la Società ha predisposto adeguate procedure al fine di assicurare che i Terzi Destinatari:

- garantiscano la propria idoneità tecnico professionale in relazione ai lavori da eseguire in appalto o mediante contratto d'opera o di somministrazione;
- recepiscano le informazioni fornite dalla Società circa i rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate dal datore di lavoro;
- cooperino per l'attuazione delle misure di prevenzione e protezione dai rischi sul lavoro incidenti sull'attività lavorativa oggetto di contratto di appalto o d'opera o di somministrazione;
- coordinino gli interventi di protezione e prevenzione dai rischi cui sono esposti i lavoratori.

CAPITOLO 5
I REATI AMBIENTALI

Premessa

Con la pubblicazione del d.lgs. 7 luglio 2011, n. 121 (nel prosieguo, "d.lgs. 121/2011") si è concluso l'*iter* legislativo che ha portato alla inclusione nel d.lgs. 231/2001 di un nuovo articolo, il 25-*undecies*, il quale estende l'ambito dei c.d. "reati presupposto" a un numero rilevante di fattispecie di reato genericamente etichettabili come "reati ambientali" e previsti specificamente:

(i) nel Codice Penale:

- all'art. 727-*bis*;
- all'art. 733-*bis;*

(ii) nel Decreto Legislativo 3 aprile 2006, n.152, e successive modificazioni ed integrazioni, recante "*norme in materia ambientale*" (nel prosieguo, "d.lgs. 152/2006"):

- all'art. 137, commi 2, 3, 5, primo e secondo periodo, 11 e 13;
- all'art. 256, commi 1, lettere a) e b), 3, primo e secondo periodo, 4, 5 e 6, primo periodo;
- all'art. 257, commi 1 e 2;
- all'art. 258, comma 4, secondo periodo;
- all'art. 259, comma 1;
- all'art. 260, commi 1 e 2;
- all'art. 260-*bis*, commi 6, 7, secondo e terzo periodo, e 8, primo e secondo periodo;
- all'art. 279, comma 5;

(iii) nella Legge 7 febbraio 1992, n. 150, e successive modificazioni ed integrazioni, recante "*disciplina dei reati relativi all'applicazione in Italia della convenzione sul commercio internazionale delle specie animali e vegetali in via di estinzione, firmata a Washington il 3 marzo 1973, di cui alla legge 19 dicembre 1975, n. 874, e del regolamento (CEE) n. 3626/82, e successive modificazioni, nonché norme per la commercializzazione e la detenzione di esemplari vivi di mammiferi e rettili che possono costituire pericolo per la salute e l'incolumità pubblica*" (nel prosieguo, "L. 150/1992"):

- all'art. 1, commi 1 e 2;
- all'art. 2, commi 1 e 2;
- all'art. 6, comma 4;
- all'art. 3-*bis*, comma 1 ovvero ai reati del Codice Penale ivi richiamati;

(iv) nella Legge 28 dicembre 1993, n. 549, e successive modificazioni ed integrazioni, recante "*misure a tutela dell'ozono stratosferico e dell'ambiente*" (nel prosieguo, "L. 540/1993"):

- all'art. 3, comma 6;

(v) nel Decreto Legislativo 6 novembre 2007, n. 202, e successive modificazioni ed integrazioni, recante "*attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni*" (nel prosieguo, "d.lgs. 202/2007"):

- all'art. 8, commi 1 e 2;
- all'art. 9, commi 1 e 2.

La Società ha considerato come potenzialmente rilevanti per essa le fattispecie di reato previste dall'art. 25-*undecies* del Decreto e ha proceduto alla elaborazione del presente Capitolo 5, nel quale vengono:

(i) descritte le fattispecie di reato previste dall'art. 25-*undecies* del Decreto (paragrafo 5.1);
(ii) individuate le attività poste in essere dalla Società nel cui ambito potrebbero astrattamente esser realizzate le fattispecie di reato richiamate dall'art. 25-*undecies* del d.lgs. 231/2001 (paragrafo 5.3);
(iii) per ciascuna di tali attività, identificati i presidi finalizzati alla prevenzione del rischio di commissione dello specifico reato presupposto (paragrafo 5.4).

5.1 I reati ambientali dall'art. 25-*undecies* del d.lgs. 231/2001

Ai sensi dell'art. 2 del d.lgs. 121/2011, recante "*attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni*", la responsabilità amministrativa degli enti è stata estesa ai reati ambientali attraverso l'introduzione dell'art. 25-*undecies* del d.lgs. 231/2001.

La punibilità di tali reati, tra cui si annoverano delitti e contravvenzioni, è prevista, a seconda dei casi concreti, anche a semplice titolo di colpa oltre che di dolo.

È dunque bene premettere che, ai sensi dell'art. 43, comma 1, c.p., un reato:

- è doloso, o secondo l'intenzione, quando l'evento dannoso o pericoloso, che è il risultato dell'azione od omissione e da cui la legge fa dipendere l'esistenza del delitto, è dall'agente preveduto e voluto come conseguenza della propria azione od omissione;
- è colposo, o contro l'intenzione, quando l'evento, anche se preveduto, non è voluto dall'agente e si verifica a causa di negligenza o imprudenza o imperizia, ovvero per inosservanza di leggi, regolamenti, ordini o discipline.

Si rende dunque necessario passare in rassegna ciascuno dei reati ambientali di cui sopra, riservando l'analisi delle relative sanzioni al successivo paragrafo 5.2.

5.1.1 Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette

L'art. 727-*bis* c.p. recita: "*1. Salvo che il fatto costituisca più grave reato, chiunque, fuori dai casi consentiti, uccide, cattura o detiene esemplari appartenenti ad una specie animale selvatica protetta è punito con l'arresto da uno a sei mesi o con l'ammenda fino a 4. 000 euro, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie.*

2. Chiunque, fuori dai casi consentiti, distrugge, preleva o detiene esemplari appartenenti ad una specie vegetale selvatica protetta è punito con l'ammenda fino a 4. 000 euro, salvo i casi in cui l'azione riguardi una quantità trascurabile di tali esemplari e abbia un impatto trascurabile sullo stato di conservazione della specie".

Le principali caratteristiche della fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: la norma è stata emanata in attuazione di quanto previsto dalla Direttiva 2008/99/CE del 19 novembre 2008 "*sulla tutela penale dell'ambiente*". Essa si prefigge di

tutelare l'ambiente ed, in particolare, le specie animali e vegetali selvatiche protette così come definite dall'art. 1, comma 2, del d.lgs. 121/2011, secondo cui "*ai fini dell'applicazione dell'articolo 727-bis del codice penale, per specie animali o vegetali selvatiche protette si intendono quelle indicate nell'allegato IV della direttiva 92/43/CE* [c.d. "Direttiva Habitat"; n.d.r.] *e nell'allegato I della direttiva 2009/147/CE* [c.d. "Direttiva Uccelli"; N.d.r.]."[24]. Tra le specie protette ve ne sono numerose appartenenti ai generi dei mammiferi, dei pesci, dei cetacei e dei rettili nonché numerose specie della flora selvatica, a prescindere dal fatto che si tratti di specie rare o in via di estinzione. La condotta penalmente rilevante ha ad oggetto una quantità non trascurabile di esemplari tale da esporre la specie ad un pericolo o ad un danno. Le condotte descritte sono punibili "*fuori dai casi consentiti*" con conseguente esclusione della punibilità in tutti i casi in cui le condotte medesime siano riconducibili all'applicazione di disposizioni di legge[25];

- *soggetto attivo*: alla stregua di quanto previsto dalla lettera dell'art. 727-bis c.p., trattasi di reato comune in quanto suscettibile di commissione da parte di qualunque soggetto (i.e. "chiunque");
- *elemento soggettivo*: il reato è punibile sia a titolo di dolo sia a titolo di colpa. Il soggetto attivo versa in colpa quando la sua condotta violi le regole cautelari, cioè le regole che impongono comportamenti, non realizzando i quali è prevedibile che si realizzi l'evento dannoso, mentre, realizzandoli, tale evento non è prevedibile ed è evitabile. Tuttavia, la presenza della clausola di riserva "*salvo che il fatto non costituisca più grave reato*" fa prevalere fattispecie interferenti punite più severamente (quale, ad esempio, l'ipotesi del c.d. "furto venatorio", laddove è pacifico che la fauna selvatica resta pur sempre patrimonio indisponibile dello Stato), con la conseguenza che l'ambito concreto di applicazione della norma si presta ad essere ridotto a casi quale, ad esempio, l'uccisione colposa di animali fuori dell'ambito della caccia.

5.1.2 Distruzione o deterioramento di habitat all'interno di un sito protetto

L'art. 733-*bis* c.p. recita: "*1. Chiunque, fuori dai casi consentiti, distrugge un habitat all'interno di un sito protetto o comunque lo deteriora compromettendone lo stato di conservazione, è punito con l'arresto fino a diciotto mesi e con l'ammenda non inferiore a 3.000 euro*".

Il reato in discorso si caratterizza per i seguenti elementi:

- *oggetto*: al pari dell'art. 727-*bis* c.p., anche la norma ora in commento è stata emanata in attuazione della Direttiva 2008/99/CE del 19 novembre 2008 "*sulla tutela penale dell'ambiente*". Essa tutela, in particolare, gli habitat posti all'interno di siti protetti così come definiti dall'art. 1, comma 3, del d.lgs. 121/2011, secondo cui "*ai fini dell'applicazione dell'articolo 733-bis del codice penale per 'habitat all'interno di un sito protetto' si intende qualsiasi habitat di specie per le quali una zona sia classificata come*

[24] Le Direttive Habitat ed Uccelli hanno istituito speciali aree protette comprese in una rete ecologica denominata "Natura 2000" e principalmente costituite da: Zone Speciali di Conservazione ("ZSC"), Zone di Protezione Speciale ("ZPS") e Siti di Interesse Comunitario ("SIC"). L'individuazione di tali zone sul territorio nazionale è definita con decreto del Ministero dell'Ambiente.

[25] Vedasi, al riguardo, la "*Relazione dell'ufficio del massimario presso la Corte Suprema di Cassazione*" n. III/09/2011, dell'agosto 2011, di Luca Pistorelli e Alessio Scarcella, la quale menziona tra le varie esclusioni, le deroghe previste dall'art. 16 della direttiva 92/43/CE e precisamente: a) per proteggere la fauna e la flora selvatiche e conservare gli habitat naturali; b) per prevenire gravi danni, segnatamente alle colture, all'allevamento, ai boschi, al patrimonio ittico e alle acque e ad altre forme di proprietà; c) nell'interesse della sanità e della sicurezza pubblica o per altri motivi imperativi di rilevante interesse pubblico, inclusi motivi di natura sociale o economica, e motivi tali da comportare conseguenze positive di primaria importanza per l'ambiente; d) per finalità didattiche e di ricerca, di ripopolamento e di reintroduzione di tali specie e per operazioni di riproduzione necessarie a tal fine, compresa la riproduzione artificiale delle piante; e) per consentire, in condizioni rigorosamente controllate, su base selettiva ed in misura limitata, la cattura o la detenzione di un numero limitato di taluni esemplari delle specie di cui all'allegato IV, specificato dalle autorità nazionali competenti.

zona a tutela speciale a norma dell'articolo 4, paragrafi 1 o 2, della direttiva 2009/147/CE [c.d. "Direttiva Uccelli"; N.d.r.]*, o qualsiasi habitat naturale o un habitat di specie per cui un sito sia designato come zona speciale di conservazione a norma dell'art. 4, paragrafo 4, della direttiva 92/43/CE* [c.d. "Direttiva Habitat"; N.d.r.]*."*. La fattispecie in esame punisce sia la distruzione[26] sia il semplice deterioramento dell'habitat compromettendone lo stato di conservazione[27].

- *soggetto attivo*: il reato può essere commesso da *"chiunque"*, al pari del reato di cui all'art. 727-*bis* c.p. (v. *supra 5.1.1.*);
- *elemento soggettivo*: anche in questo caso la norma non presenta alcuna peculiarità rispetto a quanto già descritto nel reato di cui all'art. 727-*bis* c.p. (v. *supra 5.1.1.*).

5.1.3 Reati in materia di scarichi

L'art. 25-*undecies*, comma 2, lettera a), del Decreto contempla i reati di cui all'art. 137, commi 2, 3, 5, primo e secondo periodo, 11 e 13 del d.lgs. 152/2006 in tema di scarichi di acque reflue industriali.

Deve intendersi come "*scarico*", ai sensi dell'art. 74, comma 1, lett. ff) del d.lgs. 152/2006, "*qualsiasi immissione effettuata esclusivamente tramite un sistema stabile di collettamento che collega senza soluzione di continuità il ciclo di produzione del refluo con il corpo ricettore acque superficiali, sul suolo, nel sottosuolo e in rete fognaria, indipendentemente dalla loro natura inquinante, anche sottoposte a preventivo trattamento di depurazione. Sono esclusi i rilasci di acque previsti all'articolo 114*[28]".

Le "*acque reflue industriali*" sono invece definite dall'art. 74, comma 1, lett. h) del d.lgs. 152/2006 come "*qualsiasi tipo di acque reflue scaricate da edifici od impianti in cui si svolgono attività commerciali o di produzione di beni, diverse dalle acque reflue domestiche*[29] *e dalle acque meteoriche di dilavamento*".

Esiste un orientamento giurisprudenziale univoco e confermato anche da una recente sentenza della Corte di Cassazione del 2011 (Cass. pen., sez. III, 6 luglio 2011, n. 36979) che ritiene qualificabili come "acque reflue industriali" le acque meteoriche che, cadendo su luoghi aziendali[30] in cui si verifica il deposito di sostanze in forma solida (es. polveri) o liquida (es. oli), defluiscano nei vari corpi recettori[31] (Cass. pen., sez. III., 11 ottobre 2007, n. 40191; P. Fimiani, *La tutela penale dell'ambiente*, Giuffrè, 2011, p. 123). Alle volte sono le stesse normative Regionali a qualificare le acque meteoriche di dilavamento come acque reflue industriali in presenza di certi requisiti.

---

[26] Si avrà distruzione quando l'habitat sia completamente soppresso (v. "*Relazione dell'ufficio del massimario presso la Corte Suprema di Cassazione*" cit.; pag. 21).

[27] Rispetto all'ipotesi di distruzione, risulta più complicato individuare quando possa ritenersi integrata la fattispecie in presenza di una condotta di deterioramento dell'habitat che ne comprometta lo stato di conservazione. Un'utile indicazione in proposito può senz'altro provenire dalla giurisprudenza formatasi a proposito del delitto di danneggiamento (art. 635 c.p.), reato che include tra le condotte in cui può alternativamente oggettivarsi l'azione proprio quella di "*deteriorare*" cose mobili od immobili. In tal senso, si è affermato che si ha "*deterioramento*" tutte le volte in cui una cosa venga resa inservibile, anche solo temporaneamente, all'uso cui è destinata, non rilevando, ai fini dell'integrazione della fattispecie, la possibilità di reversione del danno, anche se tale reversione avvenga non per opera dell'uomo, ma per la capacità della cosa di riacquistare la sua funzionalità nel tempo (v. "*Relazione dell'ufficio del massimario presso la Corte Suprema di Cassazione*" cit.; pag. 61; quest'ultima richiama espressamente Cass. Sez. IV, n. 9343 del 21 ottobre 2010, dep. 9 marzo 2011, V., rv 249808).

[28] L'art. 114 del d.lgs. 152/2006 reca la disciplina in tema di dighe.

[29] Ai sensi dall'art. 74, comma 1, lett. g) del d.lgs. 152/2006, le "*acque reflue domestiche*" sono quelle "*acque reflue provenienti da insediamenti di tipo residenziale e da servizi e derivanti prevalentemente dal metabolismo umano e da attività domestiche*".

[30] Piazzali, cisterne, vasche.

[31] Suolo, sottosuolo, acque superficiali, fognatura.

L'art. 137 del d.lgs. 152/2006, per quanto qui rileva, dispone che: *"1. Chiunque apra o comunque effettui nuovi scarichi di acque reflue industriali, senza autorizzazione, oppure continui ad effettuare o mantenere detti scarichi dopo che l'autorizzazione sia stata sospesa o revocata, è punito con l'arresto da due mesi a due anni o con l'ammenda da millecinquecento euro a diecimila euro.*

2. Quando le condotte descritte al comma 1 riguardano gli scarichi di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto, la pena è dell'arresto da tre mesi a tre anni.

3. Chiunque, al di fuori delle ipotesi di cui al comma 5, effettui uno scarico di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del presente decreto senza osservare le prescrizioni dell'autorizzazione, o le altre prescrizioni dell'autorità competente a norma degli articoli 107, comma 1, e 108, comma 4, è punito con l'arresto fino a due anni. (omissis…)

5. Chiunque, in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza del presente decreto, nell'effettuazione di uno scarico di acque reflue industriali, superi i valori limite fissati nella tabella 3 o, nel caso di scarico sul suolo, nella tabella 4 dell'Allegato 5 alla parte terza del presente decreto, oppure i limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente a norma dell'articolo 107, comma 1, è punito con l'arresto fino a due anni e con l'ammenda da tremila euro a trentamila euro. Se sono superati anche i valori limite fissati per le sostanze contenute nella tabella 3/A del medesimo Allegato 5, si applica l'arresto da sei mesi a tre anni e l'ammenda da seimila euro a centoventimila euro. (omissis…)

11. Chiunque non osservi i divieti di scarico previsti dagli articoli 103 e articolo 104 è punito con l'arresto sino a tre anni. (omissis…)

13. Si applica sempre la pena dell'arresto da due mesi a due anni se lo scarico nelle acque del mare da parte di navi od aeromobili contiene sostanze o materiali per i quali è imposto il divieto assoluto di sversamento ai sensi delle disposizioni contenute nelle convenzioni internazionali vigenti in materia e ratificate dall'Italia, salvo che siano in quantità tali da essere resi rapidamente innocui dai processi fisici, chimici e biologici, che si verificano naturalmente in mare e purché in presenza di preventiva autorizzazione da parte dell'autorità competente. (omissis…)".

Per assicurare la massima comprensione del contenuto dell'art. 137 del d.lgs. 152/2006 di cui sopra, si riportano qui di seguito gli ulteriori articoli citati dalla norma in esame.

Ai sensi dell'art. 103 del d.lgs. 152/2006 ("*Scarichi sul suolo*"): "*1. È vietato lo scarico sul suolo o negli strati superficiali del sottosuolo, fatta eccezione:*

a) per i casi previsti dall'articolo 100, comma 3;

b) per gli scaricatori di piena a servizio delle reti fognarie;

c) per gli scarichi di acque reflue urbane e industriali per i quali sia accertata l'impossibilità tecnica o l'eccessiva onerosità, a fronte dei benefici ambientali conseguibili, a recapitare in corpi idrici superficiali, purché gli stessi siano conformi ai criteri ed ai valori-limite di emissione fissati a tal fine dalle regioni ai sensi dell'articolo 101, comma 2. Sino all'emanazione di nuove norme regionali si applicano i valori limite di emissione della Tabella 4 dell'Allegato 5 alla parte terza del presente decreto;

d) per gli scarichi di acque provenienti dalla lavorazione di rocce naturali nonché dagli impianti di lavaggio delle sostanze minerali, purché i relativi fanghi siano costituiti esclusivamente da acqua e inerti naturali e non comportino danneggiamento delle falde acquifere o instabilità dei suoli;

e) per gli scarichi di acque meteoriche convogliate in reti fognarie separate;

f) per le acque derivanti dallo sfioro dei serbatoi idrici, dalle operazioni di manutenzione delle reti idropotabili e dalla manutenzione dei pozzi di acquedotto.

2. Al di fuori delle ipotesi previste al comma 1, gli scarichi sul suolo esistenti devono essere convogliati in corpi idrici superficiali, in reti fognarie ovvero destinati al riutilizzo in conformità alle prescrizioni fissate con il decreto di cui all'articolo 99, comma 1. In caso di mancata ottemperanza agli obblighi indicati, l'autorizzazione allo scarico si considera a tutti gli effetti revocata.

3. Gli scarichi di cui alla lettera c) del comma 1 devono essere conformi ai limiti della Tabella 4 dell'Allegato 5 alla parte terza del presente decreto. Resta comunque fermo il divieto di scarico sul suolo delle sostanze indicate al punto 2.1 dell'Allegato 5 alla parte terza del presente decreto."

Ai sensi del successivo art. 104 del d.lgs. 152/2006 ("*Scarichi nel sottosuolo e nelle acque sotterranee*"): "*1. È vietato lo scarico diretto nelle acque sotterranee e nel sottosuolo.*

2. In deroga a quanto previsto al comma 1, l'autorità competente, dopo indagine preventiva, può autorizzare gli scarichi nella stessa falda delle acque utilizzate per scopi geotermici, delle acque di infiltrazione di miniere o cave o delle acque pompate nel corso di determinati lavori di ingegneria civile, ivi comprese quelle degli impianti di scambio termico.

3. In deroga a quanto previsto al comma 1, per i giacimenti a mare, il Ministero dell'ambiente e della tutela del territorio e del mare, d'intesa con il Ministero dello sviluppo economico e, per i giacimenti a terra, ferme restando le competenze del Ministero dello sviluppo economico in materia di ricerca e coltivazione di idrocarburi liquidi e gassosi, le regioni possono autorizzare lo scarico di acque risultanti dall'estrazione di idrocarburi nelle unità geologiche profonde da cui gli stessi idrocarburi sono stati estratti ovvero in unità dotate delle stesse caratteristiche che contengano, o abbiano contenuto, idrocarburi, indicando le modalità dello scarico. Lo scarico non deve contenere altre acque di scarico o altre sostanze pericolose diverse, per qualità e quantità, da quelle derivanti dalla separazione degli idrocarburi. Le relative autorizzazioni sono rilasciate con la prescrizione delle precauzioni tecniche necessarie a garantire che le acque di scarico non possano raggiungere altri sistemi idrici o nuocere ad altri ecosistemi.

4. In deroga a quanto previsto al comma 1, l'autorità competente, dopo indagine preventiva anche finalizzata alla verifica dell'assenza di sostanze estranee, può autorizzare gli scarichi nella stessa falda delle acque utilizzate per il lavaggio e la lavorazione degli inerti, purché i relativi fanghi siano costituiti esclusivamente da acqua ed inerti naturali ed il loro scarico non comporti danneggiamento alla falda acquifera. A tal fine, l'Agenzia regionale per la protezione dell'ambiente (ARPA) competente per territorio, a spese del soggetto richiedente l'autorizzazione, accerta le caratteristiche quantitative e qualitative dei fanghi e l'assenza di possibili danni per la falda, esprimendosi con parere vincolante sulla richiesta di autorizzazione allo scarico.

5. Per le attività di prospezione, ricerca e coltivazione di idrocarburi liquidi o gassosi in mare, lo scarico delle acque diretto in mare avviene secondo le modalità previste dal Ministro dell'ambiente e della tutela del territorio con proprio decreto, purché la concentrazione di olii minerali sia inferiore a 40 mg/1. Lo scarico diretto a mare è progressivamente sostituito dalla iniezione o reiniezione in unità geologiche profonde, non appena disponibili pozzi non più produttivi ed idonei all'iniezione o reiniezione, e deve avvenire comunque nel rispetto di quanto previsto dai commi 2 e 3.

5-bis. In deroga a quanto previsto al comma 1 è consentita l'iniezione, a fini di stoccaggio, di flussi di biossido di carbonio in formazioni geologiche prive di scambio di fluidi con altre formazioni che per motivi naturali sono definitivamente inadatte ad altri scopi, a condizione che l'iniezione sia effettuata a norma del decreto legislativo di recepimento della direttiva 2009/31/CE in materia di stoccaggio geologico di biossido di carbonio.

6. Il Ministero dell'ambiente e della tutela del territorio, in sede di autorizzazione allo scarico in unità geologiche profonde di cui al comma 3, autorizza anche lo scarico diretto a mare, secondo le modalità previste dai commi 5 e 7, per i seguenti casi:

a) per la frazione di acqua eccedente, qualora la capacità del pozzo iniettore o reiniettore non sia sufficiente a garantire la ricezione di tutta l'acqua risultante dall'estrazione di idrocarburi;

b) per il tempo necessario allo svolgimento della manutenzione, ordinaria e straordinaria, volta a garantire la corretta funzionalità e sicurezza del sistema costituito dal pozzo e dall'impianto di iniezione o di reiniezione.

7. Lo scarico diretto in mare delle acque di cui ai commi 5 e 6 è autorizzato previa presentazione di un piano di monitoraggio volto a verificare l'assenza di pericoli per le acquee per gli ecosistemi acquatici.

8. Al di fuori delle ipotesi previste dai commi 2, 3, 5 e 7, gli scarichi nel sottosuolo e nelle acque sotterranee, esistenti e debitamente autorizzati, devono essere convogliati in corpi idrici superficiali ovvero destinati, ove possibile, al riciclo, al riutilizzo o all'utilizzazione agronomica. In caso di mancata ottemperanza agli obblighi indicati, l'autorizzazione allo scarico è revocata.".

