LUMIT S.P.A.

MODELLO DI ORGANIZZAZIONE,

GESTIONE E CONTROLLO

ex D. Lgs. 8 giugno 2001, n. 231

(aggiornamento ottobre 2020)

SOMMARIO

PARTE I
CONTESTO E PRESIDI
(PARTE GENERALE)

PARTE II

MAPPATURA DEL RISCHIO E SPECIFICI PRESIDI (PARTE SPECIALE)

Definizioni

- **Attività a Rischio:** fase del Processo Sensibile all'interno della quale si possono presentare presupposti/potenzialità per la commissione di un reato;
- **Attività Strumentali:** attività attraverso la quale è possibile commettere il reato di corruzione /concussione;
- **CCNL Commercio:** Contratto Collettivo Nazionale di Lavoro attualmente in vigore ed applicato da LumIT S.p.A.;
- **Codice Etico:** codice etico adottato da LumIT S.p.A.;
- **Consulenti:** coloro che prestano la loro opera con riferimento ad uno specifico settore di attività e/o agiscono in nome e/o per conto di LumIT S.p.A., sulla base di un mandato o di altro rapporto di collaborazione anche coordinata;
- **Collaboratori:** coloro che prestano la loro opera con riferimento ad un progetto specifico, ovvero ad un abito di attività definito contrattualmente;
- **La Società:** LumIT S.p.A.;
- **Dipendenti:** tutti i dipendenti di LumIT S.p.A. (compresi i dirigenti, i quadri aziendali e, per la parte inerente al Codice Etico, anche i consulenti);
- **D. Lgs. 231 del 2001:** il decreto legislativo n. 231 dell'8 giugno 2001, rubricato Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 se n. 300, e successive modifiche;
- **Esponenti Aziendali:** dirigenti, amministratori, dipendenti, a qualsiasi titolo operanti nell'ambito dell'attività di LumIT S.p.A.;
- **Linee Guida:** le Linee Guida contenenti i principi e le regole generali per la predisposizione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231 del 2001 elaborate dal consulente preposto alla predisposizione del Modello di Organizzazione, Gestione e Controllo;

- **Linee Guida di Confindustria:** le Linee Guida per la predisposizione dei modelli di organizzazione, gestione e controllo ex D. Lgs. 231 del 2001 approvate da Confindustria in data 7 marzo 2002 e successive modifiche ed integrazioni (marzo 2014);
- **Modelli o Modello:** i modelli o il modello di organizzazione, gestione e controllo previsti dal D. Lgs. 231 del 2001;
- **Operazione Sensibile:** operazione o atto che si colloca nell'ambito dei Processi Sensibili e può avere natura commerciale, finanziaria o societaria;
- **Organi Sociali:** i membri del Consiglio di Amministrazione e del Collegio Sindacale di LumIT S.p.A.;
- **Organismo di Vigilanza:** organismo preposto alla vigilanza sul funzionamento e sull'osservanza del Modello e al relativo aggiornamento;
- **PP.AA.:** la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio;
- **Partner:** controparti contrattuali di LumIT S.p.A., sia persone fisiche sia persone giuridiche, con cui la società addivenga ad una qualunque forma di collaborazione contrattualmente regolata (acquisto e cessione di beni e servizi, associazione temporanea d'impresa - ATI, joint venture, consorzi, ecc.), ove destinati a cooperare con l'azienda nell'ambito dei Processi Sensibili;
- **Processi Sensibili:** attività di LumIT S.p.A. nel cui ambito ricorre il rischio di commissione dei Reati;
- **Reati:** i reati ai quali si applica la disciplina prevista dal D. Lgs. 231 del 2001 e successive modifiche

Premessa

La **società LumIT S.p.A.** (di seguito anche, per brevità, la Società o LumIT) è stata costituita in data 28 settembre 2009, con atto a rogito del notaio dott.ssa Fabiana Tuccillo, con n. Rep. 6554 e n. di raccolta 2278; la Società, avente codice fiscale e numero di iscrizione al registro delle imprese della città di Milano n. 06745090966, ha sede legale in Milano, Foro Bonaparte, 68 e un'unità locale in Sesto San Giovanni (MI), via Milanese, 20 (cfr. visura camerale del 20 maggio 2020).

La Società si configura quale società per azioni aventi come soci i sig.ri Paolo Giovanni Ferrari (C.F. FRRPGV77M07F205P) e la sig.ra Mara Arcidiacono (C.F. RCDMRA74C44F158B), entrambi detentori del 50% delle azioni, con capitale sociale pari a Euro 120.000 (cfr. visura camerale del 20 maggio 2020).

In data 16 ottobre 2019, l'assemblea dei soci di LumIT ha approvato il progetto di fusione per incorporazione nella LumIT della Mon-K Data Protection S.r.l. – Unico Socio; società quest'ultima, peraltro, già interamente controllata dalla stessa LumIT

La Società ha per oggetto sociale:

- Il commercio all'ingrosso e al dettaglio di personal computer, hardware, software e materiale informatico;
- La prestazione di servizi inerenti a quanto sopra;
- L'attività saltuaria di agente e rappresentante di commercio di beni, prodotti e servizi per l'informatica e per l'ufficio;
- L'attività di riparazione e manutenzione di prodotti elettronici;
- La fornitura di servizi di assistenza sistematica e di consulenza per l'installazione di applicazioni informatiche e per la gestione operativa delle stesse, restando esclusa qualsiasi attività di carattere professionale;
- L'attività di formazione prestata a favore dei clienti, relativamente a quanto sopra;

- l’attività di gestione e di manutenzione degli impianti tecnologici dei clienti nell’area, nei centri di elaborazione dati e presso i clienti stessi;
- le attività complementari all’espletamento di ognuna delle attività sopra elencate;
- lo studio, ingegnerizzazione, produzione e commercializzazione di prodotti informatici ad alto valore tecnologico (funzione acquisita a seguito della fusione);
- la realizzazione di investimenti produttivi e l'attuazione di progetti di innovazione per lo sviluppo di prodotti ricorrendo all'utilizzo di nuove tecnologie (funzione acquisita a seguito della fusione).

Come si può notare, a seguito della fusione, LumIT ha ampliato parzialmente il proprio oggetto sociale. Tuttavia, le nuove competenze sono perfettamente compatibili col core business della Società e sono perfettamente integrabili con i processi produttivi della medesima; inoltre la sede operativa è unica: ne consegue che la fusione non ha comportato un impatto particolarmente significativo sulla predisposizione ed implementazione dei Modelli.

La Società può inoltre assumere e concedere agenzie, commissioni, concessioni, rappresentanze, mandati relativi ai prodotti e alle attività di cui sopra. Può compiere tutte le operazioni commerciali, industriali, finanziarie, mobiliari ed immobiliari, ritenute dall’organo amministrativo, necessarie o utili per il conseguimento dell’oggetto sociale.

La Società potrà inoltre acquisire, non in via prevalente né ai fini di raccolta o di collocamento del pubblico risparmio, e con l’esclusione dell’esercizio professionale nei confronti del pubblico, interessenze, quote, partecipazioni in consorzi, in altre società, costituite o costituende, o ditte, aventi scopi affini, analoghi o connessi con quello sociale; costituirsi in associazioni temporanee di impresa; prestare garanzie reali o personali a favore di terzi, il tutto purché si tratti di operazioni connesse all’oggetto o ai fini che essa si propone di conseguire.

Infine, va dato atto che, in seguito al diffondersi del cd. “coronavirus”, la Società è dovuta ricorrere al cd. “lavoro agile” (o *“smart working”*), il quale è risultato essere perfettamente compatibile con i processi produttivi della Società.

Il “lavoro agile”, infatti, impone al dipendente di operare con sistemi informatici e ciò è coerente con l’attività principale dell’azienda e con le modalità di lavoro del personale, al quale è sempre stato richiesto di fare uso di questi sistemi anche sul posto di lavoro.

Atteso che i Modelli prendono già in considerazione forme di controllo dei processi anche da remoto (necessarie quando si opera prevalentemente con sistemi informatici), non si è dovuto modificarne in modo significativo le prescrizioni.

PARTE I

CONTESTO E PRESIDI

(PARTE GENERALE)

1. IL DECRETO LEGISLATIVO N. 231 DELL'8 GIUGNO 2001

1.1 La responsabilità amministrativa degli enti

Il decreto legislativo n. 231 dell'8 giugno 2001, rubricato Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000 n. 300 (di seguito, per brevità, **Decreto**), così come entrato in vigore il successivo 4 luglio 2001, ha introdotto nel nostro ordinamento la responsabilità in sede penale degli Enti, che si aggiunge alla responsabilità delle persone fisiche ad essi riferibili e che materialmente hanno realizzato il fatto.
Secondo tale disciplina, gli Enti possono essere ritenuti responsabili e, conseguentemente, sanzionati, in relazione a talune fattispecie di reato (cd. "reati presupposto"), commessi o tentati, nell'interesse o a vantaggio dell'Ente stesso, da amministratori o dipendenti.

1.2 Principi fondamentali del Decreto: i presupposti della responsabilità

Il Decreto ha introdotto nell'ordinamento italiano una responsabilità amministrativa (riferibile sostanzialmente alla responsabilità penale) a carico degli enti per alcune fattispecie di reato commesse o tentate nell'interesse o vantaggio degli stessi da parte di:

- persone fisiche che rivestano funzioni di rappresentanza, amministrazione o direzione degli enti stessi o di una loro unità organizzativa che sia dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione o il controllo degli enti medesimi (cd. "apicali", art. 5, comma 1, lettera a);

- persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati (cd. "sottoposti", art. 5, comma 1, lettera b).

In particolare, il sistema della responsabilità dell'ente si fonda su un duplice presupposto:

- Il primo - di tipo soggettivo - è individuabile nel fatto che una persona legata da un rapporto funzionale con l'ente commetta un reato (trattasi dei soggetti appena individuati);
- Il secondo - di tipo oggettivo - attiene all'esistenza di un collegamento di tipo obiettivo tra l'illecito commesso dalla persona fisica e l'ente, nel senso che la commissione del reato deve essere finalizzata al vantaggio o all'interesse della persona giuridica. In particolare, per "**vantaggio**" si intende il complesso dei benefici tratti dal reato, che si valutano ex post in un momento successivo alla commissione del medesimo, mentre il termine "**interesse**" si riferisce alla sfera volitiva della persona fisica che agisce ed è valutabile al momento della condotta. Ne deriva che l'impresa non è responsabile nel caso in cui manchi del tutto l'interesse – perché, per esempio, il soggetto qualificato ha agito per realizzare un interesse esclusivo proprio o di terzi; al contrario se un interesse dell'ente, sia pure marginale, si ritiene sussistente, l'illecito dipendente da reato si configura anche nell'ipotesi in cui l'ente non abbia tratto ex post alcun effettivo vantaggio dalla commissione del reato.

  Riguardo all'interpretazione dei requisiti dell'interesse e del vantaggio, è necessaria una precisazione per quanto concerne la loro compatibilità con i reati colposi introdotti tra i reati presupposto nel Decreto (in particolar modo ci si riferisce ai reati in materia di salute e sicurezza sul lavoro e ai reati ambientali). Si pensi all'ipotesi di omicidio colposo in violazione delle norme in materia di antinfortunistica e di sicurezza sul lavoro: difficilmente l'evento morte del dipendente può essere considerato l'interesse perseguito dalla società ovvero tradursi in un vantaggio per la stessa. In questi casi, pertanto, la giurisprudenza ha ritenuto che i due requisiti di interesse e vantaggio debbano essere valutati non tanto con riferimento all'evento ma all'intera fattispecie di reato, e

dovrebbero riferirsi alla condotta inosservante le norme cautelari (così, nell'esempio sopra riportato, l'interesse o il vantaggio dovrebbero ravvisarsi nel risparmio di costi per la sicurezza, ovvero nell'incremento della produttività sacrificando l'adozione di presidi antinfortunistici).

1.3. Le fattispecie di reato

Le fattispecie di reato rilevanti ai fini del Decreto e successive integrazioni possono essere comprese nelle seguenti categorie

- delitti contro la Pubblica Amministrazione (in senso ampio, non del tutto corrispondete alla suddivisione presente nel codice penale);
- reati societari;
- abusi di mercato;
- omicidio colposo e lesioni colpose gravi e gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul luogo di lavoro;
- reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio;
- delitti contro la fede pubblica, contro l'industria e il commercio;
- delitti in materia di terrorismo e di eversione dell'ordine democratico, ivi incluso il finanziamento ai suddetti fini;
- delitti contro la personalità individuale;
- reati transnazionali;
- reati informatici;
- delitti di criminalità organizzata;
- pratiche di mutilazione degli organi genitali femminili;
- delitti in materia di violazione del diritto d'autore;
- reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- reati ambientali;

- reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare;
- delitto di propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa
- reati tributari

La particolare natura della Società rende sovrabbondante la presenza di presidi verso determinate categorie di reati. In ogni caso, saranno inclusi presidi di massima valevoli anche per evitare il verificarsi di simili fattispecie.

1.4. Le Sanzioni per l'ente

Le sanzioni previste a carico dell'Ente, in conseguenza della commissione o tentata commissione dei reati summenzionati, sono:

- **sanzioni pecuniarie**, individuate secondo il sistema delle quote, fino a circa 1,5 milioni di Euro;
- **sanzioni interdittive**, quali l'interdizione dall'esercizio dell'attività, la sospensione o la revoca di licenze o concessioni, il divieto di contrarre con la Pubblica Amministrazione, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi, tutte applicabili anche nella fase cautelare;
- **confisca**, o sequestro preventivo nella fase cautelare, del profitto che l'Ente ha tratto dal reato;
- **pubblicazione della sentenza**, in caso di applicazione di una sanzione interdittiva.