L'art. 107 del d.lgs. 152/2006 ("*Scarichi in reti fognarie*") dispone che: "*1. Ferma restando l'inderogabilità dei valori-limite di emissione di cui alla tabella 3/A dell'Allegato 5 alla parte terza del presente decreto e, limitatamente ai parametri di cui alla nota 2 della Tabella 5 del medesimo Allegato 5, alla Tabella 3, gli scarichi di acque reflue industriali che recapitano in reti fognarie sono sottoposti alle norme tecniche, alle prescrizioni regolamentari e ai valori-limite adottati dall'Autorità d'ambito competente in base alle caratteristiche dell'impianto, e in modo che sia assicurata la tutela del corpo idrico ricettore nonché il rispetto della disciplina degli scarichi di acque reflue urbane definita ai sensi dell'articolo 101, commi 1 e 2. (omissis…)*.".

Infine, l'art. 108 del d.lgs. 152/2006 ("*Scarichi di sostanze pericolose*") prevede che: "*(omissis…) 4. Per le sostanze di cui alla Tabella 3/A dell'Allegato 5 alla parte terza del presente decreto, derivanti dai cicli produttivi indicati nella medesima tabella, le autorizzazioni stabiliscono altresì la quantità massima della sostanza espressa in unità di peso per unità di elemento caratteristico dell'attività inquinante e cioè per materia prima o per unità di prodotto, in conformità con quanto indicato nella stessa Tabella. Gli scarichi contenenti le sostanze pericolose di cui al comma 1 sono assoggettati alle prescrizioni di cui al punto 1.2.3. dell'Allegato 5 alla parte terza del presente decreto. (omissis…)*.".

Come si evince dalla lettura delle disposizioni appena riportate, l'art. 137 d.lgs. 152/2006 contempla una pluralità di ipotesi di reato, che si caratterizzano per i seguenti peculiari elementi:

- *oggetto*: la norma in esame (commi 2, 3, 5, 11 e 13) tutela l'ambiente con particolare riferimento agli scarichi di acque industriali e, in particolare, sanziona:

  a) alcune condotte relative a scarichi (in rete fognaria, nel suolo, sottosuolo, acque sotterranee e acque superficiali) di acque reflue industriali contenenti sostanze pericolose, ed in particolare:

  - in relazione agli scarichi di acque reflue industriali contenenti le sostanze pericolose di cui alle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del d.lgs. 152/2006, sia l'apertura o l'effettuazione di nuovi scarichi senza autorizzazione sia la prosecuzione o il mantenimento di detti scarichi in costanza di sospensione o revoca dell'autorizzazione o di decadenza della stessa decorso il termine di sei mesi senza che sia stata rilasciato il rinnovo dell'autorizzazione per il quale è stata presentata regolare richiesta (art. 137, comma 2, d.lgs. 152/2006);
  - al di fuori delle ipotesi di cui all'art. 137, comma 5 del d.lgs. 152/2006 (v. *infra*),

in relazione alle sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A dell'Allegato 5 alla parte terza del d.lgs. 152/2006, l'effettuazione di uno scarico di acque reflue industriali contenenti le sostanze pericolose comprese nelle famiglie e nei gruppi di sostanze indicate nelle tabelle 5 e 3/A del medesimo Allegato 5, in violazione delle prescrizioni autorizzatorie o delle prescrizioni impartite dall'autorità competente per lo scarico in rete fognaria (art. 137, comma 3, d.lgs. 152/2006);

- in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza del d.lgs. 152/2006, l'effettuazione di uno scarico di acque reflue industriali che superi i valori limite fissati nella tabella 3 del medesimo Allegato 5 (ed, eventualmente, anche i valori limite fissati per le sostanze contenute nella tabella 3/A del medesimo Allegato 5), oppure i limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente a norma dell'art. 107, comma 1 del d.lgs. 152/2006 (art. 137, comma 5, d.lgs. 152/2006);
- in relazione alle sostanze indicate nella tabella 5 dell'Allegato 5 alla parte terza del d.lgs. 152/2006, l'effettuazione di uno scarico sul suolo che superi i valori limite fissati nella tabella 4 del medesimo Allegato 5 (ed, eventualmente, anche i valori limite fissati per le sostanze contenute nella tabella 3/A del medesimo Allegato 5), oppure i limiti più restrittivi fissati dalle regioni o dalle province autonome o dall'Autorità competente a norma dell'art. 107, comma 1 del d.lgs. 152/2006 (art. 137, comma 5, d.lgs. 152/2006);

b) condotte relative allo scarico diretto nel suolo, nel sottosuolo e nelle acque sotterranee di acque reflue, in particolare:

- l'inosservanza dei divieti di scarico diretto al suolo, nel sottosuolo e nelle acque sotterranee di cui agli artt. 103 e 104 del d.lgs. 152/2006, sopra integralmente trascritti (art. 137, comma 11, d.lgs. 152/2006). Tale divieto di scarico riguarda non solo le acque reflue industriali ma anche le acque meteoriche di dilavamento, di prima pioggia, domestiche e assimilate alle domestiche. Lo scarico al suolo ove autorizzato deve essere convogliato in corpi idrici superficiali;

c) condotte relative agli scarichi in mare da parte di navi o aeromobili, in particolare:

- lo scarico nelle acque del mare da parte di navi od aeromobili contenenti sostanze o materiali per i quali è imposto il divieto assoluto di sversamento in mare ai sensi delle disposizioni contenute nelle convenzioni internazionali vigenti in materia e ratificate dall'Italia[32], salvo che siano in quantità tali da essere resi rapidamente innocui dai processi fisici, chimici e biologici, che si verificano naturalmente in mare e purché in presenza di preventiva autorizzazione da parte dell'autorità competente (art. 137, comma 13, d.lgs. 152/2006). Per "scarico" in questa particolare fattispecie, non si deve fare riferimento alla nozione tecnica esaminata nelle pagine che precedono, ma al generale "sversamento".

- *soggetto attivo*: tutti i reati di cui all'art. 137 del d.lgs. 152/2006, qui in esame, possono essere commessi da *"chiunque"*. È tuttavia ragionevole ritenere che il fatto tipico possa essere rimproverato a coloro che hanno un reale potere, anche se meramente di fatto, di gestione dello scarico.
- *elemento soggettivo*: i reati di cui all'art. 137 del d.lgs. 152/2006 sono punibili sia a titolo di dolo sia a titolo di colpa.

[32] Si richiamano, in particolare, la Convenzione MARPOL 73/78 e la Convenzione di Barcellona per la protezione del Mar Mediterraneo dall'inquinamento, 1978.

5.1.4 Attività di gestione di rifiuti non autorizzata

L'art. 25-*undecies*, comma 2, lettera b), del Decreto concerne i reati di cui all'art. 256, commi 1, lettere a) e b), 3, primo e secondo periodo, 4, 5 e 6, primo periodo, del d.lgs. 152/2006 in tema di attività di gestione di rifiuti[33] non autorizzata.

L'art. 256 del d.lgs. 152/2006, per quanto qui rileva, dispone che: "*1. Chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui agli articoli 208, 209, 210, 211, 212, 214, 215 e 216[34] è punito:*

---

[33] Il rifiuto è definito ai sensi dell'art. 183, comma 1, lettera a), del d.lgs. 152/2006 come "*qualsiasi sostanza od oggetto di cui il detentore si disfi o abbia l'intenzione o abbia l'obbligo di disfarsi*". Non tutti i "residui" di produzione e di consumo sono rifiuti. Sono esclusi dalla disciplina dei rifiuti: (i) i c.d. "rifiuti che hanno cessato di essere tali" o "Materie Prime Secondarie" ("MPS") o "End of Waste" (EoW) (art. 184-*ter* del d.lgs. 152/2006); (ii) i c.d. "sottoprodotti" (art. 184-*bis* del d.lgs. 152/2006). Le definizioni normative di MPS/EoW e di sottoprodotto hanno subito nel tempo numerose modifiche, fino alla versione attualmente in vigore introdotta dal d.lgs. 205/2010 ("Quarto correttivo"). L'art. 184-*ter* del d.lgs. 152/2006, in tema di MPS/EoW, oggi stabilisce che "*Un rifiuto cessa di essere tale, quando è stato sottoposto a un'operazione di recupero, incluso il riciclaggio e la preparazione per il riutilizzo, e soddisfi i criteri specifici, da adottare nel rispetto delle seguenti condizioni:*
a) la sostanza o l'oggetto è comunemente utilizzato per scopi specifici;
b) esiste un mercato o una domanda per tale sostanza od oggetto;
c) la sostanza o l'oggetto soddisfa i requisiti tecnici per gli scopi specifici e rispetta la normativa e gli standard esistenti applicabili ai prodotti;
d) l'utilizzo della sostanza o dell'oggetto non porterà a impatti complessivi negativi sull'ambiente o sulla salute umana.
2. L'operazione di recupero può consistere semplicemente nel controllare i rifiuti per verificare se soddisfano i criteri elaborati conformemente alle predette condizioni. I criteri di cui al comma 1 sono adottati in conformità a quanto stabilito dalla disciplina comunitaria ovvero, in mancanza di criteri comunitari, caso per caso per specifiche tipologie di rifiuto attraverso uno o più decreti del Ministro dell'ambiente e della tutela del territorio e del mare, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400. I criteri includono, se necessario, valori limite per le sostanze inquinanti e tengono conto di tutti i possibili effetti negativi sull'ambiente della sostanza o dell'oggetto. […] La disciplina in materia di gestione dei rifiuti si applica fino alla cessazione della qualifica di rifiuto".
La definizione di sottoprodotto, invece, è disposta dall'art. 184-*bis* del d.lgs. 152/2006, che stabilisce che sia un sottoprodotto, e non un rifiuto, "*qualsiasi sostanza od oggetto"* che soddisfi tutte le seguenti condizioni:
a) la sostanza o l'oggetto è originato da un processo di produzione, di cui costituisce parte integrante, e il cui scopo primario non è la produzione di tale sostanza od oggetto;
b) è certo che la sostanza o l'oggetto sarà utilizzato, nel corso dello stesso o di un successivo processo di produzione o di utilizzazione, da parte del produttore o di terzi;
c) la sostanza o l'oggetto può essere utilizzato direttamente senza alcun ulteriore trattamento diverso dalla normale pratica industriale;
d) l'ulteriore utilizzo è legale, ossia la sostanza o l'oggetto soddisfa, per l'utilizzo specifico, tutti i requisiti pertinenti riguardanti i prodotti e la protezione della salute e dell'ambiente e non porterà a impatti complessivi negativi sull'ambiente o la salute umana".
Il Decreto del Ministero dell'Ambiente e della Tutela del Territorio e del Mare, 10 agosto 2012, n. 161, reca inoltre la disciplina dell'utilizzazione delle terre e rocce da scavo ed, in particolare, i criteri e le condizioni da soddisfare affinché i materiali da scavo (così come definiti dall'art. 1, comma 1, lettera b, del Decreto citato) possano essere considerati come sottoprodotti e non rifiuti.
La giurisprudenza di legittimità, dalla novella legislativa, è intervenuta a circoscrivere alcuni requisiti. Cass., sez. III, 7 giugno 2011, n. 28734, ha sottolineato la necessità della "*prova certa del loro utilizzo nel corso dello stesso o di un successivo processo di produzione o di utilizzazione*". Cass., sez. III, 10 maggio 2012, n. 17453, sul "trattamento" di "normale pratica industriale", ha precisato che l'intervento è tale solo se "*rientra tra le operazioni che l'impresa normalmente effettua sulla materia prima sostituita dal sottoprodotto*" (si segnala anche Cass., 25 maggio 2011, n. 34753, che dà conto dell'effetto di sostanziale ampliamento della portata del "sottoprodotto" in seguito alla nuova definizione del d.lgs. 205/2010, con particolare riferimento alla compatibilità di trattamenti, sul residuo, di "*normale pratica industriale*"). È opportuno mappare l'eventuale utilizzo di MPS o Sottoprodotti nel proprio ciclo produttivo, poiché, nel caso in cui non integrino i requisiti prescritti dagli artt. 184-*bis* e 184-*ter* d.lgs. 152/2006, potrebbero essere qualificati dall'accertatore procedente come "*rifiuti*", esponendo l'impresa al rischio reato in relazione agli illeciti illustrati nella presente sezione.

[34] Per comodità si riportano le rubriche degli articoli qui citati, rinviando alla loro integrale lettura per quanto d'occorrenza: art. 208 ("*Autorizzazione unica per i nuovi impianti di smaltimento e di recupero dei rifiuti*"); art. 209 ("*Rinnovo delle autorizzazioni alle imprese in possesso di certificazione ambientale*"); art. 210 ("*Autorizzazioni in*

a) con la pena dell'arresto da tre mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti non pericolosi;

b) con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti pericolosi. (omissis…)

3. Chiunque realizza o gestisce una discarica[35] non autorizzata è punito con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro. Si applica la pena dell'arresto da uno a tre anni e dell'ammenda da euro cinquemiladuecento a euro cinquantaduemila se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi.

4. Le pene di cui ai commi 1, 2 e 3 sono ridotte della metà nelle ipotesi di inosservanza delle prescrizioni contenute o richiamate nelle autorizzazioni, nonché nelle ipotesi di carenza dei requisiti e delle condizioni richiesti per le iscrizioni o comunicazioni.

5. Chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti, è punito con la pena di cui al comma 1, lettera b).

6. Chiunque effettua il deposito temporaneo[36] presso il luogo di produzione di rifiuti sanitari pericolosi[37], con violazione delle disposizioni di cui all'articolo 227, comma 1, lettera b), è punito con la pena dell'arresto da tre mesi ad un anno o con la pena dell'ammenda da duemilaseicento euro a ventiseimila euro. (omissis…)".

A sua volta, l'art. 187 del d.lgs. 152/2006 ("*divieto di miscelazione di rifiuti pericolosi*"), prevede che: "*1. È vietato miscelare rifiuti pericolosi aventi differenti caratteristiche di pericolosità ovvero rifiuti pericolosi con rifiuti non pericolosi. La miscelazione comprende la diluizione di sostanze pericolose.*

2. In deroga al comma 1, la miscelazione dei rifiuti pericolosi che non presentino la stessa caratteristica di pericolosità, tra loro o con altri rifiuti, sostanze o materiali, può essere autorizzata ai sensi degli articoli 208, 209 e 211[38] a condizione che:

a) siano rispettate le condizioni di cui all'articolo 177, comma 4[39], e l'impatto negativo della gestione dei rifiuti sulla salute umana e sull'ambiente non risulti accresciuto;

---

ipotesi particolari"); art. 211 ("*Autorizzazione di impianti di ricerca e di sperimentazione*"); art. 212 ("*Albo nazionale gestori ambientali*"); art. 214 ("*Determinazione delle attività e delle caratteristiche dei rifiuti per l'ammissione alle procedure semplificate*"); art. 215 ("*Autosmaltimento*"); art. 216 ("*Operazioni di recupero*").

[35] La nozione di discarica è offerta dall'art. 2, comma 1, lettera g) del Decreto Legislativo 13 gennaio 2003, n. 36 e successive modificazioni ed integrazioni, in questi termini: *"area adibita a smaltimento dei rifiuti mediante operazioni di deposito sul suolo o nel suolo, compresa la zona interna al luogo di produzione dei rifiuti adibita allo smaltimento dei medesimi da parte del produttore degli stessi, nonché qualsiasi area ove i rifiuti sono sottoposti a deposito temporaneo per più di un anno. Sono esclusi da tale definizione gli impianti in cui i rifiuti sono scaricati al fine di essere preparati per il successivo trasporto in un impianto di recupero, trattamento o smaltimento, e lo stoccaggio di rifiuti in attesa di recupero 0 trattamento per un periodo inferiore a tre anni come norma generale, o 10 stoccaggio di rifiuti in attesa di smaltimento per un periodo inferiore a un anno"*.

[36] Il deposito temporaneo è definito dall'art. 183, comma 1, lett. bb) del d.lgs. 152/2006, come "*il raggruppamento dei rifiuti effettuato, prima della raccolta, nel luogo in cui gli stessi sono prodotti o, per gli imprenditori agricoli di cui all' articolo 2135 del codice civile, presso il sito che sia nella disponibilità giuridica della cooperativa agricola di cui gli stessi sono soci, alle seguenti condizioni*".

[37] La disciplina dei rifiuti sanitari è offerta dal Decreto del Presidente della Repubblica n. 254 del 15 luglio 2003 ("*Regolamento recante disciplina della gestione dei rifiuti sanitari a norma dell'articolo 24 della legge 31 luglio 2002, n. 179*").

[38] Per comodità si riportano le rubriche degli articoli qui citati, rinviando alla loro integrale lettura per quanto d'occorrenza: art. 208 ("*Autorizzazione unica per i nuovi impianti di smaltimento e di recupero dei rifiuti*"); art. 209 ("*Rinnovo delle autorizzazioni alle imprese in possesso di certificazione ambientale*"); art. 211 ("*Autorizzazione di impianti di ricerca e di sperimentazione*").

[39] L'art. 177, comma 4, del d.lgs. 152/2006, recita quanto segue: "*I rifiuti sono gestiti senza pericolo per la salute dell'uomo e senza usare procedimenti o metodi che potrebbero recare pregiudizio all'ambiente e, in particolare:*
a) senza determinare rischi per l'acqua, l'aria, il suolo, nonché per la fauna e la flora;
b) senza causare inconvenienti da rumori o odori;
c) senza danneggiare il paesaggio e i siti di particolare interesse, tutelati in base alla normativa vigente.".

b) l'operazione di miscelazione sia effettuata da un ente o da un'impresa che ha ottenuto un'autorizzazione ai sensi degli articoli 208, 209 e 211;

c) l'operazione di miscelazione sia conforme alle migliori tecniche disponibili di cui all'articolo 183, comma 1, lettera nn)[40].

3. Fatta salva l'applicazione delle sanzioni specifiche ed in particolare di quelle di cui all'articolo 256, comma 5, chiunque viola il divieto di cui al comma 1 è tenuto a procedere a proprie spese alla separazione dei rifiuti miscelati, qualora sia tecnicamente ed economicamente possibile e nel rispetto di quanto previsto dall'articolo 177, comma 4."

Infine, l'art. 227, comma 1, lettera b) del d.lgs. 152/2006 ("*rifiuti elettrici ed elettronici, rifiuti sanitari, veicoli fuori uso e prodotti contenenti amianto*"), dispone che: "*Restano ferme le disposizioni speciali, nazionali e comunitarie relative alle altre tipologie di rifiuti, ed in particolare quelle riguardanti: (omissis…)*

b) rifiuti sanitari: decreto del Presidente della Repubblica 15 luglio 2003, n. 254; (omissis…).".

Le principali caratteristiche delle fattispecie di reato ora in esame sono così sintetizzabili:

- *oggetto*: per esigenze di carattere sistematico è opportuno analizzare separatamente ciascuna ipotesi di reato, di cui segnaliamo altresì le peculiarità interpretative:
    - comma 1 (gestione non autorizzata di rifiuti): il reato consiste nello svolgimento di attività di gestione dei rifiuti (quali la raccolta, il trasporto, il recupero, lo smaltimento, il commercio e l'intermediazione) in assenza della titolarità di una valida ed efficace autorizzazione, iscrizione o comunicazione. Sono parimenti punibili le attività gestorie svolte in relazione a rifiuti non contemplati dal titolo autorizzativo (seppur valido ed efficace) o, comunque, svolte in luoghi o con modalità diverse da quelle consentite da tale titolo;
    - comma 3 (discarica non autorizzata): ai fini della configurabilità del reato di discarica non autorizzata occorre che l'agente ponga in essere una condotta abusiva, ripetuta nel tempo, di accumulo di rifiuti in un'area determinata, potenzialmente idonea a provocare il degrado dell'ambiente o contribuisca in modo attivo e diretto alla realizzazione della discarica;
    - comma 4 (violazione di autorizzazioni): il reato consiste nella semplice inosservanza di una prescrizione prevista nell'autorizzazione[41], anche se meramente formale, tanto se essa discenda da una previsione di legge quanto se sia stata introdotta *motu proprio* dall'autorità che ha emesso l'autorizzazione;
    - comma 5 (divieto di miscelazione): la condotta vietata consiste nella miscelazione di rifiuti pericolosi con caratteristiche di pericolosità diverse o di rifiuti pericolosi e non pericolosi tra loro; tale reato è volto ad evitare che, in una

[40] L'art. 183, comma 1, lettera nn) del d.lgs. 152/2006 definisce le *"migliori tecniche disponibili"* come: *"le migliori tecniche disponibili quali definite all'articolo 5, comma 1, lett. l-ter) del presente decreto"*. A sua volta, *ex* art. 5, comma 1, lettera l-*ter*) del d.lgs. 152/2006, le "*migliori tecniche disponibili*" sono definite come: "*la più efficiente e avanzata fase di sviluppo di attività e relativi metodi di esercizio indicanti l'idoneità pratica di determinate tecniche a costituire, in linea di massima, la base dei valori limite di emissione intesi ad evitare oppure, ove ciò si riveli impossibile, a ridurre in modo generale le emissioni e l'impatto sull'ambiente nel suo complesso. Nel determinare le migliori tecniche disponibili, occorre tenere conto in particolare degli elementi di cui all'allegato XI. Si intende per:*
1) tecniche: sia le tecniche impiegate sia le modalità di progettazione, costruzione, manutenzione, esercizio e chiusura dell'impianto;
2) disponibili: le tecniche sviluppate su una scala che ne consenta l'applicazione in condizioni economicamente e tecnicamente idonee nell'ambito del relativo comparto industriale, prendendo in considerazione i costi e i vantaggi, indipendentemente dal fatto che siano o meno applicate o prodotte in ambito nazionale, purché il gestore possa utilizzarle a condizioni ragionevoli;
3) migliori: le tecniche più efficaci per ottenere un elevato livello di protezione dell'ambiente nel suo complesso.".

[41] Le autorizzazioni devono intendersi relative alla raccolta, trasporto, recupero, smaltimento, commercio e/o intermediazione di rifiuti nonché alla discarica.

qualsiasi fase di gestione dei rifiuti, vengano alterate le caratteristiche dei rifiuti pericolosi attraverso il mescolamento con altri rifiuti pericolosi o non pericolosi (ad esempio al fine di ridurre le concentrazioni delle sostanze pericolose così da mutarne la classificazione da pericoloso a non pericoloso);

- comma 6 (deposito temporaneo di rifiuti sanitari pericolosi): il reato presuppone la gestione di rifiuti sanitari pericolosi, punendo l'attività di deposito temporaneo degli stessi presso il luogo di produzione, effettuata in violazione della normativa di settore di cui al Decreto del Presidente della Repubblica 15 luglio 2003, n. 254 e successive modificazioni ed integrazioni ("D.P.R. 254/2003"); ai rifiuti sanitari, salve le disposizioni specifiche recate dal ai sensi del D.P.R. 254/2003, si applicano le regole generali in materia di rifiuti;

– *soggetto attivo*[42]: le fattispecie qui in evidenza ben si prestano ad essere analizzate separatamente:

- i reati di cui all'art. 256, commi 1 e 5 del d.lgs. 152/2006, possono essere commessi da *"chiunque"*, palesandosi, quindi, come reati comuni;
- il reato di cui all'art. 256, comma 3 del d.lgs. 152/2006, è di regola commesso da colui che realizza o gestisce una discarica; segnaliamo tuttavia che un orientamento restrittivo della giurisprudenza di legittimità rileva una responsabilità a titolo di concorso a carico del proprietario dell'area nel caso in cui acconsenta consapevolmente alla realizzazione o alla gestione della discarica nel suo terreno[43];
- la fattispecie di cui all'art. 256, comma 4 del d.lgs. 152/2006, invece, integra gli estremi del reato proprio poiché il soggetto autorizzato è il responsabile dell'adempimento dell'autorizzazione ed anche l'inadempimento da parte di un collaboratore risulta imputabile al titolare (salvo che il preposto abbia violato le prescrizioni che richiedano l'esercizio di limitate mansioni di carattere tecnico/operativo, con esclusione di quelle scelte generali ed autonome sull'organizzazione e/o la gestione o che, comunque, presuppongano autonomia finanzia, imputabili al predetto titolare);
- quanto al reato di cui all'art. 256, comma 6 del d.lgs. 152/2006, sebbene la norma si riferisca a qualunque soggetto, contemplando la violazione delle disposizioni dell'art. 227, comma 1, lettera b), il quale a sua volta dispone l'applicazione *in toto* del D.P.R. 254/2003, si rivolge principalmente al "*responsabile della struttura sanitaria pubblica o privata e del cimitero*" di cui all'art. 17 di quest'ultimo testo di legge, quale soggetto a cui "*è attribuito il compito di sovrintendere alla applicazione delle disposizioni*" del medesimo D.P.R. 254/2003[44].

---

[42] Per effetto dell'art. 188 del d.lgs. 152/2006 il produttore iniziale dei rifiuti o comunque il detentore dei rifiuti "*conserva la responsabilità per l'intera catena di trattamento*": in altri termini anche se il produttore/detentore trasferisce i rifiuti a un intermediario, un commerciante, un soggetto che effettui operazioni di recupero dei rifiuti, o ad un soggetto pubblico o privato addetto alla raccolta dei rifiuti, la responsabilità di regola comunque sussiste. Il produttore/detentore di rifiuti, quando non provveda all'autosmaltimento o al conferimento a soggetti che gestiscono il servizio pubblico, può consegnarli ad altri soggetti, ma, in tal caso, ha l'obbligo di controllare che si tratti di soggetti autorizzati alle attività di raccolta/recupero/smaltimento. Ove manchi tale verifica il produttore/detentore può rispondere a titolo di concorso con il soggetto eventualmente autore del reato ex art. 256 comma 1 del d.lgs. 152/2006 (Cass. Pen., sez. III, 1° marzo 2012, n. 8018; Cass. Pen., sez. III, 25 febbraio 2008, n. 8367; Cass. Pen., sez. III, 28 novembre 2007, n. 44291; Cass. Pen., sez. III, 11 maggio 2007, n. 18030).

[43] Cassazione penale sez. III, 30 novembre 2006, n. 13456.

[44] La giurisprudenza ha occasionalmente esteso tali obblighi e sanzioni anche a centri estetici e parrucchieri che detengano questo materiale.

– *elemento soggettivo*: tutti i reati sopra analizzati di cui all'art. 256 del d.lgs. 152/2006 sono punibili sia a titolo di dolo sia a titolo di colpa.

5.1.5. Reati relativi alla bonifica dei siti contaminati

L'art. 257 del d.lgs. 152/2006 dispone che: "*1. Chiunque cagiona l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio è punito con la pena dell'arresto da sei mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila euro, se non provvede alla bonifica in conformità al progetto approvato dall'autorità competente nell'ambito del procedimento di cui agli articoli 242 e seguenti. In caso di mancata effettuazione della comunicazione di cui all'articolo 242, il trasgressore è punito con la pena dell'arresto da tre mesi a un anno o con l'ammenda da mille euro a ventiseimila euro.*

2. Si applica la pena dell'arresto da un anno a due anni e la pena dell'ammenda da cinquemiladuecento euro a cinquantaduemila euro se l'inquinamento è provocato da sostanze pericolose.".

L'art. 242 del d.lgs. 152/2006 ("*Procedure operative ed amministrative*"), richiamato dal predetto art. 257 del d.lgs. 152/2006, prevede che: "*1. Al verificarsi di un evento che sia potenzialmente in grado di contaminare il sito, il responsabile dell'inquinamento mette in opera entro ventiquattro ore le misure necessarie di prevenzione e ne dà immediata comunicazione ai sensi e con le modalità di cui all'articolo 304, comma 2*[45]*. La medesima procedura si applica all'atto di individuazione di contaminazioni storiche che possano ancora comportare rischi di aggravamento della situazione di contaminazione. (omissis…)*".

Due sono le fattispecie di reato previste dal 1 comma dell'art. 257 d.lgs. 152/2006 .

Per quanto attiene alla prima frase del primo comma dell'articolo in discorso, che configura il reato c.d. di "omessa bonifica" gli elementi della fattispecie sono così sintetizzabili:

– *oggetto*: ai fini dell'integrazione del reato è necessario il verificarsi dell'evento di danno-inquinamento, con il superamento della concentrazione della soglia di rischio previste *ex lege,* cui abbia fatto seguito una condotta omissiva rispetto all'obbligo di procedere alla bonifica [46].(omissione che recente giurisprudenza ritiene integrata anche nel caso in cui il soggetto attivo, omettendo di adempiere all'obbligo di tempestiva redazione e

[45] L'art. 304 del d.lgs. 152/2006 recita quanto segue: *"1. Quando un danno ambientale non si è ancora verificato, ma esiste una minaccia imminente che si verifichi, l'operatore* [ai sensi dell'art. 302, comma 4, del d.lgs. 152/2006 per "*operatore*" s'intende "*qualsiasi persona, fisica o giuridica, pubblica o privata, che esercita o controlla un'attività professionale avente rilevanza ambientale oppure chi comunque eserciti potere decisionale sugli aspetti tecnici e finanziari di tale attività, compresi il titolare del permesso o dell'autorizzazione a svolgere detta attività*"; N.d.r.] *interessato adotta, entro ventiquattro ore e a proprie spese, le necessarie misure di prevenzione e di messa in sicurezza.*

2. L'operatore deve far precedere gli interventi di cui al comma 1 da apposita comunicazione al comune, alla provincia, alla regione, o alla provincia autonoma nel cui territorio si prospetta l'evento lesivo, nonché al Prefetto della provincia che nelle ventiquattro ore successive informa il Ministro dell'ambiente e della tutela del territorio. Tale comunicazione deve avere ad oggetto tutti gli aspetti pertinenti della situazione, ed in particolare le generalità dell'operatore, le caratteristiche del sito interessato, le matrici ambientali presumibilmente coinvolte e la descrizione degli interventi da eseguire. La comunicazione, non appena pervenuta al comune, abilita immediatamente l'operatore alla realizzazione degli interventi di cui al comma 1. Se l'operatore non provvede agli interventi di cui al comma 1 e alla comunicazione di cui al presente comma, l'autorità preposta al controllo o comunque il Ministero dell'ambiente e della tutela del territorio irroga una sanzione amministrativa non inferiore a mille euro né superiore a tremila euro per ogni giorno di ritardo (omissis…)."

[46] Come noto, è vivo il dibattito sulla natura della fattispecie criminosa di cui si tratta. Taluni, infatti, ritengono che il reato si configuri *tout court* come reato omissivo, rilevando –in sostanza- la sola omissione dell'attività di bonifica; altri –e fra essi la prevalente giurisprudenza- definiscono il reato in discorso come reato commissivo d'evento, in cui l'aver proceduto alla bonifica è una condizione obiettiva di non punibilità.

presentazione del piano di caratterizzazione, impedisca la stessa formazione del progetto di bonifica e, quindi, la sua realizzazione)[47].

- *soggetto attivo*: il reato di omessa bonifica di cui all'art. 257, comma 1, primo periodo, del d.lgs. 152/2006 può essere commesso da *"chiunque"*, sebbene –in termini pratici- è opportuno notare come dello stesso risponda soltanto il responsabile dell'inquinamento.
- *elemento soggettivo*: il reato di cui si tratta è punibile sia a titolo di dolo sia a titolo di colpa.

Per quanto attiene, invece, al reato previsto alla seconda parte del primo comma dell'art. 257, gli elementi costitutivi dello stesso possono essere così individuati e sintetizzati:

- *oggetto*: ai fini dell'integrazione del reato è necessario il verificarsi di un evento (accidentale), cui abbia fatto seguito una condotta omissiva rispetto all'obbligo di comunicare l'evento agli enti, nei tempi prescritti. La comunicazione di cui all'art. 242 del d.lgs. 152/2006 è dovuta in occasione di qualsiasi evento potenzialmente in grado di contaminare il sito e prescinde quindi dall'effettivo superamento delle soglie di contaminazione previste dalla legge; essa inoltre, è necessaria anche nel caso in cui intervengano sul luogo dell'inquinamento gli operatori di vigilanza preposti alla tutela ambientale; tale comunicazione deve essere tempestiva e consentire agli organi preposti alla tutela ambientale del territorio in cui si prospetta l'evento lesivo di prenderne compiutamente cognizione con riferimento ad ogni possibile implicazione e di verificare lo sviluppo delle iniziative ripristinatorie intraprese.
- *soggetto attivo*: il reato in discorso – come già visto in relazione al reato di omessa bonifica di cui all'art. 257, comma 1, primo periodo – può essere commesso soltanto dal responsabile dell'inquinamento, mentre ai soggetti non responsabili della potenziale contaminazione di cui all'art. 242 del d.lgs. 152/2006 competeranno i doveri ed i diritti di cui all'art. 245 del d.lgs. 152/2006 ("*Obblighi di intervento e di notifica da parte dei soggetti non responsabili della potenziale contaminazione*")[48].
- *elemento soggettivo*: il reato è punibile sia a titolo di dolo sia a titolo di colpa.

5.1.6 Reati inerenti alla violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari

L'art. 258, comma 4, secondo periodo, del d.lgs. 152/2006 dispone che: "*Si applica la pena di cui all'articolo 483 del codice penale[49] a chi, nella predisposizione di un certificato di analisi di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi fa uso di un certificato falso durante il trasporto*".

Le principali caratteristiche della fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: la norma in esame punisce, in primo luogo, chi, nella predisposizione di un certificato di rifiuti, fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti stessi. In secondo luogo la norma punisce il trasportatore che utilizzi un certificato falso durante il trasporto; allo stesso è quindi richiesto di assicurare la regolarità del trasporto verificando, per quanto pertinente alla sua

[47] Si veda, in proposito, Cass. 2 luglio 2010, n. 35774; in senso contrario, tuttavia Cass. Penale 13 aprile 2012, n. 22006.

[48] V. in proposito Cassazione Penale, sezione III, 11 maggio 2011 (ud. 16 marzo 2011), n. 18503.

[49] L'art. 483 c.p. ("*Falsità ideologica commessa dal privato in atto pubblico*") dispone che: "*Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile la reclusione non può essere inferiore a tre mesi.*".

funzione ed avvalendosi della diligenza richiesta dalla natura dell'incarico, la corrispondenza tra i dati enucleati nei certificati di analisi ed i relativi rifiuti[50].

- *soggetto attivo*: il reato in analisi può essere commesso dal soggetto incaricato di svolgere le analisi sui rifiuti ivi inclusi i laboratori interni all'ente ovvero, nel caso previsto dall'ultima parte della norma in esame, dal trasportatore. In ogni caso, deve trattarsi di soggetti che -una volta che sia entrata a regime l'operatività del SISTRI- non abbiano l'obbligo di adesione o non abbiano aderito su base volontaria allo stesso;
- *elemento soggettivo*: il reato è punibile solo a titolo di dolo, essendo dunque necessario che il soggetto agente preveda e voglia che l'evento consegua alla propria azione od omissione.

5.1.7 Traffico illecito di rifiuti

Ai sensi dell'art. 259, comma 1, del d.lgs. 152/2006 *"chiunque effettua una spedizione di rifiuti costituente traffico illecito ai sensi dell'articolo 26 del regolamento (CEE) 1° febbraio 1993, n. 259, o effettua una spedizione di rifiuti elencati nell'Allegato II del citato regolamento in violazione dell'articolo 1, comma 3, lettere a), b), c) e d), del regolamento stesso è punito con la pena dell'ammenda da millecinquecentocinquanta euro a ventiseimila euro e con l'arresto fino a due anni. La pena è aumentata in caso di spedizione di rifiuti pericolosi.*".

Il riferimento al regolamento (CEE) 1 febbraio 1993, n. 259 ("reg. 259/1993"), oramai abrogato, può intendersi oggi indirizzato al regolamento (CE) n. 1013/2006 del 4 giugno 2006 relativo alle spedizioni di rifiuti, e successive modificazioni ed integrazioni ("reg. 1013/2006")[51].

La definizione di "*traffico illecito*" contenuta nel Reg. 259/1993 e così richiamata dall'art. 259, comma 1, del d.lgs. 152/2006, è oggi sostituita dalla definizione di "*spedizione illegale*" di cui all'art. 2, n. 35 del reg. 1013/2006 corrispondente a "*qualsiasi spedizione di rifiuti[52] effettuata:*

a) senza notifica a tutte le autorità competenti interessate a norma del presente regolamento; o

b) senza l'autorizzazione delle autorità competenti interessate a norma del presente regolamento; o

---

[50] È bene precisare a questo riguardo che la legge richiede a tutti i soggetti coinvolti nel ciclo di gestione del rifiuto di attivarsi al fine di assicurare, per quanto loro possibile, il rispetto della normativa ambientale anche in relazione alle caratteristiche dei rifiuti ed in particolare: (i) il produttore dei rifiuti deve provvedere alla corretta caratterizzazione dei propri rifiuti, caso per caso ed in concreto, effettuandone il prelievo, il campionamento e le successive analisi al fine della loro classificazione, avvalendosi all'uopo di tecnici e/o laboratori idonei, di comprovata fama ed esperienza a cui devono essere fornite tutte le informazioni utili per svolgere le predette attività, quali quelle attinenti al ciclo produttivo da cui scaturiscono i rifiuti medesimi, alle caratteristiche eventualmente già note di tali rifiuti, delle metodologie di prelievo e campionamento (se ed in quanto effettuate direttamente dal produttore); (ii) il destinatario, il commerciante e l'intermediario dei rifiuti, in considerazione della diversa funzione dagli stessi ricoperta nel ciclo di gestione dei rifiuti, devono verificare, utilizzando la diligenza richiesta dalla natura dei rispettivi incarichi, la corrispondenza tra i dati enucleati nei certificati di analisi ed i relativi rifiuti.

[51] È bene precisare che, in ossequio ad un'interpretazione rigorosa del diritto penale, il richiamo a testi di legge abrogati (c.d. norma penale in bianco) potrebbe comportare l'inefficacia della norma penale a cagione della sua indeterminatezza e genericità. Per tutiorismo e in un'ottica conservativa, ai soli fini della redazione del presente Modello, ogni riferimento effettuato dalla norma in esame si intenderà diretto al testo di legge che ha sostituito, abrogandolo, la previgente disciplina espressamente richiamata dalla norma in esame.

[52] L'art. 2, n. 35 del reg. 1013/2006 definisce la "*spedizione*" come: *"il trasporto di rifiuti destinati al recupero o allo smaltimento previsto o effettuato:*
a) tra un paese ed un altro paese; o
b) tra un paese e paesi e territori d'oltremare o altre zone, sotto la protezione di tale paese; o
c) tra un paese e un territorio che non faccia parte di alcun paese in virtù del diritto internazionale; o
d) tra un paese e l'Antartico; o
e) da un paese attraverso una delle zone sopra citate; o
f) all'interno di un paese attraverso una delle zone sopra citate e che ha origine e fine nello stesso paese; o
g) da una zona geografica non soggetta alla giurisdizione di alcun paese, verso un paese."

c) con l'autorizzazione delle autorità competenti interessate ottenuto mediante falsificazioni, false dichiarazioni o frodi; o

d) in un modo che non è materialmente specificato nella notifica o nei documenti di movimento; o

e) in un modo che il recupero o lo smaltimento risulti in contrasto con la normativa comunitaria o internazionale; o

f) in contrasto con gli articoli 34, 36, 39, 40, 41 e 43; o

g) per la quale, in relazione alle spedizioni di rifiuti di cui all'articolo 3, paragrafi 2 e 4, sia stato accertato che:

i) i rifiuti non sono elencati negli allegati III, III A o III B; o

ii) l'articolo 3, paragrafo 4, non è stato rispettato;

iii) la spedizione è effettuata in un modo che non è materialmente specificato nel documento di cui all'allegato VII.

Le principali caratteristiche della fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: la norma punisce qualsiasi ipotesi di effettuazione di una "*spedizione illegale*" così come definita ai sensi dell'art. 2, n. 35 del reg. 1013/2006 e, dunque: in violazione delle regole in materia di notifica preventiva (lettera a); in mancanza di autorizzazione (lettera b); con autorizzazione ottenuta mediante falsificazioni, false dichiarazioni o frodi (lettera c); in modo diverso da quello dichiarato nella documentazione di accompagnamento (lettera d); in violazione di uno dei divieti di esportazione (lettera f); in violazione di alcuni obblighi relativi alla procedura degli "*obblighi generali di informazione*" di cui all'art. 18 del reg. 1013/2006 in relazione ai rifiuti inclusi nel c.d. "*elenco verde*" di cui agli Allegati III, IIIA e IIB del reg. 1013/2006 ed ai rifiuti destinati alle analisi da laboratorio (lettera g); quale norma di chiusura, in ogni caso in cui il trattamento risulti in contrasto con la normativa comunitaria e internazionale (lettera e).
- *soggetto attivo*: il reato in analisi può essere commesso da *"chiunque*", sebbene sia ragionevole immaginarne la commissione solo ad opera di uno dei soggetti coinvolti nel ciclo di gestione dei rifiuti.
- *elemento soggettivo*: il reato è punibile sia a titolo di dolo sia a titolo di colpa.

5.1.8 Attività organizzate per il traffico illecito di rifiuti

L'art. 260 del d.lgs. 152/2006 prevede che "*1. Chiunque, al fine di conseguire un ingiusto profitto, con più operazioni e attraverso l'allestimento di mezzi e attività continuative organizzate, cede, riceve, trasporta, esporta, importa, o comunque gestisce abusivamente ingenti quantitativi di rifiuti è punito con la reclusione da uno a sei anni.*

2. Se si tratta di rifiuti ad alta radioattività[53] *si applica la pena della reclusione da tre a otto anni. (omissis)*".

Le principali caratteristiche della fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: l'art. 260 del d.lgs. 152/2006 concerne qualsiasi attività di gestione dei rifiuti ivi incluse quelle di commercio ed intermediazione. La quantità di rifiuti gestita deve essere ingente -anche con riferimento al quantitativo di rifiuti complessivamente gestito attraverso una pluralità di operazioni e nonostante i quantitativi delle singole operazioni possano

[53] Il concetto di alta radioattività non è definito da questa norma né dalla legislazione speciale in materia di rifiuti radioattivi. La disciplina sui materiali radioattivi è contenuta nel Decreto Legislativo 17 marzo 1995, n. 230 e successive modificazioni ed integrazioni, il quale tuttavia non fornisce una definizione o il criterio di classificazione dei rifiuti in base al grado di radioattività.

essere qualificati come modesti. L'ingiusto profitto perseguito dall'agente è configurabile anche nella semplice riduzione dei costi aziendali. Per l'integrazione del reato non è richiesto né il compimento della condotta in mancanza di un'autorizzazione o in sua violazione né il verificarsi di un danno ambientale o la minaccia di tale danno.

- *soggetto attivo*: trattasi di reato comune, potendo essere commesso da *"chiunque*", e monosoggettivo, anche se nella pratica può assumere di fatto carattere associativo e di criminalità organizzata.
- *elemento soggettivo*: il reato è punibile a titolo di dolo specifico.

5.1.9 Reati commessi nell'ambito del Sistema informatico di controllo della tracciabilità dei rifiuti (SISTRI)

L'art. 25-*undecies*, comma 2, lettera g), del Decreto include tra i reati ambientali suscettibili di configurare una responsabilità amministrativa degli enti quelli di cui all'art. 260-*bis*, commi 6, 7, secondo e terzo periodo, e 8, primo e secondo periodo, relativi al sistema informatico di controllo della tracciabilità dei rifiuti ("SISTRI").

In particolare, l'art. 260-*bis* del d.lgs. 152/2006, per quanto qui rileva, dispone che: "*(omissis…) 6. Si applica la pena di cui all'articolo 483 c.p.*[54] *a colui che, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti fornisce false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e a chi inserisce un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti.*

7. (omissis…). Si applica la pena di cui all'art. 483 del codice penale in caso di trasporto di rifiuti pericolosi. Tale ultima pena si applica anche a colui che, durante il trasporto fa uso di un certificato di analisi di rifiuti contenente false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti trasportati.

8. Il trasportatore che accompagna il trasporto di rifiuti con una copia cartacea della scheda SISTRI - AREA Movimentazione fraudolentemente alterata è punito con la pena prevista dal combinato disposto degli articoli 477 e 482[55] *del codice penale. La pena è aumentata fino ad un terzo nel caso di rifiuti pericolosi.*".

Le principali caratteristiche delle fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: le fattispecie qui in evidenza ben si prestano ad essere analizzate separatamente:
  - quanto ai reati in materia di certificazione ed analisi falsa, l'art. 260-*bis*, commi 6 e 7 prima parte, del d.lgs. 152/2006 è speculare a quello di cui all'art. 258, comma 4, del d.lgs. 152/2006 in tema di falsità ideologica del certificato di analisi di rifiuti con la precisazione che, nel caso di specie, il riferimento è volto alla gestione di rifiuti in ossequio al SISTRI (v. al riguardo le considerazioni svolte al precedente paragrafo 2.1.5.).
  - quanto ai reati in materia di trasporto, l'art. 260-*bis*, commi 7 seconda parte e 8,

[54] L'art. 483 c.p. ("*Falsità ideologica commessa dal privato in atto pubblico*") dispone che: "*Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile la reclusione non può essere inferiore a tre mesi.*".

[55] L'art. 477 c.p. ("*Falsità materiale commessa da pubblico ufficiale in certificati o autorizzazioni amministrative*") prevede che: "*il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni."*
L'art. 482 ("*Falsità materiale commessa dal privato*") dispone che: "*se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.*".

del d.lgs. 152/2006, richiamando agli artt. 477 e 482 c.p. configura un'ipotesi di falsità materiale della documentazione che deve accompagnare il trasporto in ossequio al SISTRI (i.e. la scheda denominata "*SISTRI - AREA Movimentazione*").

- *soggetto attivo*: i reati in materia di certificazione ed analisi falsa di cui all'art. 260-*bis*, commi 6 e 7 prima parte, del d.lgs. 152/2006 possono essere commessi da chi predispone il certificato, da chi lo utilizza, da chi lo inserisce nel sistema informatico e da chi lo trasporta. I reati in materia di trasporto di cui all'art. 260-*bis*, commi 7 seconda parte e 8, del d.lgs. 152/2006, possono essere commessi solo dal trasportatore.
- *elemento soggettivo*: il reato è punibile solo a titolo di dolo, essendo dunque necessario che il soggetto agente preveda e voglia che l'evento consegua alla propria azione od omissione.

5.1.10 Reati connessi alle emissioni in atmosfera

Tra i reati rilevanti ai fini dell'applicazione del Decreto, si annovera anche l'art. 279, comma 5 del d.lgs. 152/2006, secondo il quale: "*Nei casi previsti dal comma 2 si applica sempre la pena dell'arresto fino ad un anno se il superamento dei valori limite di emissione determina anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa.*".

Per comodità, si riporta il contenuto dell'art. 279, comma 2, del d.lgs. 152/2006, alla cui stregua "*chi, nell'esercizio di uno stabilimento[56], viola i valori limite di emissione o le prescrizioni stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla parte quinta del presente decreto, dai piani e dai programmi o dalla normativa di cui all'articolo 271[57] o le prescrizioni altrimenti imposte dall'autorità competente ai sensi del presente titolo[58] è punito con l'arresto fino ad un anno o con l'ammenda fino a 1.032 euro. Se i valori limite o le prescrizioni violati sono contenuti nell'autorizzazione integrata ambientale si applicano le sanzioni previste dalla normativa che disciplina tale autorizzazione*".

Le principali caratteristiche della fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: la norma in esame sanziona il superamento dei valori limiti di qualità dell'aria stabiliti dalla legge se accompagnata alla violazione dei valori limite di emissione o delle prescrizioni stabiliti dall'autorizzazione, dagli Allegati I, II, III o V alla parte V del d.lgs.152/2006, dai piani e dai programmi o dalla normativa di cui all'articolo 271 del d.lgs. 152/2006 o dalle prescrizioni altrimenti imposte dall'autorità competente, anche se afferenti ad adempimenti prodromici alla messa in esercizio dell'impianto.
- *soggetto attivo*: la norma si rivolge a coloro i quali sono titolari di autorizzazioni o, comunque, destinatari dei precetti richiamati dall'art. 279, comma 2 del d.lgs. 152/2006.
- *elemento soggettivo*: i reati di cui all'art. 137 del d.lgs. 152/2006 sono punibili sia a titolo di dolo sia a titolo di colpa.

---

[56] Ai sensi dell'art. 268, comma 1, lettera h), del d.lgs. 152/2006 lo "*stabilimento*" è definito come: "*il complesso unitario e stabile, che si configura come un complessivo ciclo produttivo, sottoposto al potere decisionale di un unico gestore, in cui sono presenti uno o più impianti o sono effettuate una o più attività che producono emissioni attraverso, per esempio, dispositivi mobili, operazioni manuali, deposizioni e movimentazioni. Si considera stabilimento anche il luogo adibito in modo stabile all'esercizio di una o più attività*". La definizione di "*impianto*" citata nella norma da ultimo citata è offerta dall'art. 268, comma 1, lettera l), del d.lgs. 152/2006, nei seguenti termini: "*il dispositivo o il sistema o l'insieme di dispositivi o sistemi fisso e destinato a svolgere in modo autonomo una specifica attività, anche nell'ambito di un ciclo più ampio*".

[57] La norma di cui all'art. 271 del d.lgs. 152/2006 concerne i "*Valori limite di emissione e prescrizioni per gli impianti e le attività*".

[58] Il Titolo I della Parte V del d.l.gs. 152/2006 disciplina la "*Prevenzione e limitazione delle emissioni in atmosfera di impianti e attività*".

5.1.11 Reati aventi ad oggetto specie animali e vegetali in via di estinzione

L'art. 25-*undecies*, comma 3 del Decreto contempla diverse figure di reato relative alla tutela delle specie animali e vegetali in via di estinzione offerta dalla L. 150/1992, che possono essere esaminate nel contesto del presente paragrafo per le loro spiccate similarità.

La L. 150/1992 richiama a più riprese quanto statuito dal Regolamento (CE) n. 338/97 del Consiglio del 9 dicembre 1996, e successive integrazioni e modificazioni, ("reg. 338/97") relativo alla protezione di specie della flora e della fauna selvatiche mediante il controllo del loro commercio.