1.5. L'esonero dalla responsabilità: il Modello di Organizzazione, Gestione e Controllo

Nel caso in cui il reato presupposto sia stato commesso da un cd. soggetto apicale, in presenza del citato nesso oggettivo tra illecito ed ente, è ravvisabile la responsabilità di quest'ultimo salvo che l'ente dimostri (art. 6):

1. di avere adottato ed efficacemente attuato prima della commissione del fatto un Modello di organizzazione e di gestione idoneo a prevenire reati della specie di quello commesso;
2. di aver istituito un apposito Organismo di Vigilanza allo scopo di verificare il funzionamento e l'osservanza di tale modello, nonché il suo aggiornamento;
3. che il reato sia stato commesso eludendo fraudolentemente il modello;
4. che non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di controllo.

Se non dimostra la sussistenza di tutte e 4 le suddette circostanze, l'ente verrà ritenuto responsabile in quanto risulterebbe ad esso imputabile una colpa organizzativa consistente nella mancata adozione ovvero nel carente funzionamento del modello preventivo.

Nell'ipotesi in cui il reato presupposto sia stato commesso da **persona sottoposta alla direzione e alla sorveglianza** dei soggetti apicali, in presenza del nesso oggettivo, l'ente è responsabile unicamente nel caso in cui la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza.
In ogni caso, è esclusa l'inosservanza di tali obblighi se l'ente, prima della commissione del reato, ha adottato ed efficacemente attuato un modello di organizzazione, di gestione e controllo idoneo a prevenire reati della specie di quello verificatosi (prevedendosi misure idonee allo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio). Tale modello dovrà essere sottoposto a verifica periodica e modifiche nell'ipotesi di mutamenti nell'organizzazione dell'ente e dovrà prevedere un sistema disciplinare destinato a sanzionare chiunque violi le misure indicate nel modello.

La differenza principale tra reati commessi da soggetti in posizione apicale e soggetti sottoposti all'altrui direzione si avrà, quindi, nel diverso onere probatorio.
Nel primo caso la colpa è presunta e per evitare la sanzione sarà onere della società dimostrare l'adeguatezza e l'efficacia dei modelli organizzativi adottati.

Qualora invece la responsabilità della società si ricolleghi a soggetti sottoposti ad altrui direzione, l'onere della prova sarà in capo alla pubblica accusa, che dovrà dimostrare la mancata adozione ed attuazione, prima della commissione del reato, di modelli idonei a prevenire reati della stessa specie di quello verificatosi, o quanto meno il loro mancato aggiornamento.

I modelli di organizzazione dovranno:

1. individuare le diverse aree di rischio all'interno dell'ente (cd. "**mappatura del rischio**");
2. configurare un **sistema strutturato ed organico di procedure**, regolamenti interni ed attività di controllo volti a razionalizzare lo svolgimento delle attività aziendali ed a prevenire il rischio di commissione dei reati rilevanti ai sensi della normativa;
3. prevedere un **effettivo ed efficace sistema di vigilanza** (affidando tali attribuzioni ad un organismo autonomo ed indipendente a ciò preposto) sul rispetto degli standard di comportamento;
4. prevedere, al fine di garantire l'effettività di quanto previsto nel modello organizzativo, un **sistema di sanzioni disciplinari** rivolto sia agli Organi Societari, sia ai dipendenti, sia a *partner* esterni alla società nel caso in cui tengano un comportamento rilevante ai sensi del sistema etico-organizzativo della società. Ad esempio, il cd. "codice etico" (di cui si parlerà in seguito) prevede una serie di principi cui devono attenersi i soggetti che agiscono in nome e per conto della società, nonché i suoi *partner* commerciali, quali in ipotesi la trasparenza nei rapporti con la Pubblica Amministrazione e il tassativo divieto di retribuire in qualsiasi modo il Pubblico funzionario; nell'ipotesi in cui il *partner* non rispettasse tali principi, il modello dovrà prevedere che nei contratti sia prevista l'obbligatoria risoluzione del contratto tra società e *partner* commerciale.

2. IL SISTEMA DELLA GOVERNANCE IN LUMIT

2.1. Principi generali

- Il sistema di Governance della Società, inteso come insieme dei principi e degli strumenti che presidiano il governo della Società da parte degli organi sociali preposti, è retto dai seguenti principi:
- correttezza;
- trasparenza;
- rispetto della legge e dei regolamenti interni ed esterni alla Società;
- creazione di valore e rispetto degli interessi di tutti i Soci Consorziati;
- segregazione delle attività.

2.2. Gli Strumenti

Il rispetto dei principi di cui sopra è evidentemente fondamentale per evitare che vengano commessi i reati previsti dal D. lgs. 231 del 2001 da parte dei soggetti considerati dal Decreto. Pertanto la Società ha adottato i seguenti strumenti di Governance:

- adeguato sistema delle deleghe e delle procure;
- suddivisione dei poteri per funzioni;
- codice etico.

2.2.1. Il sistema delle deleghe e delle procure.

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

Si intende per **delega** quell'atto interno di attribuzione di funzioni e compiti, riflesso nel sistema di comunicazioni organizzative, e per **procura** l'atto giuridico unilaterale con cui la Società attribuisce poteri di rappresentanza nei confronti dei terzi.

Ai **titolari di una funzione aziendale** (generalmente dirigenti non facenti parte del Consiglio di Amministrazione, ovvero quadri aziendali) che necessitano, per lo svolgimento dei loro incarichi, di poteri di rappresentanza, viene conferita una procura generale funzionale di estensione adeguata e coerente con le funzioni ed i poteri di gestione attribuiti al titolare attraverso la delega.

I requisiti essenziali del sistema delle deleghe, ai fini di un'efficace prevenzione dei reati, sono i seguenti:

- tutti coloro, compresi i dipendenti e i consulenti, che intrattengono per conto della Società rapporti con qualsiasi terzo soggetto, devono essere dotati di delega formale in tal senso, a firma del Consigliere Delegato;
- ciascuna delega deve definire in modo inequivocabile:
  - i poteri del delegato;
  - il soggetto (organo o individuo) a cui il delegato fa capo in via gerarchica;
  - eventualmente, altri soggetti ai quali le deleghe siano congiuntamente o disgiuntamente conferite;
- il delegato deve disporre dei poteri di spesa adeguati alle funzioni conferite al delegato;
- i poteri gestionali assegnati con le deleghe e la loro attuazione devono essere coerenti con gli obiettivi aziendali.

Per quanto concerne l'eventuale delega di funzioni in materia di tutela della salute e della sicurezza nei luoghi di lavoro, si rinvia anche all'art. 16 del Decreto legislativo 9 aprile n°81 del 2008.

I requisiti essenziali del sistema di attribuzione delle procure, ai fini di un'efficace prevenzione dei reati, sono i seguenti:

- le procure descrivono i poteri di gestione conferiti e, ove necessario, sono accompagnate da un'apposita comunicazione aziendale che fissa l'estensione dei poteri di rappresentanza ed i limiti di spesa;
- la procura può essere conferita a persone fisiche espressamente individuate nella stessa oppure a persone giuridiche, che agiranno a mezzo di propri procuratori investiti, nell'ambito di queste, di analoghi poteri;
- le procure generali funzionali sono conferite esclusivamente a soggetti dotati di delega interna che descrive i relativi poteri di gestione e, ove necessario, sono accompagnate da un'apposita comunicazione che fissa l'estensione dei poteri di rappresentanza ed eventualmente anche i limiti di spesa;
- una procedura ad hoc garantirà modalità e responsabilità per garantire un aggiornamento tempestivo delle procure, stabilendo i casi in cui le stesse dovranno essere attribuite, modificate o revocate;
- le procure indicano gli eventuali altri soggetti a cui sono conferiti congiuntamente o disgiuntamente, in tutto o in parte, i medesimi poteri di cui alla procura conferita.

2.2.2. Suddivisione dei poteri per funzioni.

La segregazione dei ruoli e dei poteri in ambito aziendale è uno strumento fondamentale di Corporate Governance, finalizzato al coinvolgimento dei soggetti con diversi poteri di gestione dell'impresa, affinché nessuno possa disporre di poteri illimitati e svincolati dalla verifica di altri soggetti.

Il sistema di segregazione dei ruoli, per essere funzionale rispetto alle previsioni del d.lgs. 231/2001, deve essere supportato da un'adeguata separazione dei poteri fra le diverse funzioni societarie. La segregazione dei poteri, infatti, consente di distribuire le facoltà e le responsabilità a seconda delle competenze di ciascun soggetto coinvolto nell'attività aziendale: se le fasi in cui si articola un processo vengono ricondotte a soggetti diversi, allora nessuno di questi può

essere dotato di poteri illimitati. Inoltre, suddividendo i poteri all'interno della società viene anche favorita l'attività di controllo sulle fasi più sensibili di ciascun processo.

2.2.3. Il Codice Etico

Il codice etico è un insieme di diritti e doveri, cui devono attenersi tutti i "dipendenti" della società (apicali e sottoposti), nonché i suoi partner commerciali, che mirano a promuovere o vietare determinati comportamenti e che prevede sanzioni disciplinari nell'ipotesi di commissione di infrazioni. Il codice etico ha pertanto un ruolo fondamentale nell'ambito del sistema preventivo delineato d. lgs. 231 del 2001. Il codice Etico adottato dalla Società, modificato contestualmente all'aggiornamento del Modello, è allegato al presente Modello ed è pubblicato sul sito internet aziendale.

3. I PRESIDI

3.1. Il sistema dei controlli interni

3.1.1. Il Sistema dei Controlli Interni – Considerazioni generali

Il Sistema dei Controlli Interni (di seguito, per brevità **SCI**), definito secondo gli standard internazionali tratti dal *CoSO Report* quale *"processo, svolto dal consiglio di amministrazione, dai dirigenti e dagli operatori della struttura aziendale, attuato per fornire una ragionevole assicurazione in merito al raggiungimento degli obbiettivi d'impresa[1]", è costituito "dall'insieme delle risorse, delle strutture organizzative, delle regole e delle procedure per assicurare il conseguimento delle strategie aziendali e dell'efficacia ed efficienza dei processi aziendali, della salvaguardia del valore delle attività e della protezione dalle perdite, dell'affidabilità e integrità delle informazioni contabili e gestionali, della conformità delle operazioni con la legge, le normativa di sorveglianza di eventuali autorità e le disposizioni interne dell'azienda.*
Nel sistema dei controlli interni rientrano le strategie, le politiche, i processi e i meccanismi riguardanti la gestione dei rischi a cui l'azienda è o potrebbe essere esposta e per determinare e controllare il livello di rischio tollerato. In questo contesto, la gestione dei rischi include le funzioni di individuazione, assunzione, misurazione, sorveglianza e attenuazione dei rischi [...]".

[1] *CoSO Report*, elaborato nel 1992 su incarico del Committee of Sponsoring Organisation of Treadway Commission (USA) ed aggiornato nel 2013, è comunemente accettato quale modello di riferimento in tema di governance e controllo interno, ed è considerato un riferimento per la predisposizione dei sistemi di controllo interno ai fini del D. Lgs. 231 del 2001 dalle Linee guida di Confindustria, accanto all'*Enterprise Risk Management Framework* (c.d. ERM), anch'esso emesso dal CoSO nel 2004 in materia di gestione dei rischi.

In particolare, assumono particolare rilievo:

- **Il rischio operativo**, direttamente collegato all'operatività presso i clienti;
- **Il rischio di natura legale**, che può discendere (anche) dai rapporti con la clientela;
- Il **rischio** legato alle previsioni del D. Lgs. 231 del 2001.

Al fine di monitorare al meglio la correttezza e la sicurezza dell'operatività aziendale, LumIT ha stabilito di attivare le seguenti tipologie di controllo che insisteranno sull'intera struttura (cfr. infra, Parte II, *Principi*):

1. **Controlli di linea informatizzati**, o di *primo livello*, insistenti sulla struttura dei servizi offerti nell'ambito dell'operatività di LumIT. Tali controlli, che saranno automatici e totalmente informatizzati per quanto concerne la struttura del servizio fornito alla clientela -e implicanti in tal caso l'immediato blocco dell'operatività in caso di anomalie informatiche- sono affidati al costante monitoraggio dei Responsabili di Funzione. Mensilmente, i Responsabili di Funzione, così come precedentemente individuati, procederanno ad effettuare controlli (a campione, sistematici e gerarchici) nell'ambito dell'attività di back office, dandone gli opportuni feedback al CD;

2. **Controlli sulla gestione dei rischi**, o di *secondo livello*, per ciò che concerne il rischio operativo, aventi lo scopo e l'obiettivo di concorrere:
   - alla definizione delle metodologie di individuazione e di misurazione dei rischi aziendali, con particolare attenzione al rischio operativo;
   - alla verifica del rispetto delle mansioni e dei limiti assegnati alle varie funzioni operative;
   - al controllo della coerenza e della congruenza delle metodologie adottate dalle singole funzioni con gli obiettivi di rischio-rendimento assegnati;

   Per quanto concerne i rischi di reato ai fini del D. Lgs. 231/2001, tali controlli sono affidati all'Organismo di Vigilanza all'uopo istituito che vigilerà:

- sulla scrupolosa osservanza del Codice Etico di LumIT;
- sulla scrupolosa osservanza delle procedure e dei protocolli previsti dal Modello di Organizzazione, Gestione e Controllo di LumIT, mediante verifiche a campione;
- sull'implementazione corretta e graduale delle procedure in relazione a mutamenti o nuove esigenze dettate dall'attività sociale;
- sulla verifica delle eventuali segnalazioni che giungeranno dai vari comparti della società;
- sul corretto recepimento delle prescrizioni di MOGC e Codice Etico da parte delle varie Funzioni di LumIT;

3. **Attività di revisione interna**, affidata particolarmente al Responsabile della Qualità e volta ad individuare andamenti anomali, violazioni delle procedure e delle regolamentazioni, focalizzata sulla valutazione periodica dell'andamento della completezza, della funzionalità e dell'adeguatezza del sistema dei controlli interni e del sistema informativo. I controlli sono effettuati con cadenza prefissata;

4. **Attività di revisione esterna**, finalizzata a verificare la regolare tenuta della contabilità sociale e la redazione del bilancio di esercizio in conformità con i principii contabili applicabili ed affidata al Collegio Sindacale.

Con particolare riferimento ai rischi aziendali, e in particolare al rischio operativo, LumIT, in relazione all'attività svolta:

- presta particolare attenzione agli eventi di maggiore gravità anche se di scarsa frequenza, individuando le diverse forme e modalità con cui possono manifestarsi i rischi operativi, in relazione alle caratteristiche organizzative e operative che contraddistinguono la struttura di LumIT;

- valuta i rischi operativi connessi con l'introduzione di nuovi prodotti, attività, reti distributive, processi e sistemi rilevanti e con l'eventuale partecipazione, anche indiretta, a nuove iniziative imprenditoriali;
- si dota, con riferimento particolare alle attività svolte presso i clienti, e in sinergia con le necessità dei responsabili IT interni, di piani di emergenza e di continuità operativa che assicurano la propria capacità di operare su base continuativa e di limitare le perdite operative in caso di gravi interruzioni dell'attività.

In conclusione, LumIT ha istituito una serie di funzioni indipendenti di controllo di conformità alle norme, di gestione del rischio e di revisione interna, strutturate di modo che:

- dispongano dell'autorità, delle risorse e delle competenze necessarie ai loro compiti;
- i responsabili non siano gerarchicamente subordinati ai Responsabili delle Funzioni e degli uffici sottoposti a controllo e siano nominati direttamente dal CdA, di concerto con il Collegio Sindacale e sentito il CD;
- i responsabili riferiscano direttamente agli organi aziendali;
- il metodo per la determinazione della remunerazione di coloro che partecipano alle funzioni aziendali di controllo non ne comprometta l'obiettività.

Lo schema delle funzioni aziendali di controllo è pertanto così esemplificabile:

- **il Collegio Sindacale;**
- **l'Organismo di Vigilanza;**
- **il Responsabile della Qualità;**
- **il Responsabile EDP.**

3.1.2. L'Organismo di vigilanza

L'art. 6 del D. Lgs. 231 del 2001 prevede, quale esimente dalle responsabilità della persona giuridica accanto ai MOGC (se efficacemente attuati ed idonei), l'istituzione di un organismo di

controllo, denominato per l'appunto, Organismo di Vigilanza (di seguito, per brevità, **OdV**), dotato di autonomi poteri di iniziativa e di controllo, i cui compiti consistono:

- nell'effettuare verifiche su specifiche attività od operazioni individuate nelle singole aree di rischio, coordinandole con quelle riconosciute e affidate ai responsabili di unità, al fine di valutare l'osservanza e il funzionamento del MOGC;
- nel vigilare sull'osservanza delle norme da parte dell'intera organizzazione, e, di conseguenza, sui singoli comportamenti materiali che con la stessa possano porsi in contrasto;
- nel vigilare sull'adeguatezza e sull'aggiornamento dei protocolli rispetto alle esigenze di prevenzione dei reati;
- nel vigilare sul sistema di deleghe, al fine di garantire la coerenza fra i poteri conferiti e le attività in concreto espletate;
- nel promuovere adeguate iniziative volte alla diffusione della conoscenza e della comprensione del MOGC;
- nel valutare le segnalazioni di possibili violazioni e/o inosservanze del MOGC e di condotte illecite;
- nel coordinarsi con il CdA e il CD per valutare l'adeguatezza e le esigenze di aggiornamento del MOGC;
- nell'attivare e svolgere inchieste interne, raccordandosi di volta in volta con le Funzioni e gli Uffici interessati, per acquisire ulteriori elementi di indagine, anche in coordinamento con le altre funzioni di controllo.

Durante la propria attività l'Organismo di Vigilanza dovrà mantenere la massima discrezione e riservatezza, avendo come principale referente oltre che il CDA, il Collegio Sindacale e gli altri soggetti cui sono affidate le funzioni di controllo, un soggetto appositamente individuato in LumIT, anch'esso vincolato ai medesimi obblighi di discrezione e riservatezza.

L'OdV deve essere necessariamente dotato delle seguenti caratteristiche:

- **autonomia ed indipendenza**, requisiti fondamentali perché l'OdV non sia coinvolto in attività gestionali;
- **professionalità**, che garantisce l'adeguatezza delle competenze tecnico-professionali dei suoi membri;
- **continuità d'azione**, per curare l'attuazione del modello e assicurarne il continuo aggiornamento.

Considerate le attuali peculiarità societarie, gestionali ed economiche di LumIT, fotografate nel presente MOGC, si ritiene idoneo a svolgere le funzioni ad esso demandate dal D. Lgs. 231 del 2001 anche un **ODV a composizione monocratica**, purché dotato di tutti i requisiti sopra menzionati.

Il CDA attribuisce all'ODV tutti i poteri d'iniziativa e di controllo e le prerogative necessari per garantire all'Organismo la possibilità di svolgere l'attività di vigilanza sul funzionamento e sull'osservanza del Modello (e di aggiornamento dello stesso) in conformità a alle prescrizioni del D. Lgs. 231 del 2001.

a. L'attività di reporting dell'OdV.

L'attività dell'OdV dovrà essere caratterizzata da un'adeguata formalizzazione, con redazione di verbali idonei a documentare ogni riunione dello stesso a cura del segretario dell'OdV, nominato dall'OdV stesso nel corso delle varie sedute.

Ogni traccia degli interventi, così come ogni proposta avanzata al CdA e ogni attività di controllo eseguita dovrà essere adeguatamente documentata mediante la redazione di documenti digitali non modificabili, in modo da fornire un valido strumento in caso di possibili contestazioni, e da costituire riscontro evidente dei provvedimenti concreti adottati

dall'organizzazione al fine di scongiurare i rischi di commissione di uno dei reati ai sensi del D. Lgs. 231 del 2001.

L'Organismo di Vigilanza riferisce direttamente al Consiglio di Amministrazione in merito all'attuazione del Modello e alla rilevazione di eventuali criticità. Per una piena aderenza ai dettami del D. Lgs. 231 del 2001, l'Organismo di Vigilanza riporta direttamente al Consiglio di Amministrazione, in modo da garantire la sua piena autonomia ed indipendenza nello svolgimento dei compiti che gli sono affidati.
L'Organismo di Vigilanza presenta annualmente al Consiglio di Amministrazione il piano di attività per l'anno successivo, che potrà essere oggetto di apposita delibera e un rapporto consuntivo sull'attività svolta nell'anno trascorso.

L'OdV si doterà di un proprio regolamento interno, sottoposto al CdA per l'approvazione, nel quale saranno previsti e disciplinati:

- la durata in carica dell'OdV e le regole di eventuale rieleggibilità;
- le ipotesi tassative di revoca;
- le modalità con cui verranno effettuate le comunicazioni al CdA;
- i criteri che determinano la composizione dei suoi membri, i criteri che ne determinano la scelta, con l'indicazione dei requisiti di professionalità, onorabilità e indipendenza;
- il budget finanziario annuale;
- in relazione alle risorse impiegate, il ricorso a funzioni interne a LumIT, nonché a eventuali consulenti esterni;
- in relazione a potenziali situazioni di conflitto di interessi in cui possa venirsi a trovare un membro dell'OdV, la comunicazione al Presidente del CdA e del Collegio Sindacale di tale situazione, potenziale o attuale, con riferimento all'operazione, o alla categoria di operazioni potenzialmente a rischio;
- l'operatività in relazione agli aspetti organizzativi interni.

L'OdV si confronterà con l'EDP, e si coordinerà per un'azione di controllo efficace e non invasiva dell'attività delle differenti strutture di LumIT.

L'Organismo di Vigilanza propone al Consiglio di Amministrazione, sulla base delle criticità riscontrate, le azioni correttive ritenute adeguate al fine di migliorare l'efficacia del Modello.

In caso di urgenza o quando richiesto da un membro, l'Organismo di Vigilanza è tenuto a riferire immediatamente al Consiglio di Amministrazione in merito ad eventuali criticità riscontrate.

b. Il piano operativo dell'OdV.

Il piano operativo dell'OdV, allegato alla relazione annuale, definirà:

- le attività ispettive che l'OdV intende effettuare nel corso dell'anno o della frazione di anno;
- le risorse finanziarie impiegate;
- la pianificazione annuale degli interventi di verifica e di controllo e, se necessarie, le attività connesse con l'aggiornamento del modello;
- la dinamica delle segnalazioni e delle informazioni da e verso l'OdV.

Il CdA, in particolare, dovrà mettere a disposizione dell'OdV un'adeguata dotazione di risorse finanziarie, destinate all'OdV stesso, dalla quale attingere per ogni esigenza necessaria al corretto svolgimento dei compiti.

Un accurato rendiconto delle spese sarà presentato dall'OdV stesso all'atto della relazione finale annuale.

Inoltre, l'OdV collabora con l'Ufficio Amministrativo **nella programmazione della formazione dei dipendenti** con riferimento agli obblighi sanciti dal D. Lgs. 231 del 2001 (cfr. infra, 4.2).

c. I flussi informativi

I flussi informativi avranno carattere bidirezionale, ossia:

- i soggetti coinvolti nell'espletamento delle funzioni dirigenziali, amministrative e di controllo di LumIT, saranno tenuti a informare costantemente l'OdV;
- l'OdV sarà tenuto a relazionarsi costantemente con gli organi amministrativi e di controllo, anche al fine di stimolarne l'attività e di consentire di adottare gli eventuali provvedimenti di carattere sanzionatorio ovvero di altro genere che si rendessero necessari.

I flussi informativi hanno per oggetto informazioni e documenti che debbono essere portati a conoscenza dell'OdV. Gli Amministratori, i dirigenti, i dipendenti e i consulenti, nonché il Collegio Sindacale dovranno garantire la massima collaborazione all'OdV, provvedendo alla trasmissione di qualsiasi informazione utile per l'espletamento delle funzioni che gli sono proprie. Ad esempio, all'OdV dovrà essere comunicato il sistema delle deleghe e delle responsabilità operative (organigramma, funzionigramma e mansionario), e ogni modifica che dovesse intervenire sullo stesso.
Inoltre, sarà previsto uno specifico reporting funzionale da parte dei responsabili delle Funzioni e degli Uffici, secondo i seguenti principi:

- Redazione di relazioni periodiche, sull'attività svolta, particolarmente focalizzate:
  - Sui controlli effettuati;
  - Sulle modifiche suggerite a seguito di variazione dell'attività o delle procedure operative;
  - Sulle segnalazioni di eventuali nuove attività, da redigersi attraverso gli appositi documenti di sintesi denominati schede di evidenza;
- Tempestiva comunicazione in caso di gravi anomalie nel modello o di violazioni delle prescrizioni dello stesso nell'ambito dell'attività di routine o di una particolare attività.

Affinché i flussi informativi giungano tempestivamente a conoscenza dell'OdV, è prevista **un'apposita casella di posta elettronica dedicata** (ODV@LumIT.it), accessibile unicamente all'ODV, cui tutte le informazioni potranno essere inoltrate, nel pieno rispetto delle esigenze di segretezza e riservatezza aziendali, oltre che di tutela della privacy del mittente. L'indirizzo di posta elettronica sarà comunicato a tutti i dipendenti (apicali e sottoposti) con le medesime modalità previste per i MOGC.

Per quanto concerne le segnalazioni di condotte che integrano illeciti o violazioni del MOGC, al di fuori del reporting funzionale sopra citato, si rinvia a quanto previsto *infra* 4.3.3, in relazione all'ulteriore e specifico canale previsto dalla normativa in tema di *Whistleblowing*.

d. Riunioni e verbali

L'OdV stenderà un accurato verbale dell'attività svolta nel corso di ogni riunione. Il verbale, redatto a cura del Segretario dell'OdV e disponibile sia in formato cartaceo che digitale non modificabile, sarà oggetto di approvazione nel corso della seduta successiva, salva l'ipotesi in cui l'OdV sia a composizione monocratica (e sempre che non ne sia nel frattempo mutata la composizione).

Alle riunioni potranno essere chiamati, per le verifiche del caso, Responsabili delle Funzioni o degli Uffici, oltre che eventuali consulenti.

Tutte le informazioni e la documentazione raccolta, così come i verbali delle riunioni saranno custoditi in armadi chiusi e dedicati presso la sede di LumIT, a cura del Presidente dell'OdV.