(i) Specie animali e vegetali in via di estinzione di cui all'Allegato A del reg. 338/97

Ai sensi dell'art. 1, commi 1 e 2, della L. 150/1992 "*1. Salvo che il fatto costituisca più grave reato, è punito con l'arresto da tre mesi ad un anno e con l'ammenda da lire quindici milioni a lire centocinquanta milioni chiunque, in violazione di quanto previsto dal Regolamento (CE) n. 338/97 del Consiglio del 9 dicembre 1996, e successive attuazioni e modificazioni, per gli esemplari appartenenti alle specie elencate nell'allegato A del Regolamento medesimo e successive modificazioni:*

a) importa, esporta o riesporta esemplari, sotto qualsiasi regime doganale, senza il prescritto certificato o licenza, ovvero con certificato o licenza non validi ai sensi dell'articolo 11, comma 2a, del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni;

b) omette di osservare le prescrizioni finalizzate all'incolumità degli esemplari, specificate in una licenza o in un certificato rilasciati in conformità al Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni;

c) utilizza i predetti esemplari in modo difforme dalle prescrizioni contenute nei provvedimenti autorizzativi o certificativi rilasciati unitamente alla licenza di importazione o certificati successivamente;

d) trasporta o fa transitare, anche per conto terzi, esemplari senza la licenza o il certificato prescritti, rilasciati in conformità del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni e, nel caso di esportazione o riesportazione da un Paese terzo parte contraente della Convenzione di Washington, rilasciati in conformità della stessa, ovvero senza una prova sufficiente della loro esistenza;

e) commercia piante riprodotte artificialmente in contrasto con le prescrizioni stabilite in base all'articolo 7, paragrafo 1, lettera b), del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997 e successive modificazioni;

f) detiene, utilizza per scopi di lucro, acquista, vende, espone o detiene per la vendita o per fini commerciali, offre in vendita o comunque cede esemplari senza la prescritta documentazione.

2. In caso di recidiva, si applica la sanzione dell'arresto da tre mesi a due anni e dell'ammenda da lire venti milioni a lire duecento milioni. Qualora il reato suddetto viene commesso nell'esercizio di attività di impresa, alla condanna consegue la sospensione della licenza da un minimo di sei mesi ad un massimo di diciotto mesi.".

Le principali caratteristiche delle fattispecie di reato in discorso sono così sintetizzabili:

– *oggetto*: la norma punisce il traffico (ovvero sia il commercio sia il trasporto) non autorizzato di un vasto numero di esemplari (cioè di qualsiasi pianta o animale viva o morta delle specie indicate all'Allegato A del regolamento 338/97) effettuato in violazione di quanto previsto dal reg. 338/97, relativo alla protezione di specie della flora e della fauna

selvatiche mediante il controllo del loro commercio, limitatamente alle specie elencate nell'allegato A del medesimo. Ai sensi dell'art. 9 del regolamento 338/97 son consentiti spostamenti all'interno dell'Unione Europea di esemplari vivi di cui all'allegato A previa specifica licenza/autorizzazione.

- *soggetto attivo*: i reati considerati possono essere commessi da "*chiunque*".
- *elemento soggettivo*: tali reati sono punibili sia a titolo di dolo sia a titolo di colpa.

(ii) Specie animali e vegetali in via di estinzione di cui all'Allegato B del reg. 338/97

L'art. 2 della L. 150/1992 presenta lo stesso contenuto dell'articolo 1 sebbene relativamente agli esemplari inclusi nell'allegato B al reg. 338/97.

Esso, in particolare, dispone che: "*1. Salvo che il fatto costituisca più grave reato, è punito con l'ammenda da lire venti milioni a lire duecento milioni o con l'arresto da tre mesi ad un anno, chiunque, in violazione di quanto previsto dal Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni, per gli esemplari appartenenti alle specie elencate negli allegati B e C del Regolamento medesimo e successive modificazioni:*

a) importa, esporta o riesporta esemplari, sotto qualsiasi regime doganale, senza il prescritto certificato o licenza, ovvero con certificato o licenza non validi ai sensi dell'articolo 11, comma 2a, del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni;

b) omette di osservare le prescrizioni finalizzate all'incolumità degli esemplari, specificate in una licenza o in un certificato rilasciati in conformità al Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni, e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni;

c) utilizza i predetti esemplari in modo difforme dalle prescrizioni contenute nei provvedimenti autorizzativi o certificativi rilasciati unitamente alla licenza di importazione o certificati successivamente;

d) trasporta o fa transitare, anche per conto terzi, esemplari senza licenza o il certificato prescritti, rilasciati in conformità del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni, e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni e, nel caso di esportazione o riesportazione da un Paese terzo parte contraente della Convenzione di Washington, rilasciati in conformità della stessa, ovvero senza una prova sufficiente della loro esistenza;

e) commercia piante riprodotte artificialmente in contrasto con le prescrizioni stabilite in base all'articolo 7, paragrafo 1, lettera b), del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive attuazioni e modificazioni, e del Regolamento (CE) n. 939/97 della Commissione, del 26 maggio 1997, e successive modificazioni;

f) detiene, utilizza per scopi di lucro, acquista, vende, espone o detiene per la vendita o per fini commerciali, offre in vendita o comunque cede esemplari senza la prescritta documentazione, limitatamente alle specie di cui all'allegato B del Regolamento.

2. In caso di recidiva, si applica la sanzione dell'arresto da tre mesi a un anno e dell'ammenda da lire venti milioni a lire duecento milioni. Qualora il reato suddetto viene commesso nell'esercizio di attività di impresa, alla condanna consegue la sospensione della licenza da un minimo di quattro mesi ad un massimo di dodici mesi.".

Le principali caratteristiche delle fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: la norma punisce il traffico (ovvero sia il commercio sia il trasporto) non autorizzato di un vasto numero di esemplari (cioè di qualsiasi pianta o animale viva o morta

delle specie indicate all'Allegato B del regolamento 338/97) effettuato in violazione di quanto previsto dal reg. 338/97, relativo alla protezione di specie della flora e della fauna selvatiche mediante il controllo del loro commercio, limitatamente alle specie elencate nell'Allegato B del medesimo. Sono soggetti alla disciplina riguardante le specie dell'Allegato B anche gli esemplari delle specie elencate nell'Allegato A nate ed allevate in cattività o riprodotte artificialmente.

- *soggetto attivo*: i reati considerati possono essere commessi da "*chiunque*".
- *elemento soggettivo*: tali reati sono punibili sia a titolo di dolo sia a titolo di colpa.

(iii) Esemplari vivi di mammiferi e rettili

L'art. 6 della L. 150/1992, per quanto rileva ai fini dell'applicazione del Decreto, dispone quanto che: "*1. Fatto salvo quanto previsto dalla legge 11 febbraio 1992, n. 157, è vietato a chiunque detenere esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e per l'incolumità pubblica.*

4. Chiunque contravviene alle disposizioni di cui al comma 1 è punito con l'arresto fino a tre mesi o con l'ammenda da lire quindici milioni a lire duecento milioni."

Le principali caratteristiche delle fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: la norma punisce la detenzione di esemplari vivi di particolari mammiferi e rettili, provenienti da riproduzioni in cattività, che costituiscano pericolo per la salute e l'incolumità pubblica.
- *soggetto attivo*: i reati considerati possono essere commessi da "*chiunque*".
- *elemento soggettivo*: il reato è punibile sia a titolo di dolo sia a titolo di colpa.

(iv) Falsità, alterazione ed uso di certificati, licenze etc.

Ai sensi dell'art. 3-*bis*, comma 1 della L. 150/1992: "*1. Alle fattispecie previste dall'articolo 16, paragrafo 1, lettere a), c), d), e), ed l), del Regolamento (CE) n. 338/97 del Consiglio, del 9 dicembre 1996, e successive modificazioni, in materia di falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni al fine di acquisizione di una licenza o di un certificato, di uso di certificati o licenze falsi o alterati si applicano le pene di cui al libro II, titolo VII, capo III del codice penale.*"

La norma in commento è stata emanata in attuazione di quanto previsto dall'art. 16, comma 1 del reg. 338/97 secondo cui, per quanto qui rileva: "*1. Gli Stati membri adottano i provvedimenti adeguati per garantire che siano irrogate sanzioni almeno per le seguenti violazioni del presente regolamento:*

a) introduzione di esemplari nella Comunità ovvero esportazione o riesportazione dalla stessa, senza il prescritto certificato o licenza ovvero con certificato o licenza falsi, falsificati o non validi, ovvero alterati senza l'autorizzazione dell'organo che li ha rilasciati; (omissis…)

c) falsa dichiarazione oppure comunicazione di informazioni scientemente false al fine di conseguire una licenza o un certificato;

d) uso di una licenza o certificato falsi, falsificati o non validi, ovvero alterati senza autorizzazione, come mezzo per conseguire una licenza o un certificato comunitario ovvero per qualsiasi altro scopo rilevante ai sensi del presente regolamento;

e) omessa o falsa notifica all'importazione; (omissis…)

l) falsificazione o alterazione di qualsiasi licenza o certificato rilasciati in conformità del presente regolamento; (omissis…).".

Le principali caratteristiche delle fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: il reato concerne una pluralità di condotte aventi ad oggetto il falso commesso con riferimento alla documentazione richiesta dalla legge, nazionale ed europea, per gestire in modo lecito il commercio delle specie animali e vegetali protette. Le pene applicabili sono quelle previste dal Codice Penale in tema di falso di cui al Libro II ("*Dei delitti in particolare*"), Titolo VII ("*Dei delitti contro la fede pubblica*"), Capo III ("*Della falsità in atti*").
- *soggetto attivo*: i reati considerati possono essere commessi, a seconda dei casi, da pubblici ufficiali (ad esempio, in tema di "*Falsità materiale commessa da pubblico ufficiale in certificati o autorizzazioni amministrative*" di cui all'art. 477 c.p.) ovvero da qualsiasi soggetto (ad es., in tema di "*Falsità materiale commessa dal privato*" di cui all'art. 482 c.p.).
- *elemento soggettivo*: tutti i delitti di cui al libro II, titolo VII, capo III del Codice Penale sono punibili solo a titolo di dolo.

5.1.12 Reati connessi alla cessazione e riduzione dell'impiego delle sostanze lesive a tutela dell'ozono stratosferico e dell'ambiente

L'art. 25-*undecies*, comma 4, del Decreto prevede specifiche sanzioni a carico degli enti nel caso di violazione di quanto disposto dall'art. 3, comma 6 della L. 549/1993 il quale punisce ogni violazione della normativa recata da tale articolo.

Ed invero, ai sensi dell'art. 3 della L. 549/1993: "*1. La produzione, il consumo, l'importazione, l'esportazione, la detenzione e la commercializzazione delle sostanze lesive di cui alla tabella A allegata alla presente legge sono regolati dalle disposizioni di cui al regolamento (CE) n. 3093/94.*

2. A decorrere dalla data di entrata in vigore della presente legge è vietata l'autorizzazione di impianti che prevedano l'utilizzazione delle sostanze di cui alla tabella A allegata alla presente legge, fatto salvo quanto disposto dal regolamento (CE) n. 3093/94.

3. Con decreto del Ministro dell'ambiente, di concerto con il Ministro dell'industria, del commercio e dell'artigianato, sono stabiliti, in conformità alle disposizioni ed ai tempi del programma di eliminazione progressiva di cui al regolamento (CE) n. 3093/94, la data fino alla quale è consentito l'utilizzo di sostanze di cui alla tabella A, allegata alla presente legge, per la manutenzione e la ricarica di apparecchi e di impianti già venduti ed installati alla data di entrata in vigore della presente legge, ed i tempi e le modalità per la cessazione dell'utilizzazione delle sostanze di cui alla tabella B, allegata alla presente legge, e sono altresì individuati gli usi essenziali delle sostanze di cui alla tabella B, relativamente ai quali possono essere concesse deroghe a quanto previsto dal presente comma. La produzione, l'utilizzazione, la commercializzazione, l'importazione e l'esportazione delle sostanze di cui alle tabelle A e B allegate alla presente legge cessano il 31 dicembre 2008, fatte salve le sostanze, le lavorazioni e le produzioni non comprese nel campo di applicazione del regolamento (CE) n. 3093/94, secondo le definizioni ivi previste.

4. L'adozione di termini diversi da quelli di cui al comma 3, derivati dalla revisione in atto del regolamento (CE) n. 3093/94, comporta la sostituzione dei termini indicati nella presente legge ed il contestuale adeguamento ai nuovi termini.

5. Le imprese che intendono cessare la produzione e la utilizzazione delle sostanze di cui alla tabella B allegata alla presente legge prima dei termini prescritti possono concludere appositi accordi di programma con il Ministero dell'industria, del commercio e dell'artigianato e

dell'ambiente, al fine di usufruire degli incentivi di cui all'art. 10, con priorità correlata all'anticipo dei tempi di dismissione, secondo le modalità che saranno fissate con decreto del Ministro dell'industria, del commercio e dell'artigianato, d'intesa con il Ministro dell'ambiente.

6. Chiunque violi le disposizioni di cui al presente articolo, è punito con l'arresto fino a due anni e con l'ammenda fino al triplo del valore delle sostanze utilizzate per fini produttivi, importate o commercializzate. Nei casi più gravi, alla condanna consegue la revoca dell'autorizzazione o della licenza in base alla quale viene svolta l'attività costituente illecito".

Le principali caratteristiche delle fattispecie di reato in discorso sono così sintetizzabili:

- *oggetto*: ogni riferimento al regolamento (CE) n. 3093/94, oramai abrogato, può intendersi oggi indirizzato al regolamento 1005/2009/CE[59], sulle sostanze che riducono lo strato di ozono (in particolare CFC, CFC completamente alogenati, halon, tetracloruro di carbonio, metilcloroformio, bromuro di metile, idrobromuroclorofluorocarburi e idroclorofluorocarburi, quali i gruppi da 1 a 8 dell'allegato 1 Regolamento 1005/2009/CE). Giova anche segnalare che gli usi essenziali di sostanze controllate diverse dagli idroclorofluorocarburi per usi essenziali di laboratorio sono oggi disciplinati dal regolamento (UE) n. 291/2011.
- *soggetto attivo*: l'art. 3 della L. 549/1993 è suscettibile di applicazione a qualsiasi soggetto.
- *elemento soggettivo*: la punibilità è prevista sia a titolo di dolo sia a titolo di colpa.

5.1.13 Reati di inquinamento doloso e colposo provocato dalle navi

Con il Decreto Legislativo 6 novembre 2007, n. 202, e successive modificazioni ed integrazioni ("d.lgs. 202/2007") è stata data attuazione alla Direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni.

Ai fini dell'irrogazione delle sanzioni del Decreto a carico degli enti, sono contemplate due distinte ipotesi di reato previste rispettivamente dagli artt. 8 e 9 del d.lgs. 202/2007.

Ai sensi dell'art. 8 del d.lgs. 202/2007 "*1. Salvo che il fatto costituisca più grave reato, il Comandante di una nave, battente qualsiasi bandiera, nonché i membri dell'equipaggio, il proprietario e l'armatore della nave, nel caso in cui la violazione sia avvenuta con il loro concorso, che dolosamente violano le disposizioni dell'art. 4 sono puniti con l'arresto da sei mesi a due anni e con l'ammenda da euro 10.000 ad euro 50.000.*

2. Se la violazione di cui al comma 1 causa danni permanenti o, comunque, di particolare gravità, alla qualità delle acque, a specie animali o vegetali o a parti di queste, si applica l'arresto da uno a tre anni e l'ammenda da euro 10.000 ad euro 80.000.".

Ai sensi dell'art. 9 del d.lgs. 202/2007 : "*1. Salvo che il fatto costituisca più grave reato, il Comandante di una nave, battente qualsiasi bandiera, nonché i membri dell'equipaggio, il proprietario e l'armatore della nave, nel caso in cui la violazione sia avvenuta con la loro cooperazione, che violano per colpa le disposizioni dell'art. 4, sono puniti con l'ammenda da euro 10.000 ad euro 30.000.*

2. Se la violazione di cui al comma 1 causa danni permanenti o, comunque, di particolare gravità, alla qualità delle acque, a specie animali o vegetali o a parti di queste, si applica l'arresto da sei mesi a due anni e l'ammenda da euro 10.000 ad euro 30.000.

[59] È bene precisare che, in ossequio ad un'interpretazione rigorosa del diritto penale, il richiamo a testi di legge abrogati (c.d. norma penale in bianco) potrebbe comportare l'inefficacia della norma penale a cagione della sua indeterminatezza e genericità. Per tutiorismo e in un'ottica conservativa, ai soli fini della redazione del presente Modello, ogni riferimento effettuato dalla norma in esame si intenderà diretto al testo di legge che ha sostituito, abrogandolo, la previgente disciplina espressamente richiamata dalla norma in esame.

3. Il danno si considera di particolare gravità quando l'eliminazione delle sue conseguenze risulta di particolare complessità sotto il profilo tecnico, ovvero particolarmente onerosa o conseguibile solo con provvedimenti eccezionali.".

L'art. 4 del d.lgs. 202/2007, così come richiamato dall'art. 8 di cui sopra, dispone quanto segue: "*Fatto salvo quanto previsto all'articolo 5, nelle aree di cui all'articolo 3, comma 1, è vietato alle navi, senza alcuna discriminazione di nazionalità, versare in mare le sostanze inquinanti*[60] *di cui all'articolo 2, comma 1, lettera b), o causare lo sversamento di dette sostanze.".*

Le aree per cui, salvo quanto previsto dall'art. 5 del d.lgs. 202/2007 di cui *infra*, vige il divieto di sversamento sono elencate dall'art. 3, comma 1 del medesimo d.lgs. 202/2007, secondo cui: "*1. Le disposizioni del presente decreto si applicano agli scarichi in mare delle sostanze inquinanti di cui all'articolo 2, comma 1, lettera b), provenienti dalle navi battenti qualsiasi bandiera effettuati:*

a) nelle acque interne, compresi i porti, nella misura in cui è applicabile il regime previsto dalla Convenzione Marpol 73/78[61]*;*

b) nelle acque territoriali;

c) negli stretti utilizzati per la navigazione internazionale e soggetti al regime di passaggio di transito, come specificato nella parte III, sezione 2, della Convenzione delle Nazioni Unite del 1982 sul diritto del mare;

d) nella zona economica esclusiva o in una zona equivalente istituita ai sensi del diritto internazionale e nazionale;

e) in alto mare.

2. Le disposizioni del presente decreto non si applicano alle navi militari da guerra o ausiliarie e alle navi possedute o gestite dallo Stato, solo se impiegate per servizi governativi e non commerciali."

Il successivo art. 5 del d.lgs. 202/2007, contempla alcune deroghe ai divieti stabiliti dall'art. 4 disponendo che "*1. Lo scarico di sostanze inquinanti di cui all'articolo 2, comma 1, lettera b), in una delle aree di cui all'articolo 3, comma 1, è consentito se effettuato nel rispetto delle condizioni di cui all'allegato I, norme 15, 34, 4.1 o 4.3 o all'allegato II, norme 13, 3.1 o 3.3 della Convenzione Marpol 73/78.*

2. Lo scarico di sostanze inquinanti di cui all'articolo 2, comma 1, lettera b), nelle aree di cui all'articolo 3, comma 1, lettere c), d) ed e), è consentito al proprietario, al comandante o all'equipaggio posto sotto la responsabilità di quest'ultimo, se effettuato nel rispetto delle condizioni di cui all'allegato I, norma 4.2, o all'allegato II, norma 3.2 della Convenzione Marpol 73/78.".

Le principali caratteristiche della fattispecie di reato in discorso sono così sintetizzabili:

– *oggetto*: la norma sanziona lo sversamento di particolari sostanze inquinanti in mare da parte di navi al fine di tutelare l'ambiente marino. Giova precisare che, ai sensi dell'art. 2, comma 1, lettera d), d.lgs. 202/2007, per "*nave*" si intende "*un natante di qualsiasi tipo comunque operante nell'ambiente marino e battente qualsiasi bandiera, compresi gli aliscafi, i veicoli a cuscino d'aria, i sommergibili, i galleggianti, le piattaforme fisse e*

[60] Tali sostanze inquinanti sono definite dall'art. 2, comma 1, lettera b), del d.lgs. 202/2007 come "*le sostanze inserite nell'allegato I (idrocarburi) e nell'allegato II (sostanze liquide nocive trasportate alla rinfusa) alla Convenzione Marpol 73/78, come richiamate nell'elenco di cui all'allegato A alla legge 31 dicembre 1982, n. 979, aggiornato dal decreto del Ministro della marina mercantile 6 luglio 1983, pubblicato nella Gazzetta Ufficiale n. 229 del 22 agosto 1983*".

[61] Trattasi, ai sensi dell'art. 2, comma 1, lettera a), del d.lgs. 202/2007 della "*Convenzione internazionale del 1973 per la prevenzione dell'inquinamento causato dalle navi e il relativo protocollo del 1978*".

galleggianti". Ai sensi dell'art. 2, comma 1, lettera c), d.lgs. 202/2007, per "sostanze inquinanti" si intendono "*le sostanze inserite nell'allegato I (idrocarburi) e nell'allegato II (sostanze liquide nocive trasportate alla rinfusa) alla Convenzione Marpol 73/78*". E' quindi vietato lo scarico di dette sostanze, da parte di nave battente qualsiasi bandiera, nelle acque interne, nel mare territoriale, nella zona economica esclusiva, in alto mare[62] (vds. artt. 3 e 4 d.lgs. 202/2007). Sono previste deroghe a detto divieto, giusto il rinvio alle rilevanti disposizioni della Convenzione MARPOL 73/78 in materia di inquinamento provocato da navi. In particolare: (i) lo scarico di sostanze inquinanti (ad esempio idrocarburi) nelle acque territoriali è consentito se "*the discharge into the sea of oil or oily mixture necessary for the purpose of securing the safety of a ship or saving life at sea*" oppure se si tratta di scarico di sostanze contenenti idrocarburi utilizzate per combattere l'inquinamento; (ii) lo scarico di sostanze inquinanti (ad esempio idrocarburi) nella zona economia esclusiva o in alto mare è consentito al proprietario, al comandante o all'equipaggio se "*the discharge into the sea of oil or oily mixture resulting from damage to a ship or its equipment: 2.1. provided that all reasonable precautions have been taken after the occurrence of the damage or discovery of the discharge for the purpose of preventing or minimizing the discharge; and 2.2. except if the owner or the master acted either with intent to cause damage, or recklessly and with knowledge that damage would probably result"*.

- *soggetto attivo*: i reati possono essere commessi dal Comandante della nave, battente qualsiasi bandiera, nonché dai membri dell'equipaggio, dal proprietario e dall'armatore della nave.
- *elemento soggettivo*: il reato è punito a titolo sia di dolo (art. 8 d.lgs. 202/2007) sia si colpa (art. 7 d.lgs. 202/2007). L'ipotesi dolosa prevede che i membri dell'equipaggio, il proprietario e l'armatore della nave rispondono del reato se "*la violazione è avventa con il loro concorso*", che ben potrebbe essere anche concorso colposo e non solo doloso. L'ipotesi colposa prevede che i membri dell'equipaggio, il proprietario e l'armatore della nave rispondono del reato "*nel caso in cui la violazione sia avvenuta con la loro cooperazione*".

Sempre con riferimento alle ipotesi di reato di cui agli articoli 8 e 9 del d.lgs. 202/2007, in ossequio ai principi generali (Codice penale e Codice della navigazione[63]), e tenuto conto del tenore letterale di quanto disposto dall'art. 5-*bis* della Direttiva 2009/123/CE[64], risulta che:

---

[62] La Convenzione di Montego Bay stabilisce che ogni Stato è libero di stabilire l'ampiezza delle proprie acque territoriali, fino ad una ampiezza massima di 12 miglia marine. La fascia di mare che va dalle 12 miglia fino a 200 miglia dalla costa viene definita zona economia esclusiva. Al di là di detto limite vi è l'alto mare.

[63] Ai sensi dell'art. 4 del Codice della Navigazione "*Le navi italiane in alto mare e gli aeromobili italiani in luogo o spazio non soggetto alla sovranità di alcuno Stato sono considerati come territorio italiano*", mentre ai sensi dell'art. 7 "*La responsabilità dell' armatore della nave e dell' esercente dell' aeromobile per atti o fatti dell' equipaggio è regolata dalla legge nazionale della nave o dell' aeromobile*". L'art. 8 prevede, quindi, che "*poteri, i doveri e le attribuzioni del comandante della nave o dell' aeromobile sono regolati dalla legge nazionale della nave o dell' aeromobile*".

[64] Articolo 5-*bis*:

"*1. Gli Stati membri provvedono affinché le violazioni ai sensi degli articoli 4 e 5 siano considerate reati.*

2. Il paragrafo 1 non si applica ai casi di minore entità qualora l'atto commesso non provochi un deterioramento della qualità dell'acqua.

3. I casi di minore entità che si verificano ripetutamente e che provocano, non singolarmente bensì nel loro insieme, un deterioramento della qualità dell'acqua sono considerati reati se sono commessi intenzionalmente, temerariamente o per negligenza grave".

- Articolo 5-*ter*:

"*Istigazione, favoreggiamento e concorso*

Gli Stati membri provvedono affinché l'istigazione a commettere gli atti intenzionali di cui all'articolo 5 bis, paragrafi 1 e 3, o il favoreggiamento e il concorso nel commetterli siano punibili come reati".

- Art. 8-*ter*:

"*Responsabilità delle persone giuridiche*

1. Ciascuno Stato membro adotta le misure necessarie affinché le persone giuridiche possano essere ritenute responsabili dei reati di cui all'articolo 5 bis, paragrafi 1 e 3, e all'articolo 5 ter, commessi a loro vantaggio da

(i) sussiste la giurisdizione italiana in relazione allo sversamento di idrocarburi e/o altre sostanze inquinanti effettuato in acque territoriali da parte di nave battente qualsiasi bandiera;
(ii) sussiste la giurisdizione italiana in relazione allo sversamento di idrocarburi e/o altre sostanze inquinanti causato al di fuori delle acque territoriali da nave battente bandiera italiana;
(iii) sussiste la giurisdizione italiana in relazione allo sversamento di idrocarburi e/o altre sostanze inquinanti causato al di fuori delle acque territoriali da nave battente bandiera non italiana qualora, ad esempio, il proprietario o l'armatore, che abbiano concorso a causare il reato, siano italiani.

La giurisdizione italiana potrebbe essere ravvisata anche nel caso in cui le conseguenze del reato si siano verificate in Italia, ancorché lo sversamento sia stato effettuato da nave battente bandiera straniera al di fuori delle acque territoriali italiane. Infatti, ai sensi dell'art. 6 c.p. "*il reato si considera commesso nel territorio dello Stato, quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi verificato l'evento che è la conseguenza dell'azione od omissione*".

5.2 Le sanzioni previste a carico dell'ente in relazione ai reati ambientali

L'art. 25-*undecies* del Decreto prevede che per i reati sopra analizzati siano inflitte all'ente le seguenti sanzioni:

(i) in relazione al reato di uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette di cui all'articolo 727-*bis* c.p.:
   - una sanzione pecuniaria fino a 250 quote (dove ciascuna quota corrisponde ad un importo variabile fra un minimo di € 258,22 ad un massimo di € 1.549,37);

(ii) in relazione al reato di distruzione o deterioramento di habitat all'interno di un sito protetto di cui all'art. 733-*bis* c.p.:
   - una sanzione pecuniaria da 150 a 250 quote;

(iii) in relazione ai reati in tema di scarichi di acque reflue industriali di cui all'art. 137, commi 3, 5, primo periodo, e 13 del d.lgs. 152/2006:
   - una sanzione pecuniaria da 150 a 250 quote;

(iv) in relazione ai reati in tema di scarichi di acque reflue industriali di cui all'art. 137 commi 2, 5, secondo periodo, e 11 del d.lgs. 152/2006:
   - una sanzione pecuniaria da 200 a 300 quote;
   - in caso di condanna, la sanzione interdittiva per una durata non superiore a 6 mesi;

(v) in relazione ai reati in tema di attività di gestione di rifiuti non autorizzata di cui all'art. 256, commi 1, lettera a), e 6, primo periodo del d.lgs. 152/2006:
   - una sanzione pecuniaria fino a 250 quote (ovvero la metà nel caso di commissione del reato di cui all'articolo 256, comma 4, del d.lgs. 152/2006);

---

persone fisiche che agiscano a titolo individuale o in quanto membri di un organo della persona giuridica e che detengano una posizione preminente in seno alla persona giuridica, basata:
a) sul potere di rappresentanza della persona giuridica;
b) sul potere di prendere decisioni per conto della persona giuridica; oppure
c) sull'esercizio del controllo in seno a tale persona giuridica.
2. Ciascuno Stato membro provvede inoltre a che la persona giuridica possa essere ritenuta responsabile quando la carenza di sorveglianza o controllo da parte delle persone fisiche di cui al paragrafo 1 abbia reso possibile commettere un reato di cui all'articolo 5 bis, paragrafi 1 e 3, e all'articolo 5 ter a vantaggio della persona giuridica stessa da parte di una persona fisica soggetta alla sua autorità.
3. La responsabilità della persona giuridica ai sensi dei paragrafi 1 e 2 non esclude azioni penali contro le persone fisiche che abbiano commesso reati di cui all'articolo 5 bis, paragrafi 1 e 3, e all'articolo 5 ter, che abbiano istigato qualcuno a commetterli o vi abbiano concorso".

(vi) in relazione ai reati in tema di attività di gestione di rifiuti non autorizzata di cui all'art. 256, commi 1, lettera b), 3, primo periodo, e 5 del d.lgs. 152/2006:

- una sanzione pecuniaria da 150 a 250 quote (ovvero la metà nel caso di commissione del reato di cui all'articolo 256, comma 4, del d.lgs. 152/2006);

(vii) in relazione ai reati in tema di attività di gestione di rifiuti non autorizzata di cui all'art. 256, comma 3, secondo periodo del d.lgs. 152/2006:

- una sanzione pecuniaria da 200 a 300 quote (ovvero la metà nel caso di commissione del reato di cui all'articolo 256, comma 4, del d.lgs. 152/2006);
- in caso di condanna, la sanzione interdittiva per una durata non superiore a 6 mesi;

(viii) in relazione ai reati in tema di bonifica dei siti di cui all'articolo 257 , comma 1 del d.lgs. 152/2006:

- una sanzione pecuniaria fino a 250 quote;

(ix) in relazione ai reati in tema di bonifica dei siti di cui all'articolo 257, comma 2 del d.lgs. 152/2006:

- la sanzione pecuniaria da 150 a 250 quote;

(x) in relazione ai reati in tema di violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari di cui all'articolo 258, comma 4, secondo periodo del d.lgs. 152/2006:

- la sanzione pecuniaria da 150 a 250 quote;

(xi) in relazione al reato di traffico illecito di rifiuti di cui all'articolo 259, comma 1, del d.lgs. 152/2006:

- una sanzione pecuniaria da 150 a 250 quote;

(xii) in relazione al delitto di attività organizzate per il traffico illecito di rifiuti di cui all'articolo 260, comma 1 del d.lgs. 152/2006:

- una sanzione pecuniaria da 300 a 500 quote;
- in caso di condanna, la sanzione interdittiva per una durata non superiore a 6 mesi;
- se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione del reato, la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16, comma 3, del d.lgs. 231/2001;

(xiii) in relazione al delitto di attività organizzate per il traffico illecito di rifiuti di cui all'articolo 260, comma 2 del d.lgs. 152/2006:

- una sanzione pecuniaria da 400 a 800 quote;
- in caso di condanna, la sanzione interdittiva per una durata non superiore a 6 mesi;
- se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione del reato, la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16, comma 3, del d.lgs. 231/2001;

(xiv) in relazione ai reati relativi al SISTRI, di cui all'articolo 260-*bis*, commi 6, 7, secondo e terzo periodo, e 8, primo periodo del d.lgs. 152/2006:

- una sanzione pecuniaria da 150 a 250 quote;

(xv) in relazione ai reati relativi al SISTRI, di cui all'articolo 260-*bis*, comma 8, secondo periodo del d.lgs. 152/2006:

- una sanzione pecuniaria da 200 a 300 quote;

(xvi) in relazione al reato in tema di emissioni in atmosfera di cui all'articolo 279, comma 5 del d.lgs. 152/2006:

- una sanzione pecuniaria fino a 250 quote.

(xvii) in relazione ai reati relativi alla tutela della specie animali e vegetali in via di estinzione di cui all'art. 1, comma 1, all'art. 2, commi 1 e 2, e all'art. 6, comma 4, della L. 150/1992:

- una sanzione pecuniaria fino a 250 quote;

(xviii) in relazione al reato relativo alla tutela della specie animali e vegetali in via di estinzione di cui all'art. 1, comma 2 della L. 150/1992:

- una sanzione pecuniaria da 150 a 250 quote;

(xix) in relazione ai reati relativi alla tutela della specie animali e vegetali in via di estinzione di cui all'art. 3-*bis*, comma 1 della L. 150/1992:

- una sanzione pecuniaria fino a 250 quote, in caso di commissione di reati per cui è prevista la pena non superiore nel massimo ad anni 1 di reclusione;
- una sanzione pecuniaria da 150 a 250 quote, in caso di commissione di reati per cui è prevista la pena non superiore nel massimo ad anni 2 di reclusione;
- una sanzione pecuniaria da 200 a 300 quote, in caso di commissione di reati per cui è prevista la pena non superiore nel massimo ad anni 3 di reclusione;
- una sanzione pecuniaria da 300 a 500 quote, in caso di commissione di reati per cui è prevista la pena superiore nel massimo ad anni 3 di reclusione;

(xx) in relazione ai reati relativi alla tutela dell'ozono atmosferico e dell'ambiente di cui all'art. 3, comma 6, della L. 549/1993:

- una sanzione pecuniaria da 150 a 250 quote;

(xxi) in relazione al reato in tema di inquinamento colposo provocato dalle navi di cui all'art. 9, comma 1 del d.lgs. 202/2007:

- una sanzione pecuniaria fino a 250 quote;

(xxii) in relazione ai reati in tema di inquinamento colposo provocato dalle navi di cui all'art. 9, comma 2 del d.lgs. 202/2007:

- una sanzione pecuniaria da 150 a 250 quote;
- in caso di condanna, la sanzione interdittiva per una durata non superiore a 6 mesi;

(xxiii) in relazione ai reati in tema di inquinamento doloso provocato dalle navi di cui all'art. 8, comma 1 del d.lgs. 202/2007:

- una sanzione pecuniaria da 150 a 250 quote;
- in caso di condanna, la sanzione interdittiva per una durata non superiore a 6 mesi;
- se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione del reato, la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16, comma 3, del d.lgs. 231/2001;

(xxiv) in relazione al reato in tema di inquinamento doloso provocato dalle navi di cui all'art. 8, comma 2 del d.lgs. 202/2007:

- una sanzione pecuniaria da 200 a 300 quote;
- in caso di condanna, la sanzione interdittiva per una durata non superiore a 6 mesi;
- se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente di consentire o agevolare la commissione del reato, la sanzione dell'interdizione definitiva dall'esercizio dell'attività ai sensi dell'art. 16, comma 3, del d.lgs. 231/2001.

5.3 Le attività individuate come sensibili ai fini del d.lgs. 231/2001 con riferimento ai reati ambientali

L'analisi dei processi aziendali della Società ha consentito di individuare le attività nel cui ambito potrebbero astrattamente essere realizzate le fattispecie di reato richiamate dall'art. 25-*undecies* del d.lgs. 231/2001.

1. Attività sensibili relative ai reati in tema di attività di gestione di rifiuti in violazione dell'art. 256, comma 1, lett. a) e b) d.lgs. 152/2006.

   Tale fattispecie punisce una vasta serie di comportamenti illeciti ricollegabili alla c.d. "gestione" (raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione) di "rifiuti", ovvero di ogni "*sostanza od oggetto di cui il detentore si disfi o abbia l'intenzione o l'obbligo di disfarsi*".

   Le condotte astrattamente realizzabili dalla Società potrebbero essere le seguenti, a titolo esemplificativo e non esaustivo.

   a. raccolta e trasporto di rifiuti, anche propri, in assenza di iscrizione all'Albo Nazionale dei Gestori Ambientali (salvo i casi in cui l'iscrizione è sostituita dalla relativa comunicazione);
   b. detenzione di rifiuti (in particolare da parte del loro produttore) senza autorizzazione al deposito o allo stoccaggio o in violazione dei limiti di legge al deposito temporaneo (art. 183, comma 1, lett. bb) d.lgs. 152/2006);
   c. erronea attribuzione di codifica del rifiuto nell'operazione di caratterizzazione (anche in caso di assenza di analisi, ove richieste, come nel caso di rifiuti con codici a specchio), laddove si tratti di errore non materiale;
   d. raccolta, trasporto, acquisto, vendita, commercializzazione, intermediazione, deposito, stoccaggio, impiego nell'attività produttiva di "sottoprodotti" in violazione dei requisiti di legge *ex* art. 184-*bis* d.lgs. 152/2006;
   e. raccolta, trasporto, acquisto, vendita, commercializzazione, intermediazione, deposito, stoccaggio, impiego nell'attività produttiva di "materie prime secondarie" o "End of Waste" in violazione dei requisiti di legge *ex* art. 184-*ter* d.lgs. 152/2006;
   f. consegna di rifiuti a trasportatore non autorizzato e/o non iscritto all'Albo Nazionale dei Gestori Ambientali (in concorso con quest'ultimo) o con iscrizione scaduta o con mezzi non contemplati nel provvedimento di iscrizione all'Albo;
   g. conferimento di rifiuti a soggetto non autorizzato o privo di formulario (in concorso con quest'ultimo);
   h. inadempimento obblighi documentali di legge da parte del produttore dei rifiuti (MUD; c.d. "MUDINO"; registro di carico e scarico dei rifiuti; formulario di trasporto dei rifiuti);
   i. violazione delle modalità semplificate di raccolta e trasporto dei Rifiuti da Apparecchiature Elettriche ed Elettroniche ("RAEE") di cui al Decreto Legislativo 25 luglio 2005, n. 151 ed al D.M. 8 marzo 2010, n. 65;
   j. trasporto ai centri di raccolta dei RAEE su base più ampia di quella mensile ovvero per un quantitativo superiore a 3500 Kg; raggruppamento dei RAEE in luogo non idoneo o accessibile a terzi o non pavimentato; mancata protezione dei RAEE dalle acque meteoriche e dall'azione del vento; mancata salvaguardia dell'integrità dei RAEE;
   k. trasporto di un quantitativo di RAEE superiore a 3500 kg, effettuato con automezzi con portata superiore a 3500 kg e massa complessiva superiore a 6000 kg;
   l. inadempimento obblighi documentali di legge da parte dei distributori e dei trasportatori dei RAEE (registro di carico e scarico dei rifiuti, documento di trasporto e schedario prescritti dal D.M. 65/2010);

   il tutto con riferimento a qualsiasi tipologia di rifiuto, compresi i RAEE.

2. Attività sensibili relative ai reati in tema di attività di gestione di rifiuti in violazione dell'art. 256, comma 3, d.lgs. 152/2006.

Nell'ambito del reato di cui all'art. 256, comma 3, d.lgs. 152/2006, sono ritenute rilevanti ai fini della costruzione del Modello le seguenti attività:

a. realizzazione di discarica di rifiuti (tramite destinazione e allestimento di area con effettuazione -di norma- delle opere occorrenti);
b. gestione di discarica di rifiuti (mediante apprestamento di organizzazione di persone, cose e macchine) diretta al funzionamento della discarica in assenza di autorizzazione;
c. realizzazione e gestione (con le modalità di cui sopra) di discarica di rifiuti destinata, anche in parte, allo smaltimento di rifiuti pericolosi;
d. attività di deposito preliminare di rifiuti prolungata oltre i 12 mesi;

il tutto anche sotto forma di contributo, attivo o passivo, diretto a realizzare o anche semplicemente a tollerare lo stato di fatto che costituisce reato.

3. Attività sensibili relative ai reati in tema di attività di gestione di rifiuti in violazione dell'art. 256, comma 4, d.lgs. 152/2006.

Nell'ambito del reato di cui all'art. 256, comma 4, d.lgs. 152/2006, è ritenuta rilevante ai fini della costruzione del Modello la seguente attività:

a. svolgimento delle attività di raccolta e trasporto di rifiuti (ad esempio con mezzi diversi da quelli comunicati), di bonifica di siti, di bonifica dei beni contenenti amianto, di commercio e intermediazione di rifiuti senza detenzione, avendo adempiuto all'obbligo di iscrizione o comunicazione all'Albo Nazionale dei Gestori Ambientali ma in assenza delle condizioni previste all'art. 214;

4. Attività sensibili relative ai reati in tema di attività di gestione di rifiuti in violazione dell'art. 256, comma 5, d.lgs. 152/2006.

Nell'ambito del reato di cui all'art. 256, comma 5, d.lgs. 152/2006, sono ritenute rilevanti ai fini della costruzione del Modello le seguenti attività:

a. miscelazione o diluizione di rifiuti pericolosi con rifiuti non pericolosi, ad esempio nel deposito temporaneo o durante il trasporto (senza autorizzazione);
b. miscelazione o diluizione di rifiuti pericolosi con diverse caratteristiche di pericolosità, ad esempio nel deposito temporaneo o durante il trasporto (senza autorizzazione).

5. Attività sensibili relative ai reati in tema di attività di gestione di rifiuti in violazione dell'art. 256, comma 6, d.lgs. 152/2006.

Nell'ambito del reato di cui all'art. 256, comma 6, d.lgs. 152/2006, sono ritenute rilevanti ai fini della costruzione del Modello le seguenti attività:

a. deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi (ad esempio rifiuti contaminati da sangue o altri materiali biologici o che provengano da ambienti di isolamento infettivo) presso il luogo di produzione (reato tipico per strutture ospedaliere, cliniche, cimiteri, centri estetici, parrucchieri).

6. Attività sensibili relative ai reati in tema di bonifica di siti contaminati di cui all'art. 257, commi 1 e 2, d.lgs. 152/2006.

L'art. 25-*undecies*, comma 2 lett. c) del Decreto contempla i reati di cui all'art. 257, commi 1 e 2 del d.lgs. 152/2006 conseguenti all'inquinamento del suolo, del sottosuolo, delle acque superficiali e delle acque sotterranee.

Nell'ambito del reato di cui all'art. 257, comma 1 e 2, d.lgs. 152/2006, sono ritenute rilevanti ai fini della costruzione del Modello le seguenti attività:

a. omessa comunicazione di un evento potenzialmente in grado di contaminare il sito da parte del responsabile dell'evento stesso, a prescindere dal superamento delle concentrazioni soglia di contaminazione (CSC);
b. omessa presentazione o adempimento al piano di caratterizzazione ovvero compimento di altre attività che impediscano la formazione del progetto di bonifica;
c. mancata esecuzione delle attività di bonifica (comunque denominate) in conformità con il progetto approvato dall'autorità da parte di chi abbia cagionato l' inquinamento di suolo, sottosuolo, acque superficiali o sotterranee con superamento delle concentrazioni soglia di rischio (CSR);

ma anche, in via tuzioristica, l'omessa comunicazione del rinvenimento di contaminazione storica, da parte del proprietario o del gestore dell'area (in quanto tenuti a impedire la diffusione della contaminazione) o del responsabile dell'inquinamento, a prescindere dal superamento delle concentrazioni soglia di contaminazione (CSC).

7. Attività sensibili relative al reato di violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari di cui all'art. 258, comma 4, d.lgs. 152/2006

I reati contemplati dall'art. 25-*undecies*, comma 2 lett. d) del Decreto riguardano la predisposizione e l'utilizzo di certificati di analisi dei rifiuti falsi durante il trasporto.

Nell'ambito del reato di cui all'art. 258, comma 4, d.lgs. 152/2006, sono ritenute rilevanti ai fini della costruzione del Modello le seguenti attività:

a. effettuazione delle operazioni di campionamento dei rifiuti da analizzare in modo tale da non assicurare la rappresentatività del campione;
b. redazione di certificati contenenti dati falsi (ad esempio relativi al ciclo di produzione di rifiuti o alle loro caratteristiche chimiche);

In ogni caso, deve trattarsi di soggetti che non abbiano l'obbligo di adesione o non abbiano aderito su base volontaria al SISTRI.

8. Attività sensibili relative al reato di traffico illecito di rifiuti di cui all'art. 259, comma 1, d.lgs. 152/2006.

Nell'ambito dei reati di cui all'art. 259, comma 1 del d.lgs. 152/2006 in tema di spedizione transfrontaliera di rifiuti effettuata in base al regolamento (CE) n. 1013/2006 del 4 giugno 2006, sono ritenute rilevanti ai fini della costruzione del Modello le seguenti attività:

a. spedizione transfrontaliera di rifiuti effettuata senza che la notifica prevista dal Regolamento (CEE) 259/93 (oggi: 1013/2006) sia stata inviata a tutte le autorità competenti o in base a notifica (gravemente) infedele;
b. spedizione transfrontaliera di rifiuti effettuata senza il consenso delle autorità competenti o avendone ottenuto il consenso mediante falsificazioni, false dichiarazioni o frode;
c. spedizione transfrontaliera di rifiuti effettuata senza (concreta) specifica dei rifiuti nel documento di accompagnamento;
d. spedizione transfrontaliera di rifiuti che comporti uno smaltimento o un recupero in violazione del documento di accompagnamento;
e. violazione dell'art. 14 del Regolamento 259/93 (oggi: 1013/2006), che regola le esportazione dei rifiuti destinati allo smaltimento verso i paesi EFTA e vieta

l'esportazione di rifiuti destinati allo smaltimento verso i paesi extra-CE;

f. violazione dell'art. 16 del Regolamento 259/93 (oggi: 1013/2006), che regola le esportazioni di determinati rifiuti destinati al recupero verso i paesi OCSE o aderenti alla Convenzione di Basilea che hanno raggiunto un accordo con la Comunità;

g. violazione dell'art. 19 del Regolamento 259/93 (oggi: 1013/2006), che regola le importazioni di rifiuti destinati allo smaltimento da paesi EFTA aderenti alla Convenzione di Basilea e da altri paesi;

h. violazione dell'art. 21 del Regolamento 259/93 (oggi: 1013/2006), che regola le importazioni nella Comunità di rifiuti destinati al recupero ai paesi OCSE e da altri paesi;

i. spedizione di rifiuti i cui all'allegato II del regolamento 259/93 (oggi: 1013/2006) in violazione dell'art. 1, comma 3 lett. a) b), c) e d);

l. spedizione di sottoprodotti o di materie prime secondarie / End of Waste in assenza dei requisiti prescritti dalla legge nazionale e comunitaria.

9. Attività sensibili relative al reato di attività organizzate per il traffico illecito di rifiuti di cui all'art. 260, d.lgs. 152/2006.

L'art. 25-*undecies*, comma 2, lettera g), del Decreto punisce coloro che svolgono attività organizzate relative al traffico illecito di rifiuti in violazione dell'art. 260 del d.lgs. 152/2006.

Nell'ambito di tale reato, è ritenuta rilevante ai fini della costruzione del Modello la seguente attività:

a. svolgimento di attività di gestione (ad esempio, raccolta, trasporto, commercio, intermediazione, recupero o smaltimento) di rifiuti, in violazione delle norme di legge, attraverso condotte ripetute che, nel loro complesso, abbiano ad oggetto un ingente quantitativo di rifiuti.

10. Attività sensibili relative ai reati connessi al Sistema informatico di controllo della tracciabilità dei rifiuti di cui all'art. 260-*bis*, comma 6, d.lgs. 152/2006.

L'art. 25-*undecies*, comma 2, lettera g), del Decreto include tra i reati ambientali suscettibili di configurare una responsabilità amministrativa degli enti quelli di cui all'art. 260-*bis*, comma 6, in relazione al sistema informatico di controllo della tracciabilità dei rifiuti ("SISTRI").

Nell'ambito dei reati predetti, sono ritenute rilevanti ai fini della costruzione del Modello le seguenti attività, effettuate nell'ambito di operatività del SISTRI:

a. effettuazione delle operazioni di campionamento dei rifiuti da analizzare in modo tale da non assicurare la rappresentatività del campione;

b. predisposizione di un certificato di analisi recante false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti (indipendentemente dalla qualifica di pericolosità di questi);

c. inserimento di certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti (indipendentemente dalla qualifica di pericolosità di questi).

11. Attività sensibili relative ai reati in tema di cessazione e riduzione dell'impiego delle sostanze lesive a tutela dell'ozono stratosferico e dell'ambiente di cui all'art. 3, comma 6, L. 549/1993.

L'art. 25-*undecies*, comma 4, del Decreto concerne i reati in tema di violazione della normativa di cui all'art. 3, comma 6 della L. 549/1993, prevista a tutela dell'ozono.

Nell'ambito dei reati predetti, sono ritenute rilevanti ai fini della costruzione del Modello le seguenti attività sensibili:

a. possesso o utilizzazione di attrezzature quali frigoriferi, impianti di climatizzazione, celle frigorifere o altri nei quali siano utilizzate le sostanze lesive per l'ozono (in particolare CFC, CFC completamente alogenati, halon, tetracloruro di carbonio, metilcloroformio, bromuro di metile, idrobromurocloroﬂuorocarburi e idroclorofluorocarburi, quali i gruppi da 1 a 8 dell'allegato 1 Regolamento 1005/2009/CE);

b. produzione, anche involontaria, di sostanze lesive per l'ozono di cui al precedente punto a);

c. uso di sostanze lesive per l'ozono di cui al precedente punto a), ad eccezione di quelle contenute in prodotti e apparecchiature;

d. produzione, immissione sul mercato o uso di sistemi di protezione antincendio ed estintori contenenti halon, fatta eccezione per i casi di usi critici autorizzati.

5.4 Il sistema dei controlli per l'adempimento degli obblighi in materia ambientale

Il sistema dei controlli adottati dalla Società a presidio delle attività aventi un impatto anche solo potenziale sull'ambiente sono assicurati da un articolato insieme di protocolli generali e specifici di seguito descritti.

Tali protocolli sono stati recepiti dalla Società nell'ambito delle procedure indicate nell'Allegato n. 6.

5.4.1 Il Sistema di Gestione HSE per l'ambiente

La Società è dotata del Sistema di Gestione HSE che, peraltro è stato adottato anche da diverse altre società del gruppo Huawei a livello europeo, al fine di assicurare i più elevati standard di tutela nelle aree considerate.

Tale Sistema, in relazione all'area ambientale, è stato certificato in conformità allo standard ISO 14001:2004.

Come noto, lo standard ISO 14001:2004 stabilisce quali sono i criteri per un Sistema di Gestione dell'ambiente volti a consentire all'Organizzazione aziendale di sviluppare una politica e degli obiettivi che tengono in considerazione i requisiti normativi e le informazioni sugli aspetti ambientali significativi ("*This International Standard specifies requirements for an environmental management system to enable an organization to develop and implement a policy and objectives which take into account legal requirements and information about significant environmental aspects*").