L'esito delle attività di verifica, con l'evidenziazione degli eventuali profili di criticità/non conformità, e i suggerimenti circa le azioni da intraprendere, saranno inclusi nel rapporto consuntivo annuale al CDA.

3.1.3. Il responsabile della Qualità

Al Responsabile della qualità è assegnato il compito di verificare l'aderenza dell'operatività aziendale alle procedure e ai protocolli previsti dal **Manuale della qualità**.

Il Manuale ha lo scopo di descrivere, documentare, coordinare ed integrare la struttura organizzativa, le responsabilità e tutte le attività di LumIT, ed è uno strumento mediante il quale tutto il personale che opera nell'ambito della società deve essere posto nella condizione di conoscere, comprendere e, pertanto, attuare, gli impegni e gli obiettivi stabiliti nella politica della qualità. Esso, infatti, individua e descrive i processi che costituiscono il Sistema di Gestione per la qualità di LumIT e deve essere letto ed utilizzato integrando il contenuto delle sezioni con i documenti nella stessa richiamata.

Il Responsabile della qualità coadiuva i Consiglieri delegati nelle decisioni concernenti:

- Il campo di applicazione del sistema di gestione della qualità;
- I dettagli sulle eventuali esclusioni e relative giustificazioni;
- La politica della qualità;
- I processi del sistema di gestione e relative interazioni;
- Le modalità di svolgimento e le responsabilità specifiche delle attività e dei processi fondamentali al servizio (procedure operative documentate).

Attualmente il responsabile della qualità è OMISSIS.

3.1.4. Il responsabile dell'EDP

Il responsabile EDP o **Chief Information Officer (CIO)** è responsabile della funzione aziendale *information & communication technology*. Risponde direttamente ai consiglieri delegati.

Il suo compito principale è la direzione strategica dei sistemi informativi in LumIT in modo che si adattino al meglio ai processi aziendali e costituiscano un elemento di vantaggio competitivo a supporto delle attività della struttura.

Il responsabile EDP, in particolare, deve:

- raccogliere e razionalizzare le esigenze informatiche delle funzioni e degli uffici di LumIT;
- contribuire all'analisi e alla definizione dei processi aziendali;
- contribuire alla definizione dei requisiti funzionali e architetturali degli strumenti informativi;
- contribuire alla gestione del cambiamento dovuto all'introduzione di nuovi strumenti informativi;
- definire e gestire il budget destinato ai Sistemi Informativi;
- definire gli standard metodologici e tecnologici di riferimento;
- definire metriche (KPI, SLA) per la valutazione dell'efficienza interna e dei fornitori di software e servizi, ove necessari;
- organizzare e gestire il funzionamento quotidiano dei sistemi informativi.

Attualmente il responsabile è OMISSIS.

3.2. Comunicazione del Modello e formazione del personale

La **comunicazione verso l'interno del Modello** (compresi i relativi aggiornamenti ogni qualvolta vengano predisposti) e del Codice Etico è principalmente curata dal soggetto individuato dell'OdV come proprio referente in sinergia con l'Ufficio Amministrativo, attraverso i mezzi ritenuti più opportuni per la sua diffusione e conoscenza presso i tutti i dipendenti e collaboratori (apicali e sottoposti).

In particolare, la divulgazione potrà avvenire con le seguenti modalità:

- pubblicazione del Modello e del Codice Etico sull'intranet aziendale previo invio tramite posta elettronica dei riferimenti e dei collegamenti ai medesimi, chiedendo conferma di ricezione e correlata dichiarazione di impegno ad osservare le prescrizioni contenute nel MOGC e nel Codice Etico; per coloro che fossero eventualmente sprovvisti di posta elettronica, la comunicazione di tali riferimenti avverrà a cura dei soggetti sopra indicati i quali si faranno rilasciare apposita ricevuta (con sottoscrizione della correlata dichiarazione di impegno);

- qualora non fosse possibile la messa a disposizione tramite l'intranet aziendale, verrà consegnata una copia del Modello (in formato cartaceo od elettronico) a ciascun dipendente, previo rilascio di apposita ricevuta (con sottoscrizione della correlata dichiarazione di impegno).

Le medesime modalità dovranno essere seguite con riferimento alle risorse non presenti al momento dell'adozione del Modello e del Codice Etico (e relativi aggiornamenti).

Il **Codice Etico** dovrà altresì essere pubblicato sul sito internet della società. Riguardo al Modello ed ai suoi aggiornamenti, fermi restando gli obblighi di comunicazione a dipendenti e collaboratori, la scelta in ordine alla pubblicazione (anche solo in parte) è rimessa alle valutazioni della Società e alle sue esigenze di riservatezza e segretezza.
Per quanto concerne i ***partner* commerciali** di LumIT, essi dovranno impegnarsi formalmente a rispettare i principi del Codice Etico, per quanto applicabili, con conseguente risoluzione del contratto in essere in caso di gravi violazioni dei principi in esso stabiliti. Sarà pertanto necessario prevedere specifiche clausole contrattuali al riguardo, facendo espresso riferimento alla pubblicazione sul sito internet del Codice Etico.
È compito di LumIT, tramite l'Ufficio Amministrativo, con l'ausilio di esperti nelle discipline interessate dal Decreto ed in coordinamento con l'OdV, dare corso a specifici **piani di formazione**, con lo scopo di garantire l'effettiva conoscenza del Decreto, del Codice Etico e del Modello da parte dei dipendenti. L'erogazione della formazione deve essere differenziata in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano e dell'avere o meno funzioni di rappresentanza della Società.
La formazione del personale ai fini dell'attuazione del Modello è comunque obbligatoria per tutti i destinatari del medesimo.
LumIT garantisce la predisposizione di mezzi e modalità che assicurino sempre la tracciabilità delle iniziative di formazione e la formalizzazione delle presenze dei partecipanti, la possibilità di valutazione del loro livello di apprendimento e la valutazione del loro livello di gradimento del

corso, al fine di sviluppare nuove iniziative di formazione e migliorare quelle attualmente in corso, anche attraverso commenti e suggerimenti su contenuti, materiale, docenti, ecc.
La formazione, che può svolgersi anche a distanza o mediante l'utilizzo di sistemi informatici, e i cui contenuti sono vagliati dall'Organismo di Vigilanza, è operata da esperti nelle discipline dettate dal Decreto.

3.3. Whistleblowing

3.3.1. Introduzione

Con l'espressione "*whistleblowing*" si fa riferimento ad un'apposita procedura mediante la quale il destinatario del MOGC (il c.d. "*whistleblower*"), può segnalare una o più condotte illecite rilevanti ai sensi del Decreto, purché fondate su elementi di fatto precisi e concordanti, oppure violazioni del MOGC, di cui sia venuto a conoscenza in ragione delle funzioni svolte.
Tale procedura, già prevista in ambito pubblico per le amministrazioni ed enti equiparati (art. 54-bis D. Lgs. 165/2001), è stata introdotta nel settore privato dalla L. 179/2017. In particolare, i "nuovi" artt. 2 bis ss. dell'art. 6 del Dlgs. 231/2001 impongono il *whistleblowing* quale contenuto necessario del MOGC, stabilendo misure destinate ad incentivare la segnalazione degli illeciti e a tutelare il whistleblower da condotte ritorsive o altre conseguenze pregiudizievoli.

3.3.2. Destinatari ed ambito di applicazione

La procedura si applica a tutti i soggetti indicati nel comma 1 dell'art. 5 del Decreto (**soggetti apicali e soggetti sottoposti**).
Le segnalazioni devono riguardare condotte che possono integrare **i reati presupposto** previsti dal Decreto, oppure **violazioni del MOGC** e del Codice Etico, di cui il *whistleblower* sia venuto a conoscenza in ragione del rapporto di lavoro o collaborazione, ossia a causa o in occasione dello stesso. Poiché la procedura è finalizzata alla tutela della "integrità" dell'ente (cfr. art.6, comma 2 bis), il dipendente ricorre al *whistleblowing* unicamente nel caso in cui l'illecito abbia rilevanza generale e, quindi, interessi direttamente LumIT: al contrario una condotta penalmente

rilevante che interessi il solo dipendente e i cui effetti non si riverberino direttamente sull'intera società, non dovrà portare all'attivazione della speciale procedura.

Non sono prese in considerazione le segnalazioni fondate su meri sospetti o voci, né segnalazioni anonime (la procedura è infatti riferita esclusivamente alle segnalazioni provenienti da soggetti che si identificano, c.d. segnalazioni nominative).

3.3.3. La procedura di segnalazione

a. Contenuto

Il segnalante dovrà fornire tutti gli elementi utili affinché l'OdV possa procedere alle verifiche ed agli accertamenti a riscontro della fondatezza dei fatti oggetto della segnalazione. In particolare, dovranno essere presenti le seguenti informazioni:

- descrizione della condotta illecita;
- identità del soggetto che effettua la segnalazione, con indicazione di qualifica/funzione/ruolo svolto;
- chiara e completa descrizione dei fatti oggetto di segnalazione;
- qualora conosciute, le circostanze di tempo e di luogo in cui i fatti sono stati commessi;
- qualora conosciute, le generalità o altri elementi che consentano di identificare il soggetto che ha posto in essere i fatti segnalati;
- l'indicazione di eventuali soggetti che possano riferire sui fatti oggetto di segnalazione e di eventuali documenti che possano confermare la fondatezza dei fatti;
- ogni ulteriore informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

b. Modalità

La segnalazione dovrà **pervenire in forma scritta esclusivamente all'OdV**, in quanto dotato dell'indipendenza necessaria per garantire una piena tutela del *whistleblower*.

In aggiunta all'indirizzo e-mail utilizzabile in generale per i flussi informativi, è previsto un'ulteriore ed **apposito indirizzo di posta certificata** esterno ai sistemi telematici ed informatici aziendali, da utilizzarsi in via preferenziale allo scopo di ancor meglio garantire la riservatezza del segnalante (fatto salvo il reporting di *routine* da parte dei responsabili degli Uffici e delle Funzioni di cui *supra*, 4.1.2.3). Tale indirizzo deve essere comunicato a tutti i dipendenti (apicali e sottoposti) con le medesime modalità previste per la divulgazione del MOGC.

3.3.4. Verifica della fondatezza della segnalazione

L'OdV, anche attraverso il proprio referente, ha l'onere di valutare la fondatezza della segnalazione nel rispetto dei principi di imparzialità e riservatezza.

A tal fine, può richiedere l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati.

Di tali incontri va tenuta traccia, conservata in modo riservato.

Qualora dall'esito della verifica la segnalazione risulti non manifestamente infondata, l'OdV provvede a:

- inoltrare la segnalazione all'Autorità giudiziaria competente in caso di rilevanza penale dei fatti;
- trasmettere la segnalazione alle funzioni aziendali interessate, per l'acquisizione di elementi istruttori (solamente per le segnalazioni i cui fatti rappresentati non integrano ancora ipotesi di reato);
- trasmettere la segnalazione al Consiglio di Amministrazione;
- inoltrare la segnalazione alle funzioni competenti per i profili di responsabilità disciplinare, se esistenti.

L'OdV trasmette la segnalazione ai soggetti, così come sopra indicati, priva di tutte quelle informazioni/dati da cui sia possibile desumere l'identità del segnalante. Peraltro, tutti i soggetti che vengono a conoscenza della segnalazione sono tenuti alla riservatezza e all'obbligo di non divulgare quanto venuto a loro conoscenza, se non nell'ambito delle indagini giudiziarie.

L'OdV evidenzierà, qualora la segnalazione sia trasmessa a soggetti esterni, che si tratta di una segnalazione pervenuta da un soggetto al quale l'ordinamento riconosce una tutela rafforzata della riservatezza così come prevede la normativa vigente.

3.3.5. La tutela del whistleblower

L'identità del *whisteblower* viene protetta sia in fase di acquisizione della segnalazione che in ogni contesto successivo alla stessa, ad eccezione dei casi in cui l'identità debba essere rilevata per legge (es. indagini penali, tributarie o amministrative, ispezioni di organi di controllo, etc.).
L'identità del segnalante può essere rivelata ai soggetti responsabili della gestione dell'intero procedimento disciplinare e all'incolpato solo nei casi in cui:

- vi sia il consenso espresso del segnalante;
- la contestazione dell'addebito disciplinare risulti fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante risulti assolutamente indispensabile alla difesa dell'incolpato.

Tutti i soggetti che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza dell'identità del segnalante.
Nei confronti del dipendente che effettua una segnalazione non è consentita, né tollerata alcuna forma di ritorsione o misura discriminatoria (es. azioni disciplinari ingiustificate, molestie sul luogo di lavoro ed ogni altra forma di ritorsione che determini condizioni di lavoro intollerabili) diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati, direttamente o indirettamente, alla denuncia.
Il soggetto che ritiene di aver subito una discriminazione per il fatto di aver effettuato una segnalazione di illecito deve darne notizia circostanziata all'OdV che, valutata tempestivamente la sussistenza degli elementi, potrà segnalare l'ipotesi di discriminazione:

- al Responsabile dell'Ufficio di appartenenza del dipendente autore della presunta discriminazione il quale valuta tempestivamente l'opportunità e/o necessità di adottare tutti gli atti o i provvedimenti per ripristinare la situazione e/o per rimediare agli effetti

negativi della discriminazione e la sussistenza degli estremi per avviare il procedimento disciplinare nei confronti del dipendente autore della discriminazione;

- ai Consiglieri Delegati, qualora l'autore della discriminazione sia un Dirigente della Società;
- alla competente Procura della Repubblica, qualora si verifichino fatti penalmente rilevanti.

A tutela dei soggetti denuncianti la nuova legge stabilisce:

- l'adozione, nei modelli di organizzazione, di uno o più canali di segnalazione idonei a garantire la riservatezza dell'identità del segnalante;
- il divieto di atti ritorsivi o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi attinenti alla segnalazione, ad eccezione dei casi di falsa segnalazione;
- l'adozione di sanzioni disciplinari nei confronti di chi viola le misure di tutela del segnalante o di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Avverso l'adozione di eventuali misure ritorsive o discriminatorie, si prevede la possibilità di presentare denuncia all'Ispettorato nazionale del lavoro o ad una organizzazione sindacale e, in ogni caso, si stabilisce la nullità del licenziamento, del mutamento delle mansioni, nonché di qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante, con un inversione dell'onere della prova che pone in capo al datore di lavoro l'onere di dimostrare che l'irrogazione di sanzioni disciplinari o l'adozione di altra misura avente effetti pregiudizievoli nei confronti del segnalante (demansionamenti, licenziamenti, trasferimenti o altra misura organizzativa aventi effetti negativi) sia fondata su ragioni estranee alla segnalazione stessa.

L'art. 3, c. 1, L. 179/2017 contiene alcune disposizioni derogatorie in materia di segreto. Infatti, è previsto che il perseguimento dell'integrità dell'Ente e repressione degli illeciti penali costituiscono giusta causa per rivelare notizie, che normalmente sono coperte dall'obbligo del

segreto: come per es. il segreto d'ufficio (art. 326 c.p.), professionale (art. 622 c.p.), scientifico e industriale (art. 623 c.p.) e riconducibili all'obbligo di fedeltà dei lavoratori (art. 2105 c.c.).
Quindi, se nell'ambito di una procedura di whistleblowing, vengono rivelati **segreti tutelati dalla legge**, il dipendente non incorre in sanzioni di alcun tipo, poiché l'interesse alla repressione degli illeciti penali è considerato prevalente rispetto al diritto alla segretezza. La giusta causa sopra richiamata non opera, invece, se il soggetto tenuto al segreto professionale è venuto a conoscenza della notizia nell'ambito del rapporto di consulenza o assistenza con l'impresa (comma 2). In tale ipotesi l'eventuale rivelazione del segreto configura il reato.

3.3.6. La tutela della privacy

I dati personali raccolti nel procedimento di segnalazione verranno trattati nel rispetto della normativa vigente (D.lgs. 196/2003, anche in relazione alle modifiche apportate dal Reg. UE 679/2016).
In particolare, l'interesse legittimo del titolare del trattamento è fornito dall'interesse al corretto funzionamento della struttura e alla segnalazione degli illeciti, mentre la base giuridica è costituita dalla normativa specifica in materia di segnalazione degli illeciti.
Per quanto concerne la conservazione dei dati, gli stessi dovranno essere conservati sino al completo esaurimento della procedura, ferme restando le esigenze di giustizia.
Al momento della segnalazione pertanto deve essere fornita al segnalante una apposita informativa, riguardante il trattamento dei dati.

3.3.7. Responsabilità del whistleblower e di altri soggetti

La presente procedura non tutela il whistleblower in caso di segnalazione calunniosa o diffamatoria o comunque o di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate. Ulteriori responsabilità sono eventualmente accertate in capo al whistleblower in tutti i casi in cui non rispetti le prescrizioni di cui alla presente sezione (ad es. segnalazioni effettuate al solo scopo di danneggiare il denunciato, ecc.).

Ugualmente saranno passibili di sanzioni i soggetti che – comunque interessati al procedimento – non rispettano le prescrizioni fornite.

3.3.8. Sanzioni

In relazione a quanto previsto dalla L. 179/2017 sono sanzionabili le seguenti condotte:

- violazione delle misure di tutela del segnalante, come sopra riportate:
- effettuazione, con dolo o colpa grave di segnalazioni, che si rivelano infondate.

La disciplina sanzionatoria e il relativo procedimento è quella presente nell'apposita sezione del Modello («Misure disciplinari») a cui si rinvia, con riferimento ai vari soggetti interessati.

3.4. Misure disciplinari

Ai sensi dell'art. 6, comma 2, lett. e), e dell'art. 7, comma 4, lett. b), del D. Lgs. 231/2001, il Modello può ritenersi efficacemente attuato solo qualora preveda un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure in esso contenute.
Tale sistema disciplinare si rivolge ai lavoratori dipendenti, agli amministratori, ai collaboratori esterni, fornitori esterni e partner, prevedendo adeguate sanzioni di carattere disciplinare.
L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta e le procedure interne sono vincolanti per i destinatari, indipendentemente dall'effettiva realizzazione di un reato quale conseguenza di un comportamento posto in essere od omesso.

3.4.1. Presupposti

Costituisce violazione del MOGC qualsiasi azione o comportamento non conforme alle prescrizioni del Modello stesso e/o ai principi del Codice Etico, che ne costituisce parte integrante, ovvero l'omissione di azioni o comportamenti prescritti dal Modello, comprese le

prescrizioni dettate in materia di whistleblowing, nell'espletamento di attività nel cui ambito ricorre il rischio di commissione di reati contemplati dal Decreto.

3.4.2. Misure nei confronti degli Amministratori

In caso di violazione della normativa vigente o di mancato rispetto delle procedure interne previste dal Modello e dal Codice Etico da parte degli Amministratori di LumIT, l'OdV informerà il Collegio Sindacale e l'Assemblea dei Soci, che provvederanno ad assumere le opportune iniziative (fra tutte le azioni sociali o la revoca dell'incarico) previste dalla normativa vigente.

3.4.3. Misure nei confronti dei Dipendenti

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali dedotte nel presente Modello sono definiti **illeciti disciplinari**. La commissione di illeciti disciplinari comporta l'applicazione di sanzioni disciplinari da parte del datore di lavoro.

L'art. 2104 c.c., individuando il dovere di obbedienza a carico del lavoratore, dispone che nello svolgimento del proprio lavoro il prestatore di lavoro osservi le disposizioni di natura sia legale che contrattuale impartite dal datore di lavoro. In caso di inosservanza di dette disposizioni il datore di lavoro può irrogare sanzioni disciplinari, graduate secondo la gravità dell'infrazione, nel rispetto delle previsioni contenute nel Contratto Collettivo Nazionale di Lavoro – Commercio.

Il sistema disciplinare in ogni caso rispetta i limiti al potere sanzionatorio imposti dalla L. 300/1970 (cd. **Statuto dei Lavoratori**), ove applicabili, sia per quanto riguarda le sanzioni irrogabili, sia per quanto riguarda la forma di esercizio di tale potere.

In particolare, il sistema disciplinare deve:

- essere debitamente pubblicizzato mediante affissione in luogo accessibile ai dipendenti ed eventualmente essere oggetto di specifici corsi di aggiornamento e informazione;

- prevedere sanzioni conformi al principio di proporzionalità rispetto all'infrazione, la cui specificazione è affidata, ai sensi dell'art. 2106 c.c., alla contrattazione collettiva di settore. In ogni caso, la sanzione deve essere scelta in base:
  - all'intenzionalità del comportamento;
  - al grado di negligenza, imprudenza o imperizia evidenziata;
  - al pregresso comportamento del dipendente, con particolare riguardo alla sussistenza o meno di precedenti provvedimenti disciplinari;
  - alla posizione e alle mansioni svolte dal responsabile;
  - alle altre circostanze rilevanti, tra cui l'eventuale corresponsabilità, anche di natura omissiva, del comportamento sanzionato;
- tener conto del fatto che la multa non può essere di importo superiore a quattro ore della retribuzione di base;
- assicurare il diritto di difesa al lavoratore al quale sia stato contestato l'addebito (artt. 7 L. 300/1970, e 2106 c.c.). La contestazione dovrà essere tempestiva e il lavoratore potrà far pervenire, entro cinque giorni lavorativi da questa, all'Organismo di Vigilanza osservazioni scritte (oltre che ovviamente al datore di lavoro cui spetta in via esclusiva il potere sanzionatorio). In ogni caso i provvedimenti disciplinari più gravi del rimprovero verbale o scritto non possono essere applicati prima che siano trascorsi cinque giorni lavorativi dalla contestazione per iscritto del fatto che vi ha dato causa.

La sanzione irrogata dal datore di lavoro deve essere adeguata in modo da garantire l'effettività del MOGC. In particolare, le sanzioni disciplinari sono:

- **il rimprovero verbale o scritto**. Vi incorre il lavoratore che commetta violazioni di lieve entità, quali, ad esempio: l'inosservanza delle procedure prescritte; l'omissione ingiustificata dei controlli laddove prescritti; la mancata trasmissione di informazioni rilevanti all'OdV; più in generale, l'adozione di un qualsiasi comportamento non conforme a quanto prescritto dal modello;

- **la multa**. Vi incorre il lavoratore recidivo in relazione a qualsiasi violazione che comporti il rimprovero verbale o scritto, da considerarsi tale qualora la prima violazione gli sia stata contestata nei precedenti due anni;
- **la sospensione dal servizio e dalla retribuzione**. Vi incorre il lavoratore che, nel violare le procedure interne previste dal modello o adottando, in ogni caso, un comportamento non conforme alle prescrizioni del modello, compia atti contrari all'interesse della Società, arrecando danno alla stessa o esponendola ad una situazione oggettiva di pericolo per l'integrità dei propri beni (violazioni gravi).
- **la risoluzione del rapporto di lavoro per giustificato motivo**. Vi incorre il lavoratore che adotti comportamenti contrari all'interesse della Società, arrecando danno alla stessa o esponendola ad una situazione oggettiva di pericolo per l'integrità dei propri beni, che siano fortemente difformi da quanto stabilito nei protocolli del modello e pertanto siano da qualificarsi come particolarmente gravi; oppure il lavoratore recidivo (nei termini sopra descritti) in relazione alle violazioni gravi;
- **la risoluzione del rapporto di lavoro per giusta causa**. Vi incorre il lavoratore che palesemente ponga in essere azioni dirette in modo univoco al compimento di un reato contemplato dal D. Lgs. 231/2001.

Naturalmente, saranno seguite tutte le disposizioni e le garanzie previste dalla legge e dai contratti di lavoro in materia di procedimento disciplinare, e in particolare saranno rispettati:

- l'obbligo, in relazione all'applicazione di qualunque provvedimento disciplinare, della previa contestazione dell'addebito al dipendente e dell'ascolto di quest'ultimo in ordine alla sua difesa;
- l'obbligo, con la sola eccezione dell'ammonizione verbale, che la contestazione sia fatta per iscritto e che il provvedimento non sia emanato se non siano decorsi, dalla contestazione dell'addebito. i giorni specificatamente indicati per ciascuna sanzione nei contratti di lavoro.

Per quanto concerne l'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni, restano validi i poteri conferiti al Management di LumIT, nei limiti delle rispettive deleghe e competenze.

Tenendo conto che, in ogni caso, il giudizio su ogni comportamento deteriore è demandato al Consiglio di Amministrazione, il tipo e l'entità di ciascuna delle sanzioni sopra descritte saranno applicate anche tenendo conto:

- **dell'intenzionalità del comportamento**, del grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento;
- **del comportamento complessivo del lavoratore**, con particolare riferimento alla sussistenza di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge;
- **delle mansioni del lavoratore**;
- **della posizione funzionale e del livello di responsabilità ed autonomia delle persone coinvolte nei fatti costituenti la mancanza**;
- **delle altre particolari circostanze che accompagnano l'illecito disciplinare**.

3.4.4. Misure nei confronti di collaboratori, consulenti e altri soggetti terzi

Ogni comportamento posto in essere da collaboratori, consulenti, fornitori, partner o da altri terzi collegati a LumIT da un rapporto contrattuale diverso da quello di lavoro dipendente, che violi le previsioni del MOGC e/o del Codice Etico, potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere d'incarico, o anche in loro assenza, la risoluzione del rapporto contrattuale, fatta salva l'eventuale richiesta di risarcimento qualora da tale comportamento derivino danni alla società, anche indipendentemente dalla risoluzione del rapporto contrattuale.

PARTE II

MAPPATURA DEL RISCHIO E SPECIFICI PRESIDI

(PARTE SPECIALE)

1. PRINCIPI GENERALI

1.1 Orientamenti generali del Modello di Organizzazione, Gestione e Controllo

Di seguito sono indicate le fasi di elaborazione e di aggiornamento del MOGC di LumIT, predisposto avendo cura di considerare gli ambiti dell'attività ove posso essere commessi i reati previsti dal Decreto (di seguito, i Reati):

- **Inventariazione degli ambiti aziendali**. La "fotografia" degli ambiti aziendali di attività (per attività, per funzioni, per processi) comporta il compimento di una revisione periodica esaustiva della realtà aziendale, con l'obiettivo di individuare le aree che risultano interessate da possibili casistiche di reato. Nell'ambito di LumIT la mappatura degli ambiti aziendali è stata svolta per funzione, verificando i comportamenti che potrebbero integrare eventuali fattispecie penali.
- **Analisi dei rischi potenziali.** L'analisi dei rischi potenziali concerne le possibili modalità attuative dei Reati nelle diverse aree aziendali, e deve tenere conto sia della storia dell'ente, sia di possibili comparables, affini per settore e attività. Con riferimento ai reati di omicidio e lesioni colpose gravi o gravissime commessi con violazione degli obblighi di tutela della salute e della sicurezza sul lavoro, si dovrà fare riferimento alla valutazione dei rischi operata nel documento redatto secondo i criteri stabiliti dall'art. 28 ss. del D. Lgs. 81 del 2008.
- **Valutazione/predisposizione/adeguamento del sistema di prevenzione.** Le precedenti attività si completano con una valutazione del sistema di prevenzione dei

rischi già in essere presso LumIT, individuando le misure necessarie affinché esso si tale da garantire che i rischi di commissione dei reati siano ridotti ad un livello accettabile. Le componenti di un sistema di controllo idoneo ed efficace sono molteplici. Esse devono integrarsi in un sistema organico, nel quale non devono necessariamente essere tutte presenti, e dove la possibile debolezza di una componente può essere controbilanciata dal rafforzamento di una o più altre componenti in chiave compensativa, specie per le piccole imprese, per le quali potranno essere utilizzate solo alcune componenti di controllo, mentre altre potranno essere estremamente semplificate, oppure escluse in quanto già presenti nel modello aziendale.