Il Sistema di Gestione HSE comprende, in primo luogo, il Manuale del Sistema di Gestione HSE ("*Huawei Europe EHS Management Manual*"), il quale, oltre ad una descrizione generale dell'organizzazione aziendale e della politica interna in materia di salute e sicurezza nonché di ambiente, dedica specifica attenzione agli argomenti della pianificazione, realizzazione e verifica del Sistema stesso, ivi compreso il riesame della direzione.

Oltre al predetto Manuale, la Società è dotata di un articolato insieme di procedure volte a presidiare lo svolgimento delle attività aventi un impatto, anche solo potenziale, sulla salute e la sicurezza nei luoghi di lavoro. Ulteriori documenti ed elaborati sono di volta in volta richiamati nelle procedure cui afferiscono.

Tutti i documenti che compongono il Sistema di Gestione HSE sono resi disponibili, in formato cartaceo, presso la funzione Quality ed altresì, in formato elettronico, all'interno della rete intranet aziendale così da essere facilmente accessibili a tutti gli interessati.

Le procedure sono inoltre caratterizzate dall'individuazione della data di prima emissione e dalla traccia delle revisioni apportate.

Il Sistema di Gestione HSE (così come di volta in volta integrato da altri sistemi di gestione, quali ad esempio, il sistema della qualità) reca inoltre i protocolli di controllo generali e specifici utili per assicurare e, quindi, verificare che le attività sensibili ritenute rilevanti, singolarmente ed unitariamente considerate, si svolgano nel rispetto di quanto previsto dalla normativa applicabile.

5.4.2 Protocolli di controllo generali relativi alle attività sensibili

I protocolli di controllo di carattere generale da considerare e applicare con riferimento a tutte le attività sensibili sopra individuate sono:

- ***Business Code of Conduct di Huawei***: si tratta di un insieme di enunciazioni e precetti che definiscono i principi di comportamento e le modalità operative da osservare per lo svolgimento di tutte le attività sensibili (oltre che per altre attività aziendali in genere) e che devono essere osservati da tutti i soggetti a qualunque titolo coinvolti nelle attività di Huawei.
- ***la Politica HSE di Huawei*** in base alla quale si definiscono le modalità con la quale la stessa viene dalla direzione aziendale (i) documentata, attuata e mantenuta nel tempo; (ii) comunicata a tutti i dipendenti affinché gli stessi siano coscienti dei loro obblighi individuali in tema di tutela dell'ambiente; (iii) resa disponibile alle parti interessate e (iv) riesaminata per accertarne la sua continua idoneità, in occasione dei riesami dei Sistemi di Gestione da parte della direzione ed ad ogni modifica significativa degli stessi.

5.4.3 Protocolli di controllo preventivo generici relativi alle attività sensibili

I protocolli di controllo preventivo generici applicati da Huawei al fine di prevenire la commissione delle fattispecie di reato sopra identificate (nonché alle parallele attività sensibili identificate nell'ambito del Sistema di Gestione con riferimento alla salute e sicurezza sul lavoro) sono:

- ***Definizione della struttura organizzativa e individuazione dei soggetti e delle responsabilità:*** il Huawei Europe EHS Management Manual, definisce le risorse incaricate di attuare, mantenere attivo e migliorare il Sistema di Gestione HSE;
- ***Definizione del metodo, dei criteri e delle modalità di identificazione degli aspetti ambientali***: la Società identifica gli aspetti ambientali, anche pericolosi, e ne valuta l'influenza in considerazione –tra l'altro– della loro significatività, frequenza e durata anche in applicazione di quanto previsto dalla procedura;
- ***Istituzione di un programma continuativo di formazione ed addestramento dei lavoratori***: finalizzato ad educare ed addestrare tutto il personale aziendale affinché possa acquisire particolare consapevolezza, capacità e competenze in materia ambientale, così come meglio disciplinato dalla procedura;
- ***Definizione delle regole di comunicazione interne***: tali regole sono volte ad assicurare che i diversi livelli e le diverse funzioni dell'organizzazione ricevano le informazioni ambientali di competenza o di interesse e le trasmettano a loro volta a chi di competenza o di interesse, in aderenza a quanto previsto dalla procedura;
- ***Identificazione delle Procedure di Registrazione ed Archiviazione***: la Società raccoglie e conserva tutta la documentazione relativa all'ambiente sia ai fini del miglior

funzionamento del Sistema di Gestione HSE sia per migliorare l'efficienza del Sistema stesso, avvalendosi in particolare della procedura.

5.4.4 Protocolli di controllo preventivo specifici relativi alle attività sensibili

Per tutte le attività sensibili sopra elencate, oltre ai protocolli di controllo generali ed ai protocolli di controllo preventivo generici, la Società ha predisposto i seguenti protocolli di controllo preventivo specifici:

I Individuazione e rivalutazione periodica delle prescrizioni normative applicabili a ciascuna attività e processo a rischio di violazione ambientale.

II Definizione delle modalità di gestione operativa di ogni attività o processo avente potenziale impatto ambientale, ivi inclusa la gestione delle emergenze, effettuata tramite la costruzione di procedure e istruzioni operative ad hoc.

III Verifica della congruità delle modalità di gestione operativa di ogni altra attività che -pur non direttamente rilevanti ai fini della commissione di reati ambientali- potrebbero essere prodromiche o strumentali a questi (es: procedura gestione accessi informatici in relazione agli adempimenti SISTRI).

IV Estensione del "controllo operativo" alle persone che "operano per conto" dell'organizzazione.

Tali protocolli di controllo preventivo specifici sono stati ulteriormente precisati in relazione a ciascun insieme di attività sensibili relative alla fattispecie di reato di volta in volta considerata, così come di seguito indicato.

Relativamente alle attività sensibili di cui al n. **1** del precedente paragrafo 5.3, **concernenti i reati in tema di gestione non autorizzata di rifiuti di cui all'art. 256, comma 1, lett. a) e b), d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare e avere accesso alle prescrizioni legali applicabili, ivi incluse quelle contenute in atti autorizzativi.

2. Procedura progettazione nuovi impianti o modifica impianti esistenti: formalizzazione di una procedura volta ad accertare che in sede di progettazione e acquisto di impianti nuovi (o sezioni modificative di impianti esistenti) siano tenute in considerazione le prescrizioni legali.

3. Procedura controllo documenti: formalizzazione di una procedura volta ad assicurare che la documentazione attinente alle autorizzazioni sia aggiornata e distribuita o accessibile a tutti gli interessati.

4. Procedura sorveglianza e misurazione delle prestazioni ambientali: formalizzazione di una procedura volta a pianificare ed attuare i controlli richiesti dalla normativa e dai provvedimenti autorizzatori.

5. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse ed aggiornate le dovute procedure ed istruzioni operative (e tra queste la procedura gestione rifiuti, estesa alla gestione del deposito temporaneo).

6. Procedura valutazione fornitori: formalizzazione di una procedura volta a definire le modalità di qualifica ambientale dei fornitori di servizi generali, di servizi di

manutenzione, di impianti e macchine, di analisi e prove di laboratorio, di materiali classificati pericolosi, di prestazioni nel campo della gestione dei rifiuti, e, in generale, dei terzi le cui attività possono avere un impatto ambientale.

7. Procedura appalti: formalizzazione di una procedura volta a verificare che non sia oggetto di appalto l'attività di gestione di rifiuti per la quale l'appaltatore non possieda regolare autorizzazione o abbia adempiuto agli obblighi di iscrizione o comunicazione e per verificare la predisposizione di adeguate clausole di salvaguardia in sede di negoziazione dei contratti aventi ad oggetto attività potenzialmente comportanti un impatto sull'ambiente.

Relativamente alle attività sensibili di cui al n. **2** del precedente paragrafo 5.3, **concernenti i reati in tema di discarica di rifiuti non autorizzata di cui all'art. 256, comma 3, d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare ed avere accesso alle prescrizioni legali applicabili, ivi incluse quelle contenute in atti autorizzativi.
2. Procedura controllo documenti: formalizzazione di una procedura volta ad assicurare che la documentazione attinente alle autorizzazioni sia aggiornata e distribuita o accessibile a tutti gli interessati.
3. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse ed aggiornate le dovute Procedure e Istruzioni Operative (e tra queste la procedura gestione rifiuti).
4. Procedura sorveglianza e misurazione delle prestazioni ambientali: formalizzazione di una procedura volta a pianificare ed attuare i controlli richiesti dalla normativa e dai provvedimenti autorizzatori.
5. Procedura progettazione nuovi impianti o modifica impianti esistenti: formalizzazione di una procedura volta ad accertare che in sede di progettazione e acquisto di impianti nuovi (o sezioni modificative di impianti esistenti) siano tenute in considerazione le prescrizioni legali.
6. Procedura valutazione fornitori: formalizzazione di una procedura volta a definire le modalità di qualifica ambientale dei fornitori di servizi generali, di servizi di manutenzione, di impianti e macchine, di analisi e prove di laboratorio, di materiali classificati pericolosi, di prestazioni nel campo della gestione dei rifiuti, e, in generale, dei terzi le cui attività possono avere un impatto ambientale.
7. Procedura appalti: formalizzazione di una procedura volta a verificare la predisposizione di adeguate clausole di salvaguardia in sede di negoziazione dei contratti aventi ad oggetto attività potenzialmente comportanti un impatto sull'ambiente.

Relativamente alle attività sensibili di cui al n. **3** del precedente paragrafo 5.3, **concernenti i reati in tema di inosservanza delle prescrizioni autorizzative e carenza dei requisiti e condizioni richiesti per le iscrizioni e comunicazioni di cui all'art. 256, comma 4, d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare e avere accesso alle prescrizioni legali applicabili, ivi

incluse quelle contenute in atti autorizzativi.

2. Procedura controllo documenti: formalizzazione di una procedura volta ad assicurare che la documentazione attinente alle autorizzazioni, iscrizioni e comunicazioni in materia di rifiuti sia aggiornata e distribuita o accessibile a tutti gli interessati.
3. Procedura sorveglianza e misurazione delle prestazioni ambientali: formalizzazione di una procedura volta a pianificare ed attuare i controlli richiesti dalla normativa e dai provvedimenti autorizzatori.
4. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse ed aggiornate le dovute Procedure e Istruzioni Operative (e tra queste la procedura gestione rifiuti, articolata nelle varie operazioni condotte dall'ente interessato).

Relativamente alle attività sensibili di cui al n. **4** del precedente paragrafo 5.3, **concernenti i reati in tema di miscelazione non consentita di rifiuti di cui all'art. 256, comma 5, d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare e avere accesso alle prescrizioni legali applicabili, ivi incluse quelle contenute in atti autorizzativi.
2. Procedura controllo documenti: formalizzazione di una procedura volta ad assicurare che la documentazione attinente alle autorizzazioni, iscrizioni e comunicazioni in materia di rifiuti sia aggiornata e distribuita o accessibile a tutti gli interessati.
3. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse ed aggiornate le dovute Procedure e Istruzioni Operative (e tra queste la procedura gestione rifiuti).
4. Procedura sostanze pericolose: formalizzazione di una procedura volta ad assicurare la corretta gestione di sostanze, miscele e/o articoli che possono risultare nocive per l'ambiente.

Relativamente alle attività sensibili di cui al n. **5** del precedente paragrafo 5.3, **concernenti i reati in tema di deposito temporaneo di rifiuti sanitari pericolosi di cui all'art. 256, comma 6, d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare e avere accesso alle prescrizioni legali applicabili, ivi incluse quelle contenute in atti autorizzativi.
2. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse ed aggiornate le dovute Procedure e Istruzioni Operative (e tra queste la procedura gestione rifiuti).
3. Procedura valutazione fornitori: formalizzazione di una procedura volta a definire le modalità di qualifica ambientale dei fornitori di servizi generali, di servizi di manutenzione, di impianti e macchine, di analisi e prove di laboratorio, di materiali classificati pericolosi, di prestazioni nel campo della gestione dei rifiuti, e, in generale, dei terzi le cui attività possono avere un impatto ambientale.
4. Procedura appalti: formalizzazione di una procedura volta a verificare la predisposizione di adeguate clausole di salvaguardia in sede di negoziazione dei contratti aventi ad oggetto

attività potenzialmente comportanti un impatto sull'ambiente.

5. Procedura sostanze pericolose: formalizzazione di una procedura volta ad assicurare la corretta gestione di sostanze, miscele e/o articoli che possono risultare nocive per l'ambiente.

Relativamente alle attività sensibili di cui al n. **6** del precedente paragrafo 5.3, **concernenti i reati in tema di bonifica dei siti di cui all'art. 257, commi 1 e 2, d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura gestione delle emergenze: formalizzazione di una procedura volta ad identificare, gestire e limitare le conseguenze di eventi che potrebbero comportare inquinamento del suolo, delle acque o dell'aria.
2. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare ed avere accesso alle prescrizioni legali applicabili, ivi incluse quelle contenute nella approvazione del piano di bonifica e nelle relative autorizzazioni.
3. Procedura controllo documenti: formalizzazione di una procedura volta ad assicurare che la documentazione attinente alle comunicazioni alle autorità, alle approvazioni del piano di bonifica e alle relative autorizzazioni sia aggiornata e distribuita o accessibile a tutti gli interessati
4. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse le Procedure e Istruzioni Operative volte a far sì che siano pianificate, attuate e condotte, nelle condizioni specificate dalle prescrizioni legali applicabili, tutte le attività necessarie o utili, anche sotto il profilo tecnico, al rispetto delle prescrizioni legali applicabili.
5. Procedura valutazione fornitori: formalizzazione di una procedura volta a definire le modalità di qualifica ambientale dei fornitori di servizi, di impianti e macchine, di analisi e prove di laboratorio, di materiali classificati pericolosi, le cui attività possono avere impatto sulla corretta esecuzione delle attività di caratterizzazione e bonifica e, più in generale, sulle prestazioni e caratteristiche di sicurezza di impianti e macchine rilevanti sotto il profilo ambientale.
6. Procedura appalti: formalizzazione di una procedura volta a verificare la predisposizione di adeguate clausole di salvaguardia in sede di negoziazione dei contratti aventi ad oggetto attività con impatto potenziale sulla esecuzione delle attività di caratterizzazione e bonifica e, più in generale, sulle prestazioni e caratteristiche di sicurezza di impianti e macchine rilevanti sotto il profilo ambientale.

Relativamente alle attività sensibili di cui al n. **7** del precedente paragrafo 5.3, **concernenti i reati in tema di violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari di cui all'art. 258, comma 4, d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare e avere accesso alle prescrizioni legali applicabili.
2. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse le Procedure e Istruzioni Operative volte a far sì che siano pianificate, attuate

e condotte, tutte le attività necessarie o utili, anche sotto il profilo tecnico, al rispetto delle prescrizioni legali applicabili (e tra queste la procedura gestione rifiuti con indicazioni per il corretto campionamento ed analisi dei rifiuti e l'emissione del relativo certificato).

3. Procedura valutazione fornitori: formalizzazione di una procedura volta a definire le modalità di qualifica ambientale dei fornitori di servizi di analisi e prove di laboratorio e di prestazioni nel campo della gestione dei rifiuti.
4. Procedura appalti: formalizzazione di una procedura volta a verificare la predisposizione di adeguate clausole di salvaguardia in sede di negoziazione dei contratti aventi ad oggetto attività di campionamento, analisi e gestione dei rifiuti.

Relativamente alle attività sensibili di cui al n. **8** del precedente paragrafo 5.3, **concernenti i reati di traffico illecito di rifiuti cui all'art. 259, comma 1, d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare e avere accesso alle prescrizioni legali applicabili ai vari aspetti della gestione dei rifiuti, ivi incluse le spedizioni transfrontaliere.
2. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse ed aggiornate le dovute Procedure e Istruzioni Operative (e tra queste la procedura gestione rifiuti, con particolare riferimento alle spedizioni transfrontaliere di rifiuti).
3. Procedura controllo documenti: formalizzazione di una procedura volta ad assicurare che la documentazione attinente alle autorizzazioni sia aggiornata e distribuita o accessibile a tutti gli interessati.
4. Procedura valutazione fornitori: formalizzazione di una procedura volta a definire le modalità di qualifica ambientale dei fornitori di prestazioni nel campo delle spedizioni transfrontaliere di rifiuti e, in generale, dei terzi le cui attività possono avere un impatto ambientale.
5. Procedura appalti: formalizzazione di una procedura volta a verificare la predisposizione di adeguate clausole di salvaguardia in sede di negoziazione dei contratti aventi ad oggetto attività relative alle spedizioni transfrontaliere di rifiuti.

Relativamente alle attività sensibili di cui al n. **9** del precedente paragrafo 5.3, **concernenti i reati di attività organizzate per il traffico illecito di rifiuti di cui all'art. 260, d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare e avere accesso alle prescrizioni legali applicabili ai vari aspetti della gestione dei rifiuti, ivi incluse quelle contenute in atti autorizzativi.
2. Procedura controllo documenti: formalizzazione di una procedura volta ad assicurare che la documentazione attinente alle autorizzazioni sia aggiornata e distribuita o accessibile a tutti gli interessati.
3. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse le Procedure e Istruzioni Operative volte a far sì che siano pianificate, attuate e condotte, nelle condizioni specificate dalle prescrizioni legali applicabili, tutte le attività necessarie o utili, anche sotto il profilo tecnico, al rispetto delle prescrizioni legali

applicabili (e tra queste la procedura gestione rifiuti).

4. Procedura valutazione fornitori: formalizzazione di una procedura volta a definire le modalità di qualifica ambientale dei fornitori di servizi generali, di servizi di manutenzione, di impianti e macchine, di analisi e prove di laboratorio, di materiali classificati pericolosi, di prestazioni nel campo della gestione dei rifiuti, e, in generale, dei terzi le cui attività possono avere un impatto ambientale.

5. Procedura appalti**:** formalizzazione di una procedura volta a verificare la predisposizione di adeguate clausole di salvaguardia in sede di negoziazione dei contratti aventi ad oggetto attività potenzialmente comportanti un impatto sull'ambiente.

Relativamente alle attività sensibili di cui al n. **10** del precedente paragrafo 5.3, **concernenti i reati in tema di sistema informatico di controllo sulla tracciabilità dei rifiuti di cui all'art. 260-*bis*, comma 6, d.lgs. 152/2006**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare ed avere accesso alle prescrizioni legali applicabili, ivi incluse quelle riferite alla analisi dei rifiuti e alla documentazione SISTRI.

2. Procedura controllo operativo: formalizzazione di una procedura volta ad assicurare che siano emesse le Procedure e Istruzioni Operative volte a far sì che siano pianificate, attuate e condotte, tutte le attività necessarie o utili, anche sotto il profilo tecnico, al rispetto delle prescrizioni legali applicabili (e tra queste la procedura gestione rifiuti, con indicazioni per il corretto campionamento ed analisi dei rifiuti nonché per l'accesso e l'immissione delle informazioni richieste dal SISTRI).

3. Procedura valutazione fornitori: formalizzazione di una procedura volta a definire le modalità di qualifica ambientale dei fornitori di servizi di analisi e prove di laboratorio e di prestazioni nel campo della gestione dei rifiuti e, in generale, dei terzi le cui attività possono avere un impatto ambientale.

4. Procedura appalti: formalizzazione di una procedura volta a verificare la predisposizione di adeguate clausole di salvaguardia in sede di negoziazione dei contratti aventi ad oggetto attività di campionamento, analisi e gestione rifiuti.

5. Procedura per la sicurezza degli accessi al sistema informatico: formalizzazione di una procedura volta a prevenire l'accesso non autorizzato agli elaboratori e l'utilizzo illecito dei dispositivi SISTRI.

Relativamente alle attività sensibili di cui al n. **11** del precedente paragrafo 5.3, **concernenti i reati in tema di Cessazione e riduzione dell'impiego delle sostanze lesive a tutela dell'ozono stratosferico e dell'ambiente di cui all'art. 3, comma 6, L. 549/1993**, i protocolli di controllo preventivo specifici di cui ai n. I, II, III e IV, sono ulteriormente precisati come di seguito indicato:

1. Procedura prescrizioni legali e valutazione del loro rispetto: formalizzazione di una procedura volta ad identificare e avere accesso alle prescrizioni legali applicabili, ivi incluse quelle contenute in atti autorizzativi.

2. Procedura gestione delle emergenze: formalizzazione di una procedura volta ad identificare e limitare le conseguenze di incidenti che potrebbero comportare inquinamento del suolo, delle acque o dell'aria.

3. Procedura progettazione nuovi impianti o modifica impianti esistenti: formalizzazione di

una procedura volta ad accertare che in sede di progettazione e acquisto di impianti nuovi (o sezioni modificative di impianti esistenti) siano tenute in considerazione le prescrizioni legali.

4. Procedura appalti: formalizzazione di una procedura volta a verificare la predisposizione di adeguate clausole di salvaguardia in sede di negoziazione dei contratti aventi ad oggetto attività potenzialmente comportanti un impatto sull'ambiente.

5. Procedura valutazione fornitori: formalizzazione di una procedura volta a definire le modalità di qualifica ambientale dei fornitori di servizi generali, di servizi di manutenzione, di impianti e macchine, di analisi e prove di laboratorio, di materiali classificati pericolosi, di prestazioni nel campo della gestione dei rifiuti, e, in generale, dei terzi le cui attività possono avere un impatto ambientale.

6. Procedura gestione delle manutenzioni: formalizzazione di una procedura volta ad accertare che in sede di manutenzione delle apparecchiature contenenti sostanze lesive dello strato di ozono siano adottate le adeguate precauzioni.

5.4.5 Protocolli di controllo successivi relativi alle attività sensibili

(i) Attività di vigilanza sull'applicazione dei protocolli di controllo specifici

Huawei formalizza altresì una procedura volta a garantire il rispetto delle procedure e delle istruzioni operative e la conformità delle singole attività alle leggi e alle norme interne.

(ii) Attività di verifica periodica dell'efficacia del Sistema di Gestione HSE

Oltre a quanto sopra, la Società formalizza una procedura volta a controllare periodicamente i dati e/o gli indicatori che rappresentano le caratteristiche principali delle varie attività costituenti il Sistema di Gestione HSE e, conseguentemente, la verifica dell'efficacia del Sistema nel suo insieme.

5.5 Gli obblighi di informativa all'Organismo di Vigilanza in materia di tutela dell'ambiente

Tutti i Destinatari del Modello sono tenuti a rispettare gli obblighi di informazione all'Organismo di Vigilanza di Huawei secondo quanto indicato nel Capitolo 3 della Parte Generale di questo Modello con riferimento a qualsiasi non conformità, potenziale o attuale, in materia di tutela dell'ambiente.

Il responsabile ambientale e gli eventuali delegati funzionali che dovessero essere nominati, per quanto di competenza, anche con il supporto della funzione Quality, assicurano l'adempimento di tali obblighi presso l'Organismo di Huawei.

5.6 I Terzi Destinatari

Occorre da ultimo precisare che in materia di reati ambientali può assumere particolare rilevanza la posizione di quei soggetti che, pur essendo esterni rispetto alla struttura organizzativa della Società, svolgono un'attività che può essere determinante ai fini della legittimità e liceità dell'attività di questa (es: trasportatori di rifiuti, fornitori di prestazioni tecniche di misurazione, appaltatori di servizi di audit ambientale, ma anche progettisti, fornitori e installatori di impianti e macchinari).

In questo ambito, devono pertanto considerarsi Terzi Destinatari:

a) i soggetti cui è affidato un lavoro in virtù di contratto d'appalto o d'opera o di somministrazione;

b) i fabbricanti ed i fornitori;

c) i progettisti di impianti;

d) gli installatori ed i montatori di impianti.

In particolare, la Società ha predisposto adeguate procedure al fine di assicurare che i Terzi Destinatari, le cui attività possano aver un impatto sulle prestazioni ambientali di Huawei siano selezionati, verificati e periodicamente monitorati.