- Ad ogni modo, il sistema dei controlli preventivi dovrà essere tale che lo stesso:
  - nel caso di reati dolosi, non possa essere aggirato se non con intenzionalità;
  - nel caso di reati colposi, incompatibili con l'intenzionalità fraudolenta, risulti comunque violato nonostante la puntuale vigilanza dell'OdV.

1.2. Struttura del Modello di Organizzazione, Gestione e Controllo

Tenuto conto delle dimensioni e dell'organizzazione di LumIT e dei possibili reati che possono essere commessi nello svolgimento delle attività della società (tra cui spiccano i c.d. reati informatici), il Modello si articola nelle seguenti componenti:

Sistemi di controllo preventivo dei reati dolosi:

- **Codice etico**;
- **Sistema organizzativo sufficientemente formalizzato e chiaro**, soprattutto per ciò che concerne l'attribuzione delle responsabilità, con particolare attenzione agli incentivi ai dipendenti, indispensabili per la costituzione di target di performance efficaci e calibrati sulle possibilità dei dipendenti stessi;
- **Procedure manuali ed informatiche**, per regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo, con particolare attenzione all'efficacia

preventiva rivestita dalla separazione di compiti fra coloro che svolgono fasi cruciali di un processo a rischio;

- **Poteri autorizzativi e di firma**, assegnati in coerenza con le responsabilità organizzative e gestionali, e prevedendo soglie di approvazione delle spese;
- **Sistema di controllo di gestione** in grado di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità generale e/o particolare. È necessaria la definizione di opportuni indicatori per le singole tipologie di rischio rilevato e di processi di risk assessment interni alle singole funzioni aziendali;
- **Comunicazione al personale e sua formazione**, che costituiscono requisiti essenziali del modello ai fini del suo funzionamento. In particolare, la comunicazione deve essere capillare, efficace, autorevole, chiara e dettagliata, periodicamente ripetuta.

Sistemi di controllo preventivo dei reati di omicidio doloso e lesioni personali colpose commesse in violazione delle norme di tutela della salute e sicurezza sul lavoro:

Per ciò che concerne le fattispecie colpose (dalle quali vanno esclusi i reati ambientali, alla luce del rischio estremamente ridotto nel caso di specie), oltre alle considerazioni già svolte con riferimento alle fattispecie dolose, si precisa che:

- **Il Codice Etico** è espressione della politica aziendale per la salute e la sicurezza sul lavoro e indica le convinzioni, la visione e i valori essenziali dell'azienda in tale ambito;
- **La struttura organizzativa** deve indicare i compiti e le responsabilità in materia di salute e di sicurezza sul lavoro definendoli in modo chiaro ed adeguatamente formalizzato in coerenza con lo schema organizzativo e funzionale della società, a partire dall'organismo di vertice fino all'ultimo dipendente, con particolare attenzione alle figure dell'RSPP - Responsabile del servizio di prevenzione e protezione, degli ASPP - Addetti al servizio di prevenzione e protezione e RLS – Rappresentante dei lavoratori per la sicurezza;

- **La formazione** è cruciale per sviluppare la consapevolezza della necessità che le proprie azioni siano conformi al modello organizzativo e delle conseguenze dei comportamenti che da esso si discostino;
- **La comunicazione e il coinvolgimento** sono anch'essi fondamentali, nella prospettiva della consapevolezza e dell'impegno necessari a tutti i livelli;
- **Gestione operativa**. Dall'analisi dei processi aziendali e delle loro interrelazioni e dai risultati della valutazione dei rischi deriva la definizione delle modalità per lo svolgimento in sicurezza delle attività che impattano in modo significativo sulla salute e sicurezza sul lavoro. In tale contesto, particolare attenzione deve essere prestata nei seguenti ambiti:
    - assunzione e qualificazione del personale;
    - organizzazione del lavoro e delle postazioni di lavoro;
    - acquisizione di beni e servizi impiegati dall'azienda e comunicazione delle opportune informazioni a fornitori e appaltatori;
    - manutenzione ordinaria e straordinaria;
    - qualificazione e scelta dei fornitori e degli appaltatori;
    - gestione delle emergenze.
- **Il sistema di monitoraggio della sicurezza** consiste in una fase di verifica dell'idoneità ed efficacia delle misure di prevenzione adottate. Esse dovranno essere oggetto di un monitoraggio pianificato che si svilupperà attraverso:
- la programmazione temporale delle verifiche;
- l'attribuzione di compiti e di responsabilità esecutive;
- la descrizione delle metodologie da seguire;
- le modalità di segnalazione delle eventuali situazioni difformi.

1.3. Principi

Il sistema dei controlli dovrà, in ogni caso, essere informato ai seguenti principi:

- **Ogni operazione, transazione azione deve essere verificabile, documentata, coerente e congrua**. Per ogni operazione deve cioè essere presente un adeguato

supporto documentale sulla base del quale si possa, in ogni momento, procedere all'effettuazione di controlli che attestino le motivazioni dell'operazione stessa e individuino chi abbia autorizzato, effettuato, registrato, verificato l'operazione stessa, in conformità alla normativa in tema di *privacy*.

- **Nessuno può gestire in autonomia un intero processo**. Il sistema dovrà garantire l'applicazione del principio di separazione di funzioni, per cui l'autorizzazione all'effettuazione di un'operazione deve essere avvenire sotto la responsabilità di una persona che sia diversa da chi contabilizza, esegue operativamente o controlla l'operazione.

  Inoltre, è indispensabile che:

  - a nessuno siano attribuiti poteri illimitati;
  - i poteri e le responsabilità siano chiaramente definiti e conosciuti all'interno dell'organizzazione;
  - i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative assegnate.

- **Documentazione dei controlli**. Il sistema di controllo deve documentare (mediante la redazione di verbali, anche standard) l'effettuazione dei controlli, anche di supervisione.

2. RISCHI E PRESIDI SPECIFICI

La cd. “parte speciale” del MOGC è riferita esclusivamente ai Reati che presentano rischi di verificazione non trascurabili, tenuto conto dell’operatività della società. Si precisa che per alcuni dei rimanenti Reati -rispetto ai quali peraltro sono spesso applicabili i medesimi presidi espressamente previsti dalla presente parte speciale per altre fattispecie- sono stati comunque previsti appositi presidi nel codice etico.

2.1 reati contro la pubblica amministrazione

Tabella 1. I reati contro la P.A legati all'impiego di denaro pubblico (art. 24 D. Lgs. 231/2001)

Reato	Sanzione per la persona giuridica	Misura interdittiva per la persona giuridica	Oggetto materiale della condotta
MALVERSAZIONE A DANNO DELLO STATO (ART. 316-BIS CP)	Fino a 500 quote; da 200 a 600 quote in caso di profitto di rilevante entità o in caso di danno di particolare gravità.	Divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi (art. 9, comma 2, lett. c, d ed e, D. Lgs. 231 del 2001)	Mancata destinazione di fondi pubblici allo scopo per il quale sono stati ottenuti.
INDEBITA PERCEZIONE DI EROGAZIONI A DANNO DELLO STATO (ART. 316-TER CP)	Fino a 500 quote; da 200 a 600 quote in caso di profitto di rilevante entità o in caso di danno di particolare gravità.	Divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi (art. 9, comma 2, lett. c, d ed e, D. Lgs. 231 del 2001)	Percezione indebita di erogazioni pubbliche mediante presentazione di dichiarazioni o documenti falsi, ovvero mediante presentazione di documenti falsi, ovvero mediante l'omissione di informazioni dovute.

TRUFFA AGGRAVATA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ART. 640, C. 2, N. 1 CP)	Fino a 500 quote; da 200 a 600 quote in caso di profitto di rilevante entità o in caso di danno di particolare gravità	Divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi (art. 9, comma 2, lett. c, d ed e, D. Lgs. 231 del 2001)	Procurare un profitto, per sé o per altri, inducendo in errore il soggetto con artifici o raggiri. In questo caso il soggetto passivo deve essere un ente pubblico.
TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (ART. 640-BIS CP)	Fino a 500 quote; da 200 a 600 quote in caso di profitto di rilevante entità o in caso di danno di particolare gravità	Divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi (art. 9, comma 2, lett. c, d ed e, D. Lgs. 231 del 2001)	Conseguire contributi, finanziamenti, mutui agevolati con artifici e raggiri, inducendo altri in errore.
FRODE INFORMATICA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (ART. 640-TER CP)	Fino a 500 quote; da 200 a 600 quote in caso di profitto di rilevante entità o in caso di danno di particolare gravità	Divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni o servizi (art. 9, comma 2, lett. c, d ed e, D. Lgs. 231 del 2001)	Procurare per sé o per altri un profitto (con altrui danno) alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, o intervenendo senza diritto su dati, informazioni o programmi contenuti in un sistema informatico.

Tabella 2. I reati contro la P.A. "del Pubblico Ufficiale" (art. 25 D. Lgs. 231/2001)

Reato	Sanzione per la persona giuridica	Misura interdittiva per la persona giuridica	Oggetto materiale della condotta
CORRUZIONE PER L'ESERCIZIO DELLA FUNZIONE (ART. 318 CP)	Fino a 200 quote	Nessuna	Accettazione della promessa o dell'offerta di denaro o di altra utilità per compiere un atto del proprio ufficio
CORRUZIONE IN ATTI GIUDIZIARI (ARTT. 319-TER E 322 CP)	Da 200 a 600 quote; da 300 a 800 quote in caso di aggravante.	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art. 9, comma 2, D. Lgs. 231 del 2001), da 4 a 7 anni se commesso da apicale oppure da 2 a 4 se commesso da dipendente. Ridotta se il reo mette a disposizione il prodotto del reato e fornisce i nominativi dei soggetti coinvolti.	Fatti di corruzione propria e impropria (artt. 318 e 319 c.p.) volti a favorire o danneggiare una parte in un processo civile, penale o amministrativo.
ISTIGAZIONE ALLA CORRUZIONE (ART. 322 CP)	Per i fatti ex art. 318 c.p., sanzioni pecuniarie fino a 200 quote; per quelli ex art. 319 c.p. da 200 a 600 quote	Esclusivamente per i reati ex art. 319 cp. Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali	Fatti di corruzione propria e impropria (artt. 318 e 319 c.p.) qualora la promessa o la dazione indebita non sia accettata dal

		alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art. 9, comma 2, D. Lgs. 231 del 2001), da 4 a 7 anni se commesso da apicale oppure da 2 a 4 se commesso da dipendente. Ridotta se il reo mette a disposizione il prodotto del reato e fornisce i nominativi dei soggetti coinvolti.	pubblico ufficiale o non sia prestata dal privato.
CORRUZIONE PER UN ATTO CONTRARIO AI PROPRI DOVERI DI UFFICIO AGGRAVATA (ARTT. 319 E 319-BIS CP)	Da 300 a 800 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art 9, comma 2, D. Lgs. 231 del 2001), da 4 a 7 anni se commesso da apicale oppure da 2 a 4 se commesso da dipendente. Ridotta se il reo mette a disposizione	Fatto di corruzione con il quale il PU/IPS omette o ritarda un atto del proprio ufficio oppure compie un atto contrario al proprio ufficio.

		il prodotto del reato e fornisce i nominativi dei soggetti coinvolti.	
INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ (ART. 319 – QUATER CP)	Da 300 a 800 quote.	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art 9, comma 2, D. Lgs. 231 del 2001), da 4 a 7 anni se commesso da apicale oppure da 2 a 4 se commesso da dipendente. Ridotta se il reo mette a disposizione il prodotto del reato e fornisce i nominativi dei soggetti coinvolti.	È punito il PU/IPS che, abusando della sua qualità o dei suoi poteri, induce taluno a dare o promettere indebitamente, denaro o altra utilità.
TRAFFICO DI INFLUENZE ILLECITE (ART. 346-BIS CP)	Fino a 200 quote	Nessuna	Ricorre allorquando taluno si serva di una relazione esistente con un PU/IPS per perseguire un indebito vantaggio (i cd. *favoritismi*).

2.1.1 Introduzione

a. Principi generali in materia di reati contro la PA

I reati in argomento sono suddivisibili in due gruppi, conformemente alla suddivisione topografica operata dal D. Lgs. 231/2001: da un lato, quelli che richiedono il necessario coinvolgimento del Pubblico Ufficiale o dell'Incaricato di Pubblico Servizio, e per tale motivo son definiti "reati propri" (art. 25); dall'altro, quelli che reprimono condotte fraudolente nei confronti della PA e possono essere commessi da chiunque (art. 24).

La distinzione operata dal D. Lgs 231/2001 non è casuale, ma è dettata dalla diversa consistenza dei beni giuridici coinvolti, infatti:
1) l'economia pubblica, intesa come corretta gestione delle risorse pubbliche destinate a fini di incentivazione economica, è il bene tutelato nei reati di cui all'art. 24 D. Lgs. 231/2001;
2) nelle fattispecie elencate all'art. 25 D. Lgs. 231/2001, l'interesse garantito è il regolare funzionamento della PA, nonché il prestigio degli Enti Pubblici, che trova la sua massima espressione nel principio del "buon andamento dell'Amministrazione", ai sensi dell'art. 97 Cost.

Il soggetto passivo degli illeciti in esame è la Pubblica Amministrazione, ossia l'insieme di Enti pubblici, diversamente qualificati (Stato, Regioni, Province, Comuni, etc.), e talvolta privati (ad es., concessionari, amministrazioni aggiudicatrici, S.p.A. miste, ecc.), che **perseguono a vario titolo l'interesse pubblico**.

Con esclusivo riferimento ai reati elencati all'art. 25, è opportuno approfondire le nozioni di Pubblico Ufficiale (di seguito, per brevità, "PU") e di Incaricato di Pubblico Servizio (di seguito, "IPS") cui fa riferimento il codice penale, al fine di garantire una migliore comprensione.

La nozione di Pubblico Ufficiale è fornita direttamente dal legislatore all' art. 357 cp: tale qualifica è riconosciuta a "*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 possono essere suddivisi in: legislativi, giudiziari e amministrativi.

Il ***potere legislativo*** trova la sua estrinsecazione nell'attività normativa vera e propria, ovvero in tutti quegli adempimenti accessori e/o preparatori a quest'ultima. Chiunque svolga la 'pubblica funzione legislativa', dunque, sia a livello nazionale che comunitario, è considerato PU.
I soggetti pubblici a cui, normalmente, può ricondursi tale tipo di funzione sono: il Parlamento; il Governo, nei limiti di cui agli artt. 76 e 77 Cost. (quando emana Decreti-Legge e Decreti Delegati); le Regioni, nelle materie indicate dall'art. 117 Cost.; gli organi dell'Unione Europea, a cui è affidata l'attività normativa, vale a dire il Consiglio e il Parlamento Europeo.

Il ***potere giudiziario*** trova la sua esplicazione nell'attività dello iusdicere lato sensu: sono dunque qualificabili come PU, non soltanto coloro che svolgono la vera e propria attività dello iusdicere stricto sensu (ovverosia i magistrati di ogni ordine e grado), bensì anche coloro che si occupano dell'attività amministrativa ad essa collegata, vale a dire i cancellieri, i segretari e i funzionari giudiziari. Sono ricompresi nella categoria pure i membri della Corte di Giustizia dell'UE, della Corte Europea dei Diritti Umani, della Corte dei Conti Comunitaria, e tutti i funzionari e gli addetti che svolgono la loro attività presso queste giurisdizioni.

Da ultimo, la ***pubblica funzione amministrativa*** si estrinseca mediante una serie di potestà avente carattere deliberativo, autoritativo e certificativo. Questi poteri fanno capo esclusivamente alla Pubblica Amministrazione e possono essere qualificati nei seguenti termini:

- ***il potere deliberativo*** consiste nella "formazione e manifestazione della volontà della Pubblica Amministrazione". La formula è interpretata in senso ampio, e ricomprende tutte

quelle attività che concorrano in qualunque modo ad estrinsecare la volontà della Pubblica Amministrazione; in tale prospettiva, sono stati qualificati come PU, non soltanto le persone istituzionalmente preposte ad esplicare tale potere ovvero i soggetti che svolgono le attività istruttorie o preparative all'iter deliberativo della PA, ma anche i loro collaboratori, saltuari ed occasionali;

- il ***potere autoritativo*** sussiste allorquando la legge riconosca alla PA la potestà di impartire veri e propri comandi ai destinatari. Questa posizione di "supremazia" della Pubblica Autorità è, ad esempio, facilmente individuabile nel potere della stessa di rilasciare, o meno, 'concessioni' ai privati;
- mediante il ***potere certificativo***, il PU accerta con piena certezza legale - fino a querela di falso - una determinata situazione sottoposta alla sua cognizione. È un potere che, in numerosi casi, la legge attribuisce anche ai privati (si pensi all'attività del Notaio)

L'art. 358 c.p. definisce gli incaricati di pubblico servizio come "*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*". Pertanto, l'IPS svolge una *'pubblica attività'* che, seppur non riconducibile ad alcuno dei '*poteri*' suesposti, non può ridursi a semplici mansioni d'ordine o alla prestazione di opera meramente materiale prive di alcun apporto intellettuale e discrezionale.
Gli IPS sono i dipendenti di enti, anche aventi natura privatistica, che forniscono un servizio pubblico (a titolo esemplificativo si possono citare i professori delle scuole primarie e secondarie; gli autisti di un'azienda di trasporto pubblico; ecc.).

La ricorrenza dei requisiti di cui sopra (sia per quanto riguarda i PU, che gli IPS) deve essere verificata, caso per caso, in ragione dell'effettiva attività svolta, poiché sono frequenti i casi in cui vi siano soggetti appartenenti alla medesima Amministrazione, i quali, tuttavia, espletano

funzioni o servizi: in tal caso, è evidente che la qualifica di PU/IPS possa essere attribuita dalla legge esclusivamente a chi svolge determinate mansione, ma non ad altri.

b. Principi generali dei Modelli destinati prevenire la commissione dei reati contro la PA

La presente sezione prevede l'espresso obbligo, in via diretta a carico degli esponenti aziendali e dei dipendenti, ma anche a carico dei collaboratori esterni e dei partner (mediante la previsione di apposite clausole contrattuali), di:

- osservare tutte le leggi e i regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione;
- gestire qualsiasi rapporto con la pubblica amministrazione sulla base di criteri di massima correttezza e trasparenza;
- evitare qualsiasi comportamento in evidente conflitto di interessi nei confronti della Pubblica Amministrazione, in relazione a quanto previsto dalle suddette ipotesi di reato.

Al fine di prevenire i comportamenti descritti nelle tabelle sopra riportate è necessario che:

- i rapporti nei confronti della pubblica amministrazione siano gestiti in modo unitario, individuando il responsabile per ogni operazione o pluralità di operazioni;
- gli accordi di associazione con i partner siano definiti per iscritto, con la precisazione che tutte le clausole del contratto associativo, concernenti le condizioni economiche necessarie per partecipare a procedure e bandi di gara della PA, siano proposte, verificate e approvate dal Consiglio di Amministrazione, ovvero dal Presidente e dal consigliere delegato, su delega specifica del CdA;
- gli incarichi conferiti a collaboratori esterni, a qualunque titolo, vengano redatti per iscritto, con l'indicazione del compenso pattuito, e, successivamente, proposti, verificati e approvati dal Consigliere delegato, o dal Consiglio di Amministrazione qualora si tratti di importi rilevanti;
- nessun tipo di pagamento può essere effettuato in contanti o in natura;

- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento di una delle seguenti attività, ossia pagamento di fatture, destinazione di finanziamenti ottenuti dallo Stato o da organismi comunitario, prestano particolare attenzione all'attuazione degli adempimenti stessi, riferendo immediatamente all'Organo di Vigilanza eventuali situazioni di irregolarità;
- in merito ad ogni singola attività sensibile vengono predisposte delle procedure con la relativa evidenza dei controlli in essere e viene effettuato un monitoraggio periodico delle procedure al fine di ottenere un aggiornamento tempestivo delle stesse, in virtù di nuove esigenze normative.

c. Modalità di predisposizione dei Modelli per i reati di cui agli artt. 24 e 25 del D. Lgs. n. 231/2001

Il complesso delle procedure e delle prassi aziendali che già oggi regolano le attività sensibili e i processi di supporto devono essere ulteriormente rivisti per migliorare ulteriormente la prevenzione dei reati, alla luce dei principi di controllo sotto enunciati. Tali principi indicano i requisiti del sistema organizzativo necessari per garantire una corretta gestione, nel rispetto degli obiettivi di conformità alle leggi/normative/procedure, nonché di efficacia e di efficienza.

Pertanto, la prevenzione dei reati, tramite l'adozione di tale Modello organizzativo, deve fondare i suoi presupposti:

- sulla costante verifica del rispetto delle procedure interne e dei vari livelli di controllo autorizzativi previsti;
- sul rafforzamento, potenziamento e rimozione di alcuni punti critici che l'attuale struttura organizzativa presenta e che tale modello intende eliminare.

2.1.2. I Modelli

a. I reati previsti dall'art. 24 D.Lgs. 231/2001

Malversazione ai danni dello Stato (art. 316-bis c.p.)

Risponde di questo reato chiunque, ottenendo contributi, sovvenzioni e finanziamenti dallo Stato, dall'Unione Europea o da qualsiasi altro ente pubblico destinati a favorire iniziative di pubblico interesse, non li destina alle predette finalità.
La pena prevista è la medesima sia per coloro che destinano i fondi per finalità diverse a quelle elencate nel bando, sia per coloro che non li utilizzino proprio.

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

Viene punito chiunque percepisca indebitamente finanziamenti, contributi, mutui agevolati o altre erogazioni dello stesso tipo comunque denominate erogati dallo Stato, dall'Unione Europea o da altri enti pubblici, mediante presentazione di dichiarazioni o documenti falsi, ovvero mediante presentazione di documenti falsi, ovvero mediante l'omissione di informazioni dovute.

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

Come nel reato di Indebita percezione di erogazione in danno dello Stato (art. 316-ter cp), la condotta è finalizzata ad ottenere erogazioni pubbliche, ma in questo caso è necessario un *quid pluris*, l'impiego di artifici e raggiri ad opera del soggetto agente.

Tale condotta, non dissimile da quella esaminata nel paragrafo precedente, se ne discosta in considerazione del fatto che gli artifici e i raggiri sono messi in atto al fine di conseguire specificatamente contributi, finanziamenti e mutui. Se il reo agisce per ottenere benefici differenti da quelli previamente elencati, ricorre, altrimenti, il reato di Truffa aggravata ai danni dello Stato.

Frode informatica (art. 640-ter c.p.)

Risponde del reato di frode informatica chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, o intervenendo senza diritto su dati, informazioni o programmi contenuti in un sistema informatico, procura per sé o per altri un profitto, con altrui danno.

L'alterazione del sistema informatico, quale condotta necessaria ai fini dell'integrazione del reato, è sovrapponibile a quella contemplata dai reati informatici, sicché sono applicabili i presidi predisposti per i suddetti (cfr. sezione "Reati informatici").

b. I reati previsti dall'art. 25 D. Lgs. 231/2001

Le fattispecie di reato:

Corruzione per l'esercizio della funzione (art. 318 c.p.)

È punito il PU (o l'IPS ex art. 320 c.p.) che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceva, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa, a prescindere da uno specifico atto del proprio ufficio.

Corruzione per un atto contrario ai doveri d'ufficio aggravata (319-bis c.p., in riferimento all'art. art. 319 c.p.)

La corruzione per un atto contrario ai doveri d'ufficio si realizza quando il PU (o l'IPS ex art. 320 c.p.), per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa.

Il D. Lgs. 231/2001 è applicabile unicamente in relazione alla fattispecie aggravata, la quale sussiste quando la condotta abbia 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 PU o l'IPS appartiene (art. 319-bis c.p.).

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

Di tale reato risponde chi pone in essere una delle condotte descritte agli artt. 318 e 319 c.p., per favorire o danneggiare una parte in un processo civile, penale o amministrativo. La fattispecie è aggravata qualora dal fatto derivi l'ingiusta condanna di taluno alla reclusione.

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

Il delitto in oggetto punisce il PU o l'IPS che, salvo che il fatto costituisca più grave reato, abusando della sua qualità o dei suoi poteri, induca taluno a dare o promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

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

Tale reato punisce chi offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, qualora l'offerta o la promessa non sia accettata e nel caso in cui l'offerta o la promessa sia fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a porre in essere un atto contrario ai suoi doveri.

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

È punito chiunque, sfruttando relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio, indebitamente faccia dare o promettere, a sé o ad altri, denaro o altro vantaggio patrimoniale, quale prezzo della propria mediazione illecita verso il pubblico ufficiale o l'incaricato di un pubblico servizio ovvero per remunerarlo, in relazione al compimento di un atto contrario ai doveri di ufficio o all'omissione o al ritardo di un atto del suo ufficio.
I delitti elencati precedentemente si applicano anche al caso in cui siano coinvolti in qualità di PU o IPS:

- membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee;

- i funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee;
- alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee;
- ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee;
- a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio;
- giudici, procuratori, procuratori aggiunti e funzionari della Corte Penale Internazionale.

Per effetto di quanto previsto dall'art. 321 c.p. o dalle singole fattispecie di reato, oltre che il PU o l'IPS, è punito anche il privato cd. "concorrente necessario".