ALLEGATO 1

MIAR (Matrice di Individuazione delle Aree a Rischio)

Attività sensibili relative ai reati contro la Pubblica Amministrazione (paragrafo 1.2.1 Parte Speciale)	Key Officers
PA1: Acquisizione (redazione e/o predisposizione delle domande/istanze) e/o gestione/destinazione di contributi/sovvenzioni/finanziamenti pubblici (nazionali e/o internazionali ricevuti, ad esempio, per attività di formazione, assunzione di personale, ristrutturazione immobili, ecc.).	GM Office, HR
PA2: Gestione delle domande e dei rapporti con Pubbliche Amministrazioni, aziende di Stato, enti ed uffici pubblici per l'ottenimento di concessioni, autorizzazioni e licenze e altri provvedimenti amministrativi inerenti all'esercizio delle attività aziendali (es. autorizzazioni per la costruzione e fornitura di reti di telecomunicazione, autorizzazioni per l'istallazione di siti radiomobili).	GM Office, BU Managers, Legal
PA3: Negoziazione, stipulazione ed esecuzione di contratti e/o convenzioni con la Pubblica Amministrazione anche attraverso la partecipazione a procedure ad evidenza pubblica (aperte, negoziate o ristrette) o affidamenti diretti da parte di enti pubblici (es. contratti di vendita di prodotti e servizi ICT forniti dalla Società, contratti di locazione relativi a terreni/siti per l'istallazione di siti radiomobili).	BU Managers
PA4: Gestione di software di soggetti pubblici o forniti da terzi per conto di soggetti pubblici e collegamenti telematici (in entrata e in uscita) o trasmissione di dati su supporti informatici a soggetti pubblici – in particolare in materia societaria e fiscale.	GM Office, Quality
PA5: Gestione dei contenziosi e controversie giudiziarie di qualsiasi genere, grado o giurisdizione nei quali sia coinvolta a qualsiasi titolo la Società.	Legal
PA6: Gestione rapporti con autorità e soggetti pubblici nel normale svolgimento di attività aziendali (es. Enti Pubblici Locali, Agenzia delle Entrate, Guardia di Finanza, INPS, INAIL, Ispettorato del Lavoro, autorità competenti in materia di tutela della salute e sicurezza sul lavoro, VVFF, Sportello Unico per l'Immigrazione, Prefetture, Questure, Dipartimento Provinciale del Lavoro, ASL, Camere di Commercio, Agenzia delle dogane, uffici catastali e conservatorie, istituti universitari, ecc.) e nell'ambito di collaborazione in caso di indagini basate su comunicazioni elettroniche. Adempimenti e ispezioni.	GM Office, Quality, Office Manager, HR, Legal, Integration
PA7: Gestione dei rapporti con altre Autorità pubbliche di vigilanza o regolamentari (es. Autorità Garante della Concorrenza e del Mercato, AGCOM, Autorità garante per la protezione dei dati personali, Ministeri, autorità governative, ecc.).	GM Office, Public Affairs

ALLEGATO 1

Attività strumentali relative ai reati contro la Pubblica Amministrazione (paragrafo 1.2.2 Parte Speciale)	Key Officers
STR1: Gestione dei flussi finanziari in entrata ed in uscita.	CFO, Treasury
STR2: Gestione dell'attività relativa ad azioni di recupero di crediti insoluti.	Legal
STR3: Selezione e gestione dei rapporti con fornitori di beni e servizi (ivi inclusi consulenti in materia tecnico-finanziaria, legale o altro tipo), agenti e distributori.	Acquisti, BU Managers
STR4: Gestione degli omaggi e delle spese di rappresentanza/gestione delle erogazioni liberali.	GM Office, BU Managers
STR5: Selezione, assunzione e promozione di personale dipendente (ivi compreso personale appartenente alle categorie protette o la cui assunzione è agevolata).	HR

ALLEGATO 1

Attività sensibili relative ai reati societari (paragrafo 2.2 Parte Speciale)	Key Officers
SOC1: Tenuta della contabilità, redazione del bilancio d'esercizio, delle situazioni economiche infrannuali, delle relazioni e delle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico.	CFO, Finance Corporate, Finance Tax
SOC2: Rapporti con il collegio sindacale, società di revisione legale e soci.	CFO, Finance Corporate
SOC3: Operazioni sul capitale e destinazione degli utili.	CFO, Finance Corporate
SOC4: Attività di preparazione delle riunioni assembleari, svolgimento e verbalizzazione delle assemblee.	Legal
SOC5: Comunicazioni alle Autorità di vigilanza e gestione dei rapporti con le stesse.	GM Office, Public Affairs
SOC6: Comunicazione del conflitto di interessi ai sensi dell'art. 2391, comma 1, c.c.	Legal
SOC7: Liquidazione di società.	CFO, Finance Corporate
SOC8: Emissione di comunicati tramite media (ad es.: stampa, sito internet, ecc.)	Marketing
SOC9: Gestione delle transazioni infragruppo.	Finance Corporate

ALLEGATO 1

Attività sensibili relative ai delitti informatici e trattamento illecito di dati (paragrafo 3.2 Parte Speciale)	Key Officers	Repository
CYBER1: Definizione delle regole da adottare in materia di sicurezza del sistema informatico e telematico. • Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals • Regulations on Firewall Policy Security Management • IT Security Standards • Process for the Recovery of Hard Disk Data • Construction Specifications of Proxy • Extranet Security Specifications .	GMO Director QHSE Manager IT Manager	PDMC
CYBER2: Gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione. • Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals • Management Regulations on User Account and Access • IT Security Standards • Management Regulations on System Rights • Management Regulations on User Account and Access • Construction Specifications of the iAccess • Network Security Management Process • Guide to Information Security Management of Non-Huawei Employees	GMO Director	PDMC
CYBER3: Gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni. • Regulation on Preventing Computer viruses • Management Requirements for IT System Security Logs • General Policy for IT Internal Security Control	QHSE Manager	PDMC
CYBER4: Gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni, ecc.) e delle attività di inventariazione dei beni. • Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and	IT Manager	PDMC

Peripherals • Operating Instructions for Taking Hard Disks, Servers, or Storage Devices out of Equipment Rooms • R&D Confidential Devices & Media Management Regulations • Regulation on Security Management of Office Environment • Regulations on Conference Information Security • Data Center Management Regulations • Information Security Management Regulations for R&D Environment • Regulations on Security Management of Development and Test Environments • Regulations on Type III Production Environment Security Management		
CYBER5: Acquisizione e gestione di apparecchiature, di dispositivi (anche di rilevazione) connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione). • IT Security Standards • General Policy for IT Internal Security Control • R&D Confidential Devices & Media Management Process	GMO Director	PDMC
CYBER6: Monitoraggio/verifica periodica del sistema informatico e gestione degli incidenti e dei problemi di sicurezza informatica. • IS Problem handling and recording • Reporting channel • Information Security Incident Response Process	QHSE Manager	PDMC

ALLEGATO 1

Attività sensibili relative ai reati in materia di tutela della salute e sicurezza sul lavoro (paragrafo 4.4 Parte Speciale)	Key Officers
HS1: Individuazione, valutazione e mitigazione dei rischi: si tratta dell'attività di periodica valutazione dei rischi al fine di: (i) individuare i pericoli e valutare i rischi per la salute e la sicurezza dei lavoratori sui luoghi di lavoro; (ii) identificare le misure in atto per la prevenzione e il controllo dei rischi e per la protezione dei lavoratori; (iii) definire il piano di attuazione di eventuali nuove misure di prevenzione e protezione ritenute necessarie.	Quality
HS2: Rispetto degli standard tecnico – strutturali di legge: si tratta delle attività volte a garantire la conformità a quella che è la normativa tecnica propria delle attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici presenti ed utilizzati in azienda.	Quality
HS3: Gestione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori: si tratta delle attività relative alla attuazione e alla gestione del sistema di prevenzione e protezione della salute e sicurezza dei lavoratori, comprensiva delle attività di natura organizzativa quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza.	Quality
HS4: Attività di sorveglianza sanitaria: si tratta dell'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 professionale e alle modalità di svolgimento dell'attività lavorativa.	Quality
HS5: Attività di informazione e formazione dei lavoratori: si tratta (i) della gestione di un sistema interno di diffusione delle informazioni tale da garantire a tutti i livelli aziendali un corretto approccio alle tematiche riguardanti la sicurezza e la salute dei lavoratori, nonché (ii) della gestione ed attuazione di piani sistematici di formazione e sensibilizzazione con la partecipazione periodica di tutti i dipendenti, con particolare riferimento a quei soggetti che ricoprono ruoli particolari in azienda.	Quality
HS6: Attività di vigilanza sull'applicazione e sul rispetto da parte dei lavoratori delle procedure e delle istruzioni operative: si tratta della gestione delle attività volte a verificare: (i) la corretta applicazione di politiche, programmi e procedure; (ii) la chiara definizione, la comprensione, la condivisione e l'operatività delle responsabilità organizzative; (iii) la conformità dei prodotti e delle attività industriali alle leggi e alle norme interne; (iv) l'identificazione degli eventuali scostamenti e la regolare attuazione delle relative azioni correttive; (v) l'identificazione e il controllo di tutte le situazioni di rischio conoscibili.	Quality
HS7: Acquisizione di documentazione e certificazioni obbligatorie: si tratta della gestione dell'attività volta a garantire la richiesta e raccolta della documentazione e/o delle certificazioni connesse all'esercizio dell'attività ed obbligatorie per legge.	Quality
HS8: Attività di periodica verifica dell'applicazione e dell'efficacia delle procedure adottate: si tratta della verifica sistematica e continua dei dati e/o indicatori che rappresentano le caratteristiche principali delle varie attività costituenti il SGSSL della Società e, conseguentemente, della verifica dell'applicazione ed efficacia delle procedure adottate.	Quality
HS9: Organizzazione della struttura aziendale con riferimento alle attività in tema di salute e sicurezza sul lavoro: si tratta delle attività volte a garantire una struttura organizzativa aziendale che preveda una articolazione di funzioni in grado di assicurare le competenze tecniche ed i poteri	Quality

Attività sensibili relative ai reati in materia di tutela della salute e sicurezza sul lavoro (paragrafo 4.4 Parte Speciale)	Key Officers
necessari per la verifica, la valutazione, la gestione ed il controllo dei rischi per la salute e la sicurezza dei lavoratori.	

ALLEGATO 1

Reati Ambientali: 1. Attività sensibili relative ai reati di attività di gestione (ad es. raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione) di rifiuti non autorizzata di cui all'art. 256 comma 1, lett. a) e b), d.lgs. 3 aprile 2006, n. 152 (paragrafo 5.3.4.1 Parte Speciale)	**Key Officers**
AMB1.1: Raccolta e trasporto di rifiuti, anche propri, in assenza di iscrizione all'Albo Nazionale dei Gestori Ambientali (salvo i casi in cui l'iscrizione è sostituita dalla relativa comunicazione).	Quality, consulente ambientale
AMB1.2: Detenzione di rifiuti (in particolare da parte del loro produttore) senza autorizzazione al deposito o allo stoccaggio o in violazione dei limiti di legge al deposito temporaneo (art. 183, comma 1, lett. bb) d.lgs. n.152/2006).	Quality, consulente ambientale
AMB1.3: Erronea attribuzione di codifica del rifiuto nell'operazione di caratterizzazione (anche in caso di assenza di analisi, ove richieste, come nel caso di rifiuti con codici a specchio), laddove si tratti di errore non materiale.	Quality, consulente ambientale
AMB1.4: Raccolta, trasporto, acquisto, vendita, commercializzazione, intermediazione, deposito, stoccaggio, impiego nell'attività produttiva di "sottoprodotti" in violazione dei requisiti di legge ex art. 184-bis d.lgs. n.152/2006.	Quality, consulente ambientale
AMB1.5: Raccolta, trasporto, acquisto, vendita, commercializzazione, intermediazione, deposito, stoccaggio, impiego nell'attività produttiva di "materie prime secondarie" o "End of Waste" in violazione dei requisiti di legge ex art. 184-ter d.lgs. n.152/2006.	Quality, consulente ambientale
AMB1.6: Consegna di rifiuti a trasportatore non autorizzato e/o non iscritto all'Albo Nazionale dei Gestori Ambientali (in concorso con quest'ultimo) o con iscrizione scaduta o con mezzi non contemplati nel provvedimento di iscrizione all'Albo.	Quality, consulente ambientale
AMB1.7: Conferimento di rifiuti a soggetto non autorizzato o privo di formulario (in concorso con quest'ultimo).	Quality, consulente ambientale
AMB1.8: Inadempimento obblighi documentali di legge da parte del produttore dei rifiuti (MUD; c.d. "MUDINO"; registro di carico e scarico dei rifiuti; formulario di trasporto dei rifiuti).	Quality, consulente ambientale
AMB1.9: Violazione delle modalità semplificate di raccolta e trasporto dei Rifiuti da Apparecchiature Elettriche ed Elettroniche ("RAEE") di cui al d.lgs. 25 luglio 2005, n. 151 e al D.M. 8 marzo 2010, n. 65.	Quality, consulente ambientale
AMB1.10: Trasporto ai centri di raccolta dei RAEE su base più ampia di quella mensile ovvero per un quantitativo superiore a 3500 Kg; raggruppamento dei RAEE in luogo non idoneo o accessibile a terzi o non pavimentato; mancata protezione dei RAEE dalle acque meteoriche e dall'azione del vento; mancata salvaguardia dell'integrità dei RAEE.	Quality, consulente ambientale
AMB1.11: Trasporto di un quantitativo di RAEE superiore a 3500 kg, effettuato con automezzi con portata superiore a 3500 kg e massa complessiva superiore a 6000 kg.	Quality, consulente ambientale
AMB1.12: Inadempimento obblighi documentali di legge da parte dei distributori e dei trasportatori dei RAEE (registro di carico e scarico dei rifiuti,	Quality, consulente

documento di trasporto e schedario prescritti dal D.M. 65/2010).	ambientale
Reati Ambientali: 2. Attività sensibili relative al reato di attività di gestione di rifiuti non autorizzata di cui all'art. 256, comma 3, d.lgs. 152/2006 (paragrafo 5.3.4.2 Parte Speciale)	**Key Officers**
AMB2.1: Realizzazione di discarica di rifiuti (tramite destinazione e allestimento di area con effettuazione -di norma- delle opere occorrenti).	Quality, consulente ambientale
AMB2.2: Gestione di discarica di rifiuti (mediante apprestamento di organizzazione di persone, cose e macchine) diretta al funzionamento della discarica in assenza di autorizzazione.	Quality, consulente ambientale
AMB2.3: Realizzazione e gestione (con le modalità di cui sopra) di discarica di rifiuti destinata, anche in parte, allo smaltimento di rifiuti pericolosi.	Quality, consulente ambientale
AMB2.4: Attività di deposito preliminare di rifiuti prolungata oltre i 12 mesi.	Quality, consulente ambientale
il tutto anche sotto forma di contributo, attivo o passivo, diretto a realizzare o anche semplicemente a tollerare lo stato di fatto che costituisce reato.	
Reati Ambientali: 3. Attività sensibili relative al reato di attività di gestione di rifiuti non autorizzata di cui all'art. 256, comma 4, d.lgs. 152/2006 (paragrafo 5.3.4.3 Parte Speciale)	**Key Officers**
AMB3.1: Svolgimento delle attività di raccolta e trasporto di rifiuti (ad esempio con mezzi diversi da quelli comunicati), di bonifica di siti, di bonifica dei beni contenenti amianto, di commercio e intermediazione di rifiuti senza detenzione, avendo adempiuto all'obbligo di iscrizione o comunicazione all'Albo Nazionale dei Gestori Ambientali ma in assenza delle condizioni previste all'art. 214.	Quality, consulente ambientale
Reati Ambientali: 4. Attività sensibili relative al reato di attività di gestione di rifiuti non autorizzata di cui all'art. 256, comma 5, d.lgs. 152/2006 (paragrafo 5.3.4.4 Parte Speciale)	**Key Officers**
AMB4.1: Miscelazione o diluizione di rifiuti pericolosi con rifiuti non pericolosi, ad esempio nel deposito temporaneo o durante il trasporto (senza autorizzazione).	Quality, consulente ambientale
AMB4.2: Miscelazione o diluizione di rifiuti pericolosi con diverse caratteristiche di pericolosità, ad esempio nel deposito temporaneo o durante il trasporto (senza autorizzazione).	Quality, consulente ambientale
Reati Ambientali: 5. Attività sensibili relative al reato di attività di gestione di rifiuti non autorizzata di cui all'art. 256, comma 6, d.lgs. 152/2006 (paragrafo 5.3.4.5 Parte Speciale)	**Key Officers**

AMB5.1: Deposito temporaneo di rifiuti sanitari pericolosi (ad esempio rifiuti contaminati da sangue o altri materiali biologici o che provengano da ambienti di isolamento infettivo) presso il luogo di produzione (reato tipico per strutture ospedaliere, cliniche, cimiteri, centri estetici, parrucchieri).	Quality, consulente ambientale
Reati Ambientali: 6. Attività sensibili relative ai reati connessi alla bonifica dei siti contaminati di cui all'art. 257, commi 1 e 2, d.lgs. 152/2006 (paragrafo 5.3.5 Parte Speciale)	**Key Officers**
AMB6.1: Omessa comunicazione di un evento potenzialmente in grado di contaminare il sito da parte del responsabile dell'evento stesso, a prescindere dal superamento delle concentrazioni soglia di contaminazione (CSC).	Quality, consulente ambientale
AMB6.2: Omessa presentazione o adempimento al piano di caratterizzazione ovvero compimento di altre attività che impediscano la formazione del progetto di bonifica.	Quality, consulente ambientale
AMB6.3: Mancata esecuzione delle attività di bonifica (comunque denominate) in conformità con il progetto approvato dall'autorità da parte di chi abbia cagionato l'inquinamento di suolo, sottosuolo, acque superficiali o sotterranee con superamento delle concentrazioni soglia di rischio (CSR).	Quality, consulente ambientale
ma anche, in via tuzioristica, l'omessa comunicazione del rinvenimento di contaminazione storica, da parte del proprietario o del gestore dell'area (in quanto tenuti a impedire la diffusione della contaminazione) o del responsabile dell'inquinamento, a prescindere dal superamento delle concentrazioni soglia di contaminazione (CSC).	
Reati Ambientali: 7. Attività sensibili relative al reato di violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari di cui all'art. 258, comma 4, d.lgs. 152/2006 (paragrafo 5.3.6 Parte Speciale)	**Key Officers**
AMB7.1: Effettuazione delle operazioni di campionamento dei rifiuti da analizzare in modo tale da non assicurare la rappresentatività del campione.	Quality, consulente ambientale
AMB7.2: Redazione di certificati contenenti dati falsi (ad esempio relativi al ciclo di produzione di rifiuti o alle loro caratteristiche chimiche).	Quality, consulente ambientale
Reati Ambientali: 8. Attività sensibili relative al reato di traffico illecito di rifiuti di cui all'art. 259, comma 1, d.lgs. 152/2006 (paragrafo 5.3.7 Parte Speciale)	**Key Officers**
AMB8.1: Spedizione transfrontaliera di rifiuti effettuata senza che la notifica prevista dal Regolamento (CEE) 259/93 (oggi: 1013/2006) sia stata inviata a tutte le autorità competenti o in base a notifica (gravemente) infedele.	Quality, consulente ambientale
AMB8.2: Spedizione transfrontaliera di rifiuti effettuata senza il consenso delle autorità competenti o avendone ottenuto il consenso mediante falsificazioni, false dichiarazioni o frode.	Quality, consulente ambientale

AMB8.3: Spedizione transfrontaliera di rifiuti effettuata senza (concreta) specifica dei rifiuti nel documento di accompagnamento.	Quality, consulente ambientale
AMB8.4: Spedizione transfrontaliera di rifiuti che comporti uno smaltimento o un recupero in violazione del documento di accompagnamento.	Quality, consulente ambientale
AMB8.5: Violazione dell'art. 14 del Regolamento 259/93 (oggi: 1013/2006), sulle esportazioni dei rifiuti destinati allo smaltimento verso i paesi EFTA e vieta l'esportazione di rifiuti destinati allo smaltimento verso i paesi extra-CE.	Quality, consulente ambientale
AMB8.6: Violazione dell'art. 16 del Regolamento 259/93 (oggi: 1013/2006), che regola le esportazioni di determinati rifiuti destinati al recupero verso i paesi OCSE o aderenti alla Convenzione di Basilea che hanno raggiunto un accordo con la Comunità.	Quality, consulente ambientale
AMB8.7: Violazione dell'art. 19 del Regolamento 259/93 (oggi: 1013/2006), che regola le importazioni di rifiuti destinati allo smaltimento da paesi EFTA aderenti alla Convenzione di Basilea e da altri paesi.	Quality, consulente ambientale
AMB8.8: Violazione dell'art. 21 del Regolamento 259/93 (oggi: 1013/2006), che regola le importazioni nella Comunità di rifiuti destinati al recupero ai paesi OCSE e da altri paesi.	Quality, consulente ambientale
AMB8.9: Spedizione di rifiuti i cui all'allegato II del regolamento 259/93 (oggi: 1013/2006) in violazione dell'art. 1, comma 3 lett. a) b), c) e d).	Quality, consulente ambientale
AMB8.10: Spedizione di sottoprodotti o di materie prime secondarie / End of Waste in assenza dei requisiti prescritti dalla legge nazionale e comunitaria.	Quality, consulente ambientale
Reati Ambientali: 9. Attività sensibili relative al reato di attività organizzate per il traffico illecito di rifiuti di cui all'art. 260, d.lgs. 152/2006 (paragrafo 5.3.8 Parte Speciale)	**Key Officers**
AMB9.1: Svolgimento di attività di gestione (ad esempio, raccolta, trasporto, commercio, intermediazione, recupero o smaltimento) di rifiuti, in violazione delle norme di legge, attraverso condotte ripetute che, nel loro complesso, abbiano ad oggetto un ingente quantitativo di rifiuti.	Quality, consulente ambientale
Reati Ambientali: 10. Attività sensibili relative al reato concernente il sistema informatico di controllo della tracciabilità dei rifiuti ("SISTRI") di cui all'art. 260-bis, comma 6, d.lgs. 152/2006 (paragrafo 5.3.9 Parte Speciale)	**Key Officers**
AMB10.1: Effettuazione delle operazioni di campionamento dei rifiuti da analizzare in modo tale da non assicurare la rappresentatività del campione.	Quality, consulente

	ambientale
AMB10.2: Predisposizione di un certificato di analisi recante false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti (indipendentemente dalla qualifica di pericolosità di questi).	Quality, consulente ambientale
AMB10.3: Inserimento di certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti (indipendentemente dalla qualifica di pericolosità di questi).	Quality, consulente ambientale
Reati Ambientali: 11. Attività sensibili relative ai reati di cui alla normativa prevista a tutela dell'ozono *ex* all'art. 3, comma 6 L. 549/1993 (paragrafo 5.3.12 Parte Speciale)	**Key Officers**
AMB11.1: Possesso o utilizzazione di attrezzature quali frigoriferi, impianti di climatizzazione, celle frigorifere o altri nei quali siano utilizzate sostanze lesive per l'ozono (in particolare CFC, CFC completamente alogenati, halon, tetracloruro di carbonio, metilcloroformio, bromuro di metile, idrobromuroclorofluorocarburi e idroclorofluorocarburi, quali i gruppi da 1 a 8 dell'allegato 1 Regolamento 1005/2009/CE).	Quality, consulente ambientale
AMB11.2: Produzione, anche involontaria, delle sostanze lesive per l'ozono di cui sopra.	Quality, consulente ambientale
AMB11.3: Uso delle sostanze lesive per l'ozono di cui sopra, ad eccezione di quelle contenute in prodotti e apparecchiature.	Quality, consulente ambientale
AMB11.4: Produzione, immissione sul mercato o uso di sistemi di protezione antincendio ed estintori contenenti halon, fatta eccezione per i casi di usi critici autorizzati.	Quality, consulente ambientale

ALLEGATO 2

Procedure interne attualmente adottate dalla Società in relazione alle attività sensibili e strumentali concernenti i reati contro la Pubblica Amministrazione

1.	Partecipazione a procedure ad evidenza pubblica o affidamenti diretti da parte di enti pubblici per la fornitura ad essi di prodotti, soluzioni e servizi ICT
2.	Gestione dei rapporti con autorità e soggetti pubblici
3.	Gestione del contenzioso
4.	Whistle Blowing Policy
5.	Gift and Hospitality Policy
6.	Procedura di lavoro interna della funzione Italy HR
7.	Business Code of Conduct
8.	Market to Lead Process Architecture"
9.	HW Global Tax Organization & Reporting System
10.	Operation Guide Monthly F24 Forms payment for Italy
11.	Operation Guide of Italy Monthly VAT
12.	WEU Tax related issue approval Hierarchy
13.	Business Trip Expenses Management Regulation
14.	Business Trip Travel Expenses Management Regulation
15.	Business Trip Travel-Hotel and Other Expenses Management Regulation
16.	
17.	

ALLEGATO 3

Procedure interne attualmente adottate dalla Società in relazione alle attività sensibili concernenti i reati societari

1.	Year End Closing Guide
2.	Business Code of Conduct
3.	Emissione di comunicati tramite *media*
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	
16.	
17.	

ALLEGATO 4

Procedure interne attualmente adottate dalla Società in relazione alle attività sensibili concernenti i reati informatici e trattamento illecito dei dati

Information Security SOA regarding ISO27001:2005 (2013) V1.6

ISO27001 Control Objectives and Controls		Huawei Policies and Controls
5 Security Policy		
5.1 Information Security Policy		
5.1.1	Information security policy document	**关于信息安全工作的指**导方针与原则要求Guidelines and Principles on Information Security Work http://w3.huawei.com/info/cn/doc/viewDoc.do?did=2713421&cata=215431 **信息安全策略**总纲 General Policies on Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122796&cata=6242 **信息安全政策文件管理流程** http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=128900&cata=8081 **研**发信息安全管理策略 R&D Information Security Management Policy http://w3.huawei.com/info/cn/doc/viewDoc.do?did=47226&cata=11147 IT**安全内控管理**纲要 General Policy for IT Internal Security Control http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91110&cata=6729
5.1.2	Review of information security policy	
6 Organization of Information security		
6.1 Internal Organization		
6.1.1	Management commitment to information security	**关于信息安全工作的指**导方针与原则要求Guidelines and Principles on Information Security Work http://w3.huawei.com/info/cn/doc/viewDoc.do?did=2713421&cata=215431
6.1.2	Information security co-ordination	**信息安全体系**组织架构设计指南（暂行） http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=128267&cata=8086 驻外机构信息安全管理指南 Information Security Management Guide for Overseas Offices http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=126140&cata=8086
6.1.3	Allocation of information security responsibilities	
6.1.4	Authorization process for Information processing facilities	华为员工商业行为准则 HUAWEI Employee Business Conduct Guidelines http://w3.huawei.com/info/cn/doc/viewDoc.do?did=86449&cata=20218 办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084
6.1.5	Confidentiality agreements	**保密**协议签署和存档管理规定Rules of Signing and Archiving of Non-Disclosure Agreement http://w3.huawei.com/info/cn/doc/viewDoc.do?did=18068&cata=11146
6.1.6	Contact with authorities	**信息安全策略**总纲 General Policies on Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122796&cata=6242
6.1.7	Contact with special interest groups	
6.1.8	Independent review of information security	
6.2 External Parties		
6.2.1	Identification of risk related to external parties	**外部人**员信息安全管理指南 Regulations on Information Security Management of Non-Huawei Employees http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122631&cata=8083
6.2.2	Addressing security when dealing with customers	OFF-SHORE**外包供**应商信息安全管理规定 Regulations on Information Security Management of Off-shore Outsourcing Suppliers http://w3.huawei.com/pdmc/doc/viewDoc.do?did=128037&cata=8084 **研**发合作开发信息安全管理指南 Information Security Guideline to R&D Cooperative Development http://w3.huawei.com/info/cn/doc/viewDoc.do?did=47235&cata=11147
6.2.3	Addressing security in third party agreements	**保密**协议签署和存档管理规定Rules of Signing and Archiving of Non-Disclosure Agreement http://w3.huawei.com/info/cn/doc/viewDoc.do?did=18068&cata=11146
7 Asset Management		
7.1 Responsibility for Assets		**信息保密管理**规定 Regulations on Information Confidentiality http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114428&cata=8082 **公司跨部**门信息获取操作指南 Regulation on Obtaining Cross-functional Information http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122620&cata=8082 **外来保密信息管理**规定Regulations on External Classified Information http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122617&cata=8082 **研**发信息资产安全管理规定 Security Management Regulations for R&D Information Assets http://w3.huawei.com/info/cn/doc/viewDoc.do?did=47227&cata=11147
7.1.1	Inventory of assets	
7.1.2	Ownership of Assets	
7.1.3	Acceptable use of assets	
7.2 Information Classification		
7.2.1	Classification guidelines	
7.2.2	Information labeling and handling	
8 Human Resource Security		
8.1 Prior to Employment		
8.1.1	Roles and responsibilities	华为员工商业行为准则 HUAWEI Employee Business Conduct Guidelines
8.1.2	Screening	

8.1.3	Terms and conditions of employment	http://w3.huawei.com/info/cn/doc/viewDoc.do?did=86449&cata=20218 **关于遵从**《华为员工商业行为准则》的相关规定V2.0 http://w3.huawei.com/info/cn/doc/viewDoc.do?did=993401&cata=21083 人员信息安全管理规定 Regulations on Personnel Management Regarding Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122641&cata=8083
8.2 During Employment		
8.2.1	Management Responsibility	**信息安全意**识教育 Online training: Information Security Awareness in Huawei http://ilearning.huawei.com/ilearningportal/ilearningPortal.html#!ilearningPortal/resourcesClassify/viewResources=2
8.2.2	Information security awareness, education and training	**信息安全宣**传 Information Security Publicizing CN:http://w3.huawei.com/cn/my.do?pid=11136 EN:http://w3.huawei.com/NetWeb/workplace/my.do?pid=6467
8.2.3	Disciplinary process	**信息安全**奖惩规定 Regulations on Awards and Punishments of Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=127033&cata=8083 **信息安全**奖惩事件录入指南 http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114435&cata=8083 **信息安全季度荣誉**奖申报指南 http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114434&cata=8083
8.3 Termination or change of employment		
8.3.1	Termination responsibility	人员信息安全管理规定 Regulations on Personnel Management Regarding Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122641&cata=8083
8.3.2	Return of assets	
8.3.3	Removal of access rights	**系**统权限管理规定 Management Regulations on System Rights http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91078&cata=6731 **用**户账号权限管理规定 Management Regulations on User Account and Access http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=106538&cata=6731
9 Physical and Environmental Security		
9.1 Secure Areas		
9.1.1	Physical security perimeter	办公场所安全管理规定 Regulation on Security Management of Office Environment http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=126052&cata=8084 **携物出**门电子流 e-flow：http://w3.huawei.com/dominoapp/oaf04/index.nsf/index?openform&App=takeout **外来人**员接待电子流 e-flow：http://w3.huawei.com/dominoapp/oaf05/index.nsf/index?readform&app=ismreception **卡**证门禁申请电子流 e-flow：http://w3.huawei.com/card/index.do?method=toIndex&catalogId=-1 **拍照和**摄像申请Taking Photos Or Video Apply e-flow:http://w3.huawei.com/spa/ **会**议信息安全管理指南 Regulations on Conference Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122619&cata=8082 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.4 Manage IT Service > 12.3.4.13 Physics Security > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6728 **数据中心管理制度** Data Center Management Regulations http://w3.huawei.com/pdmc/doc/viewDoc.do?did=93916&cata=6728 **研**发环境信息安全管理规定（V1.00）Information Security Management Regulations for R&D Environment http://w3.huawei.com/info/cn/doc/viewDoc.do?did=47229&cata=11147
9.1.2	Physical entry controls	
9.1.3	Securing offices, rooms and facilities	
9.1.4	Protecting against external and environmental threats	
9.1.5	Working in secure areas	
9.1.6	Public access, delivery and loading areas	
9.2 Equipment security		
9.2.1	Equipment sitting and protection	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084 **数据中心机房硬**盘及服务器、存储整机出机房操作指导 Operating Instructions for Taking Hard Disks, Servers, or Storage Devices out of Equipment Rooms http://w3.huawei.com/pdmc/doc/viewDoc.do?did=93919&cata=6728 **研**发机要设备与介质管理规定（V1.00）R&D Confidential Devices & Media Management Regulations http://w3.huawei.com/info/cn/doc/viewDoc.do?did=47234&cata=11147
9.2.2	Support utilities	
9.2.3	Cabling security	
9.2.4	Equipment maintenance	
9.2.5	Security of equipment off-premises	
9.2.6	Secure disposal or reuse of equipment	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084
9.2.7	Removal of property	
10 Communications and Operations Management		
10.1 Operational Procedures and Responsibilities		
10.1.1	Documented operating procedures	PDMC (Process Documents Management Center) http://w3.huawei.com/pdmc
10.1.2	Change management	12.0 Manage BT&IT > 12.3 Manage IT > 12.3.4 Manage IT Service > 12.3.4.6 Change Management > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6652
10.1.3	Segregation of duties	**系**统权限管理规定 Management Regulations on System Rights http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91078&cata=6731
10.1.4	Separation of development and operations facilities	**IT安全内控管理**纲要 General Policy for IT Internal Security Control http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91110&cata=6729 HWIT-CMMI项目转产标准 http://w3.huawei.com/pdmc/doc/viewDoc.do?did=90866&cata=6639
10.2 Third Party Service Delivery Management		

10.2.1	Service delivery	**信息安全策略**总纲 General Policies on Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122796&cata=6242 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.2 Implement IT Product / Platform > 12.3.2.7 Supplier Management > http://w3.huawei.com/pdmc/bpa/browseBPA.do?id=575 **研**发合作开发信息安全管理指南V2.0 Information Security Guideline to R&D Cooperative Development http://w3.huawei.com/info/cn/doc/viewDoc.do?did=47235&cata=11147
10.2.2	Monitoring and review of third party services	
10.2.3	Manage changes to the third party services	
10.3 System Planning and Acceptance		
10.3.1	Capacity management	12.0 Manage BT&IT > 12.3 Manage IT > 12.3.4 Manage IT Service > 12.3.4.4 Performance and Capacity Management > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6650
10.3.2	System acceptance	12.0 Manage BT&IT > 12.3 Manage IT > 12.3.2 Implement IT Product / Platform > 12.3.2.1 Integrated project management > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6639 HWIT-CMMI项目转产标准 HWIT-CMMI Acceptance Standard http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=90866&cata=6639 HWIT-CMMI 项目验收规程 HWIT-CMMI project acceptance procedure http://w3.huawei.com/pdmc/doc/viewDoc.do?did=106650&cata=6639 HWIT-CMMI 项目验收检查单 HWIT-CMM IPM C10-Project Acceptance Checklist http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=90869&cata=6639 HWIT-CMMI项目验收报告模板 HWIT-CMMI Project Acceptance Report http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=106780&cata=6639 应用系统认证(BAC)**管理指引** Business Application Certification (BAC)Management Instruction http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=73770&cata=6106
10.4 Protection against Malicious and Mobile Code		
10.4.1	Controls against malicious code	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084 计算机病毒防治**管理**规定 Regulation on Preventing Computer viruses http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91102&cata=6731
10.4.2	Controls against Mobile code	
10.5 Back-Up		
10.5.1	Information backup	IT备份与恢复管理流程 IT Backup and Recovery Management Process http://w3.huawei.com/pdmc/doc/viewDoc.do?did=87642&cata=6651 Personal computer: Personal backup space http://w3.huawei.com/dominoapp/it/isr/pbk/personalbackup.nsf/fmDatabase?ReadForm#
10.6 Network Security Management		
10.6.1	Network controls	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084 华为MPLS VPN**网**络设计规范 http://w3.huawei.com/pdmc/doc/viewDoc.do?did=112746&cata=5669 **防火**墙策略安全管理规定 Regulations on Firewall Policy Security Management http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91096&cata=6730 e-flow：http://w3.huawei.com/firewall/simple.do?method=simpleLogin SPES**网**络安全接入设备管理规定 http://w3.huawei.com/info/cn/doc/viewDoc.do?did=1026081&cata=18135
10.6.2	Security of network services	
10.7 Media Handling		
10.7.1	Management of removable media	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084 **硬**盘数据恢复管理流程 Process for the Recovery of Hard Disk Data e-flow：http://w3.huawei.com/spa/
10.7.2	Disposal of media	
10.7.3	Information handling procedures	
10.7.4	Security of system documentation	IT**安全**标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729
10.8 Exchange of Information		
10.8.1	Information exchange policies and procedures	**信息安全策略**总纲 General Policies on Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122796&cata=6242 **信息保密管理**规定 Regulations on Information Confidentiality http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114428&cata=8082 **公司跨部**门信息获取操作指南 Regulation on Obtaining Cross-functional Information http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122620&cata=8082 **外来保密信息管理**规定Regulations on External Classified Information http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122617&cata=8082
10.8.2	Exchange agreements	
10.8.3	Physical media in transit	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084
10.8.4	Electronic messaging	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals

		http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084
10.8.5	Business information systems	IT安全内控管理纲要 General Policy for IT Internal Security Control http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91110&cata=6729
10.9 Electronic Commerce Services (Not Applicable)		
10.9.1	Electronic commerce	
10.9.2	On-Line transactions	
10.9.3	Publicly available information	
10.10 Monitoring		
10.10.1	Audit logging	IT安全标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729 IT系统安全日志管理要求 Management Requirements for IT System Security Logs http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91086&cata=6731
10.10.2	Monitoring system use	
10.10.3	Protection of log information	
10.10.4	Administrator and operator logs	
10.10.5	Fault logging	
10.10.6	Clock synchronization	
11 Access control		
11.1 Business Requirement for Access Control		
11.1.1	Access control policy	信息保密管理规定/Regulations on Information Confidentiality http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114428&cata=8082 公司跨部门信息获取操作指南 Regulation on Obtaining Cross-functional Information http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122620&cata=8082 外来保密信息管理规定/Regulations on External Classified Information http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122617&cata=8082
11.2 User Access Management		
11.2.1	User registration	The allocation of passwords is controlled by electronic work-flow IT安全标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729 系统权限管理规定 Management Regulations on System Rights http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91078&cata=6731 用户账号权限管理规定 Management Regulations on User Account and Access http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=106538&cata=6731 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.4 Manage IT Service > 12.3.4.12 Account/Privilege Management > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6727 帐号权限申请 e-flow：http://w3.huawei.com/info/cn/doc/viewDoc.do?did=42405&cata=16584 特权帐号申请 e-flow：http://w3.huawei.com/dominoapp/oaf01/index.nsf/index?openform&App=itisr 端口特殊权限 e-flow：http://security.huawei.com/SpesWEB 文档特殊权限 e-flow：http://rmsweb.huawei.com/ODRP2/Default.aspx 其他特殊权限 e-flow：http://w3.huawei.com/spa/
11.2.2	Privilege measurement	
11.2.3	User password management	
11.2.4	Review of user access rights	
11.3 User Responsibilities		
11.3.1	Password use	The complexity of passwords is enforced by system policies. IT安全标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729
11.3.2	Unattended user equipment	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084
11.3.3	Clear desk and clear screen policy	
11.4 Network Access control		
11.4.1	Policy on use of network services	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084 IT安全标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729 IT运维安全通道管理规定 ITOC Management Regulations http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91071&cata=6730 防火墙策略安全管理规定 Regulations on Firewall Policy Security Management http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91096&cata=6730 e-flow：http://w3.huawei.com/firewall/simple.do?method=simpleLogin 对外GRE通道场景规范及建设监控模型 http://w3.huawei.com/info/cn/doc/viewDoc.do?did=1026011&cata=18135 无线局域网络安全管理规定Management Regulations on the Network Security of Wireless LAN http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91108&cata=6730 邮件过滤系统管理规定 http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91113&cata=6731 Proxy上网系统建设规范 Construction Specifications of Proxy http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=106987&cata=6731 Extranet安全规范 Extranet Security Specifications http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91093&cata=6729 Tools: SPES/iAccess
11.4.2	User authentication for external connections	
11.4.3	Equipment identification in networks	
11.4.4	Remote diagnostic and configuration port protection	
11.4.5	Segregation in networks	
11.4.6	Network connection control	
11.4.7	Network routing control	

11.5 Operating System Access Control		
11.5.1	Secure log-on procedures	IT**安全**标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729 办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084 Secure log-on enforced by domain policy Unique Domain account for each employee The complexity of passwords is enforced by system policies. Software blacklist maintained by SPES Session time-out checked by SPES Limitation of connection time enforced by domain policy
11.5.2	User identification and authentication	
11.5.3	Password management system	
11.5.4	Use of system utilities	
11.5.5	Session time-out	
11.5.6	Limitation of connection time	
11.6 Application access control		
11.6.1	Information access restriction	IT**安全**标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729 IT**系**统运维管理岗位安全管理规定与行为规范 Security Regulations and Codes of Conduct for IT System Management Personnel http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91097&cata=6730 **机要数据**库管理规定（试行） http://w3.huawei.com/info/cn/doc/viewDoc.do?did=1025541&cata=18135 **机要**NC**平台管理指南** http://w3.huawei.com/pdmc/doc/viewDoc.do?did=126127&cata=8084 **研**发环境信息安全管理规定（V1.00）Information Security Management Regulations for R&D Environment http://w3.huawei.com/info/cn/doc/viewDoc.do?did=47229&cata=11147
11.6.2	Sensitive system isolation	
11.7 Mobile Computing and Teleworking		
11.7.1	Mobile computing and communication	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定 Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084 iAccess**安全接入平台建**设规范 Construction Specifications of the iAccess http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91074&cata=6729 Security Tool: iAccess
11.7.2	Telnet working	
12 Information Systems Acquisition Development and Maintenance		
12.1 Security Requirements of Information Systems		
12.1.1	Security requirement analysis and specifications	IT**安全内控管理**纲要 General Policy for IT Internal Security Control http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91110&cata=6729 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.2 Implement IT Product / Platform > 12.3.2.2 Requirements Engineering > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6640
12.2 Correct Processing in Applications		
12.2.1	Input data validation	12.0 Manage BT&IT > 12.3 Manage IT > 12.3.2 Implement IT Product / Platform > 12.3.2.8 System Security Engineering > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6646 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.2 Implement IT Product / Platform > 12.3.2.6 Process and Product Quality Assurance > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6644
12.2.2	Control of internal processing	
12.2.3	Message integrity	
12.2.4	Output data validation	
12.3 Cryptographic controls		
12.3.1	Policy on the use of cryptographic controls	IT**安全**标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729
12.3.2	Key management	
12.4 Security of System Files		
12.4.1	Control of operational software	IT**安全内控管理**纲要 General Policy for IT Internal Security Control http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91110&cata=6729 IT**安全**标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.2 Implement IT Product / Platform > 12.3.2.5 Configuration Management > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6643 Security tool: SPES
12.4.2	Protection of system test data	
12.4.3	Access control to program source library	
12.5 Security in Development & Support Processes		
12.5.1	Change control procedures	IT**安全内控管理**纲要 General Policy for IT Internal Security Control http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91110&cata=6729 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.4 Manage IT Service > 12.3.4.6 Change Management > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6652
12.5.2	Technical review of applications after operating system changes	
12.5.3	Restrictions on changes to software packages	
12.5.4	Information leakage	12.0 Manage BT&IT > 12.3 Manage IT > 12.3.2 Implement IT Product / Platform > 12.3.2.8 System Security Engineering > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6646
12.5.5	Outsourced software development	12.0 Manage BT&IT > 12.3 Manage IT > 12.3.2 Implement IT Product / Platform > 12.3.2.7 Supplier Management >

		http://w3.huawei.com/pdmc/bpa/browseBPA.do?id=575
12.6 Technical Vulnerability Management		
12.6.1	Control of technical vulnerabilities	应用开发与部署安全技术规范 Application Development and Deployment Security Specifications http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=90804&cata=6641 **安全**补丁管理流程 System Vulnerability Fixing Process http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91085&cata=6731
13 Information Security Incident Management		
13.1 Reporting Information Security Events and Weaknesses		
13.1.1	Reporting Information security events	**信息安全**风险事件管理电子流 IS Problem handling and recording (electronic workflow)
13.1.2	Reporting security weaknesses	http://w3.huawei.com/spa/menuFlow.do?method=listMenu&menu=FA4 **信息安全和共享**问题反馈渠道 Reporting channel (published in online training) http://w3.huawei.com/info/cn/doc/viewDoc.do?did=35031&cata=12027 **信息**专员 Information security specialist/contactors in each department http://w3.huawei.com/info/cn/doc/viewDoc.do?did=28031&cata=14634 员工信息安全论坛 http://w3.huawei.com/itonline/forum.jspa?forumID=136&orderStr=null
13.2 Management of Information Security Incidents and Improvements		
13.2.1	Responsibilities and procedures	**信息安全事件响**应流程 Information Security Incident Response Process
13.2.2	Learning for Information security incidents	http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114430&cata=8085 **重大信息安全事件**调查和处理流程
13.2.3	Collection of evidence	http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=121449&cata=8085 **信息安全**团队论坛 http://3ms.huawei.com/connect/group/577
14 Business Continuity Management		
14.1 Information Security Aspects of Business Continuity Management		
14.1.1	Including information security in business continuity management process	业务连续性管理政策 Business Continuity Management Policy http://w3.huawei.com/info/cn/doc/viewDoc.do?did=2760881&cata=21087
14.1.2	Business continuity and risk assessment	业务连续性管理流程 Business Continuity Management Process
14.1.3	Developing and implementing continuity plans including information security	http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=128170&cata=8478 华为公司突发事件应急预案 Integrated Incident Management Plan（IMP） http://w3.huawei.com/info/cn/doc/viewDoc.do?did=3204401&cata=215071
14.1.4	Business continuity planning framework	IT**安全**应急处理流程 IT Security Emergency Response Process
14.1.5	Testing, maintaining and re-assessing business continuity plans	http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91112&cata=6731 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.4 Manage IT Service > 12.3.4.3 Availability Management > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6649 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.4 Manage IT Service > 12.3.4.5 IT Service Continuity Management > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6651 12.0 Manage BT&IT > 12.3 Manage IT > 12.3.4 Manage IT Service > 12.3.4.9 Incident Management > http://w3.huawei.com/pdmc/bpa/newBrowseBPA.do?id=6655 **数据中心**设施突发事件应急处置操作指导 13.1 Manage Real Estate and Site Operations > 13.1.5 Manage Facility Operations > 13.1.5.2 Manage Site Maintenance > http://w3.huawei.com/pdmc/doc/viewDoc.do?did=88830&cata=6314 **生**产采购突发事件应急管理操作指导 9.0 Procurement > 9.9 Govern Operations > 9.9.4 Manage Procurement Risk > http://w3.huawei.com/pdmc/doc/viewDoc.do?did=84056&cata=6346 华为公司健康与安全应急预案手册 http://w3.huawei.com/info/cn/doc/viewDoc.do?did=51530&cata=17260
15 Compliance		
15.1 Compliance with Legal Requirements		
15.1.1	Identification of applicable legislations	**信息安全策略**总纲 General Policies on Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122796&cata=6242 **当地法**务部门Local Legal Affairs Department
15.1.2	Intellectual Property Rights (IPR)	华为员工商业行为准则 HUAWEI Employee Business Conduct Guidelines http://w3.huawei.com/info/cn/doc/viewDoc.do?did=86449&cata=20218
15.1.3	Protection of organizational records	**信息安全策略**总纲 General Policies on Information Security http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122796&cata=6242 **信息保密管理**规定/Regulations on Information Confidentiality http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114428&cata=8082
15.1.4	Data protection and privacy of personal information	华为员工商业行为准则 HUAWEI Employee Business Conduct Guidelines http://w3.huawei.com/info/cn/doc/viewDoc.do?did=86449&cata=20218 **信息保密管理**规定/Regulations on Information Confidentiality http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114428&cata=8082 **外来保密信息管理**规定Regulations on External Classified Information http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122617&cata=8082
15.1.5	Prevention of misuse of information processing facilities	办公计算机、网络、应用系统、存储介质及办公外设安全管理规定

		Security Management Regulations for Office Computers, Networks, Applications, Storage Media, and Peripherals http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=114432&cata=8084
15.1.6	Regulation of cryptographic controls	IT**安全**标准 IT Security Standards http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=91079&cata=6729
15.2 Compliance with Security Policies and Standards and Technical compliance		
15.2.1	Compliance with security policy	**信息安全稽核管理**规定 Management Regulation of Information Security Auditing http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=122639&cata=8085
15.2.2	Technical compliance checking	IT**运**维健康检查操作指导 IT Operation Health Check Operation Guide http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=87635&cata=6649
15.3 Information System Audit Considerations		
15.3.1	Information system audit controls	IT蓝军内控制度与规范 http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=121434&cata=8085
15.3.2	Protection of information system audit tools	IT蓝军渗透测试业务流程 http://w3.huawei.com/pdmc/doc/viewDoc.do?menuFilter=yes&did=121432&cata=8085 Information system audit tools are kept by Network Security Department. Director's approval is needed to use those tools.

ALLEGATO 5

Procedure interne attualmente adottate dalla Società in relazione alle attività sensibili concernenti i reati in materia di tutela della salute e della sicurezza

Procedure di cui al Sistema di Gestione HSE relative al BS OHSAS 18001:2007

area	Description	repository
Administration area	Display Screen Equipment Driving and Mobile phones Hazardous Substances Housekeeping and Office Safety Inspections procedure Noise exposure regulation Administration Subcontractor EHS Management Induction Process Fire Precautions First Aid Ladders Legionellosis Manual Handling Temperature Sub-contractors working on Huawei Sites Pandemic preparedness and response plan Catering and Vending Regulations Safe Regulation for Electricity at Work Personal Hygiene Regulation Equipment Statutory Inspections Procedure Visitors Safety Procedure Italy RO EHS compliance procedure for Offices layout	PDMC Italy EHS teamspace

	changes and new offices opening	only
HR area	EHS Competence Training and Awareness Process Insurance Regulation Alcohol and Drugs Regulation Bullying and Violence Regulation Disabled Persons Regulation Hostile Environments Regulation Regulation FTC Employees, Temporary Staff and Consultants Stress Regulation Working Alone Regulation Hours of work Regulation Night and Shift Work Regulation Personal Protective Equipment Management Process	PDMC
Management System area	Huawei EU EHS Management Manual Huawei EHS policy EHS hazard and risk management process EHS Communication Process EHS incident management process EHS Objectives, Targets and Program Management Process	PDMC
Engineering Delivery area	Engineering subcontractor EHS Management induction Process Guide to Engineering Delivery EHS Management Italy Work Instructions Declaration Of Conformity	PDMC
Legal area	EHS Legislation and Other Requirements Management Process	PDMC

	Evaluation Form of Compliance with Laws, Regulations and Requirements Legal work on EHS List of Applicable Laws, Regulations and Requirements Update-Checking on Laws, Regulations and Requirements	

ALLEGATO 6

Procedure interne attualmente adottate dalla Società in relazione alle attività sensibili concernenti i reati ambientali

Procedure di cui al Sistema di Gestione HSE relative all'ISO 14001:2004

area	Description	repository
Administration area	Waste Management Procedure	PDMC
Engineering Delivery area	Environmental Protection Management System for Installation Sites	
Management System area	Huawei EU EHS Management Manual Huawei Environmental Policy Environmental Aspects and Impacts Analysis Procedure	PDMC
Supply Chain area	Management scrap disposal process Oversea Management Central Warehouse Outbound Process Operative Instruction for scrap process of network materials in Italy Management of Huawei waste deposit and operatives	PDMC For draft versions only local storage
Finance	Italy subsidiary inventory scrapping regulation	PDMC