È doveroso operare delle precisazioni circa i termini "dazione", "ricezione", "promessa" e "utilità", di frequente ricorso nei reati in esame:

- la "dazione" consiste nella consegna materiale di un determinato bene da parte del corruttore; laddove non siano integrati gli estremi della dazione, allora si configura una semplice promessa (che quindi è necessariamente prodromica alla dazione stessa);
- la "promessa", per avere rilevanza penale, deve essere ben individuata e suscettibile di attuazione. Nel caso in cui la promessa sia evidentemente impossibile, allora il reato non sussiste; si può, tuttavia, rispondere di tutte le fattispecie elencate nel caso in cui la promessa fatta sia verosimile, essendo sufficiente che il corrotto faccia affidamento su di essa;
- la "ricezione" ricorre quando il corrotto riceve il bene;
- il termine "utilità" è volutamente generico, e fa riferimento a qualsiasi tipo di bene patrimoniale e non (es. una prestazione sessuale) che può essere offerto.

2.2 Reati connessi agli infortuni sul lavoro

Tabella - I reati previsti dall'art. 25-septies D. Lgs. 231/2001

Reato	Sanzione per la persona giuridica	Misura interdittiva per la persona giuridica	Oggetto materiale della condotta
OMICIDIO COLPOSO COMMESSO CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO (ART. 589 COMMA 2, CP)	Da 250 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art. 9, comma 2, D. Lgs. 231 del 2001) per la durata non inferiore a tre mesi e non superiore ad un anno.	Omicidio colposo commesso con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.
LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSE CON VIOLAZIONE DELLE NORME ANTINFORTUNISTICHE E SULLA TUTELA DELL'IGIENE E DELLA SALUTE SUL LAVORO (ART. 590 COMMA 3 CP)	Fino a 250 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un	Lesioni gravi o gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.

		pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art. 9, comma 2, D. Lgs. 231 del 2001) per la durata non superiore a sei mesi	

2.2.1. I reati previsti dall'art. 25 septies del D.Lgs. n. 231/2001

La L. 3 agosto 2007, n. 123, ha introdotto l'art. 25 septies del D.Lgs. 8 giugno 2001, n. 231, a sua volta modificato dall'art. 300 del D. Lgs. 9 aprile 2008, n. 81, che prevede la responsabilità degli enti per i reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

a. Omicidio colposo commesso in violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 589, comma 2 c.p.)

Del reato in esame risponde il datore di lavoro allorquando la morte del lavoratore sia la conseguenza della violazione di una o più norme «per la prevenzione degli infortuni sul lavoro».

b. Lesioni colpose gravi o gravissime commesse in violazione delle norme sulla tutela della salute e sicurezza sul lavoro (art. 590, comma 3, c.p.)

Il reato si configura nel caso in cui si cagionino al lavoratore lesioni gravi o gravissime.

Le lesioni si considerano *gravi* nel caso in cui:

- dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;
- (oppure) il fatto produce l'indebolimento permanente di un senso o di un organo.

Le lesioni si considerano *gravissime* se dal fatto deriva (alternativamente):

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

Del reato risponde il datore di lavoro qualora la lesione grave o gravissima patita dal lavoratore sia la conseguenza della violazione di una o più norme «per la prevenzione degli infortuni sul lavoro».

In particolare, entrambi i reati sopra richiamati, ai fini del Decreto, sono ascrivibili al datore di lavoro unicamente nel caso in cui vi sia stata *violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene ed alla salute sul lavoro* (cd. colpa specifica). Tali norme sono innanzitutto individuate dal D.Lgs. 81/2008 (cd. TU Sicurezza) - oltre che in via generale dall'art. 2087 c.c - e nella normativa, anche di tipo tecnico, ad esso collegata.

2.2.2. I Modelli

a. Principi generali dei Modelli destinati a prevenire la commissione dei reati connessi agli infortuni sul lavoro

Le norme «per la prevenzione degli infortuni sul lavoro» prescrivono le condotte più disparate (dal generalissimo obbligo di adottare il documento di valutazione dei rischi, fino alle norme tecniche più dettagliate relative allo svolgimento di particolari attività).

In linea generale, i Modelli impongono:

- il rispetto degli *standard* tecnico-strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

- lo svolgimento delle attività di valutazione dei rischi e la conseguente predisposizione di misure preventive e protettive;
- l'osservanza di *standard* di natura organizzativa necessari per affrontare eventuali emergenze;
- lo svolgimento di attività di pronto soccorso;
- l'insegnamento di regole necessarie ai fini del coordinamento in materia di appalti;
- lo svolgimento di riunioni periodiche in materia di sicurezza, con conseguente consultazione dei rappresentati dei lavoratori per la sicurezza;
- lo svolgimento delle attività di sorveglianza sanitaria;
- lo svolgimento delle attività di informazione e formazione dei lavoratori;
- lo svolgimento delle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- lo svolgimento delle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni sul lavoro in sicurezza da parte dei lavoratori;
- l'acquisizione di documenti e certificazioni obbligatori di legge;
- stringenti controlli periodici e non in merito alla corretta applicazione ed efficacia delle procedure adottate.

I Modelli prevedono, altresì, l'espresso obbligo, in via diretta a carico degli esponenti aziendali, e tramite apposite clausole contrattuali a carico dei collaboratori esterni (in particolare per i collaboratori cui sono affidati compiti in tema di sicurezza dei lavoratori), oltre che dei *partner*, di:

- osservare tutte le leggi e i regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, in conformità alle Linee guida UNI-INAIL del 28 settembre 2001;
- gestire qualsiasi rapporto, anche con la pubblica amministrazione, con riferimento all'applicazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, sulla base di criteri di massima correttezza e trasparenza.

Conseguentemente, è sancito l'espresso divieto -in via diretta a carico degli esponenti aziendali, e a carico dei collaboratori esterni e *partner* da imporsi tramite apposite clausole contrattuali- di porre in essere:

- violazioni di norme antinfortunistiche idonee integrare le fattispecie di reato considerate (art. 25-septies D. Lgs. 231/2001);
- comportamenti che, sebbene non risultino tali da costituire di per sé le violazioni sopra considerate, potrebbero potenzialmente diventarlo.

Ai fini di prevenire la commissione dei reati oggetto della presente sezione è necessario che i soggetti apicali e coloro cui sono affidati compiti in materia di sicurezza dei lavoratori:

- conoscano ed osservino tutte le leggi ed i regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle disposizioni legislative in materia di sicurezza e salute dei lavoratori le cui norme di riferimento sono contenute nel D. Lgs. 81/2008, ossia il Testo Unico per la Sicurezza (di seguito, **Normativa per la sicurezza**);
- gestiscano qualsiasi rapporto inerente alla Normativa per la Sicurezza sulla base di criteri di massima sicurezza, correttezza, efficacia, efficienza, e trasparenza.

Per quanto attiene l'individuazione e l'analisi dei rischi potenziali, la quale dovrebbe considerare le possibili modalità attuative dei reati in seno all'azienda, le Linee Guida (di Confindustria) osservano, con riguardo alle fattispecie previste dalla L. n. 123/2007, che l'analisi delle possibili modalità attuative coincide con la valutazione dei rischi lavorativi effettuata dall'azienda sulla scorta della legislazione prevenzionistica vigente, ed in particolare dagli artt. 28 e ss. TU. In effetti, trattandosi di ipotesi di reato colpose, è evidente che i rischi di commissione del reato sono tendenzialmente coincidenti con i rischi di applicazione del Decreto in capo alla società, fatte salve eventuali interpretazioni della giurisprudenza volte ad interpretare in senso restrittivo i criteri di attribuzione della responsabilità alla società; così come sono tendenzialmente coincidenti le procedure destinate a prevenire il reato e l'illecito dell'ente.

Ai fini della redazione della presente Parte Speciale, LumIT ha considerato, pertanto, i fattori di rischio riportati nei Documenti di Valutazione Rischi (di seguito, anche 'DVR') redatti ai sensi della normativa vigente.

2.3 Reati societari

Tabella - I reati previsti dall'art. 25-ter D.Lgs. 231/2001

Reato	Sanzione per la persona giuridica	Misura interdittiva per la persona giuridica	Oggetto materiale della condotta
FALSE COMUNICAZIONI SOCIALI DI SOCIETÀ (ARTT. 2621 E 2621-BIS C.C.)	Da 200 a 400 quote per l'ipotesi disciplinata all'art. 2621 c.c. Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma). Da 100 a 200 quote per la fattispecie più lieve di cui all'art. 2621-bis c.c.	Nessuna	Esporre nelle comunicazioni sociali previste dalla legge fatti materiali non rispondenti al vero o omettere informazioni imposte dalla legge sulla situazione economica, patrimoniale o finanziaria della società. Il fatto può essere considerato di lieve entità (art. 2621-bis c.c.) tenendo conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta.
IMPEDITO CONTROLLO (ART. 2625, COMMA 2 C.C.)	Da 200 a 360 quote	Nessuna	Ostacolare o impedire mediante artifizi o raggiri (ad es. occultando documenti) lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali. Il reato sussiste unicamente nel caso in cui vi sia stato un danno nei confronti dei soci.
INDEBITA RESTITUZIONE DI CONFERIMENTI (ART. 2626 C.C.)	Da 200 a 360 quote. Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma).	Nessuna	Restituire ai soci i conferimenti, anche simulatamente, o liberarli dall'obbligo di eseguirli
ILLEGALE RIPARTIZIONE	Da 200 a 260 quote.	Nessuna	Ripartire utili o acconti su utili non effettivamente conseguiti o destinati

DEGLI UTILI E DELLE RISERVE (ART. 2627 C.C.)	Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma).		per legge, o per Statuto, a riserva, ripartizione di riserve, anche non costituite con utili, che non possono per legge essere distribuite
ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE (ART. 2628 C.C.)	Da 200 a 360 quote. Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma).	Nessuna	Sono puniti gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.
OPERAZIONI IN PREGIUDIZIO DEI CREDITORI (ART. 2629 C.C.)	Da 300 a 660 quote. Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma).	Nessuna	Riduzioni del capitale sociale, fusioni o scissioni che cagionino danno ai creditori.
FORMAZIONE FITTIZIA DEL CAPITALE (ART. 2632 C.C.)	Da 200 a 360 quote. Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma).	Nessuna	Aumentare fittiziamente il capitale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare dal capitale sociale, oppure mediante la sottoscrizione reciproca di azioni o quote, oppure mediante la sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione
INDEBITA RIPARTIZIONE DEI BENI SOCIALI DA PARTE DEI LIQUIDATORI (ART. 2633 C. C.)	Da 200 a 360 quote. Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma).	Nessuna	In caso di liquidazione dell'azienda, vengono puniti i liquidatori che ripartiscono i beni sociali tra i soci, piuttosto che soddisfare in via principale i creditori.

CORRUZIONE TRA PRIVATI (ART. 2635, COMMA 3 C.C.)	Da 400 a 600 quote. Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma).	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art. 9, comma 2, D. Lgs. 231 del 2001).	Offrire, promettere o dare denaro o altra utilità non dovuti ad un soggetto che riveste un ruolo di vertice in una società, perché compia od ometta un atto in violazione degli obblighi inerenti al suo ufficio o degli obblighi di fedeltà.
ISTIGAZIONE ALLA CORRUZIONE TRA PRIVATI (ART. 2635-BIS, COMMA 1 C.C.)	Da 200 a 400 quote Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma).	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni,	Risponde di questo reato chiunque offre o promette denaro o altra utilità non dovuti a soggetti apicali di una società perché compia od ometta un atto in violazione degli obblighi inerenti al suo ufficio o degli obblighi di fedeltà, qualora l'offerta o la promessa non sia accettata.

		finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art. 9, comma 2, D. Lgs. 231 del 2001).	
ILLECITA INFLUENZA SULL'ASSEMBLEA (ART. 2636 C.C.)	Da 300 a 660 quote. Se il profitto conseguito è di rilevante entità, la sanzione pecuniaria è aumentata di un terzo (art. 25-ter, u. comma).	Nessuna	Porre in essere atti simulati o fraudolenti che determinano la maggioranza in assemblea

2.3.1. Introduzione

a. Principi generali in materia di reati societari (soggetti attivi)

L'art. 25-ter del D. Lgs. n. 231 del 2001 individua specifiche ipotesi di reato in materia societaria. La previsione contenuta nella norma in esame è particolarmente complessa: a prescindere dalla moltitudine di illeciti penali elencati, non vi è uniformità circa i beni giuridici tutelati dalle diverse fattispecie.

Tuttavia, nonostante le profonde differenze tra le diverse fattispecie, di cui si darà conto, è possibile tracciare un profilo comune che consente a LumIT di introdurre anche dei presidi unici, accanto a presidi specifici per tipologie di reato. Infatti, si deve rilevare che la maggior parte delle fattispecie consiste in cd. reati propri: essi possono essere commessi esclusivamente da particolari categorie di soggetti, in particolare solo da soggetti in posizione apicale. Inoltre, anche qualora le fattispecie non richiedano una particolare qualifica soggettiva, nella prassi tali reati tendenzialmente potranno essere commessi solo da chi si trova in posizione di vertice, fatte salve alcune eccezioni (in particolare la corruzione tra privati che, per quanto collocata tra

i reati societari, presenta numerose peculiarità, tali per cui alla medesima sono efficacemente applicabili alcuni dei presidi già previsti per la prevenzione dei reati contro la PA, per quanto l'interlocutore sia il rappresentante di una società privata, anziché un funzionario pubblico).

b. Principi generali dei modelli destinati a prevenire la commissione dei reati societari

Fermo restando l'obbligo di LumIT di vigilare sull'intera attività aziendale, vi sono delle attività soggette ad un maggior rischio di commissione dei reati societari, ed in particolare:

- l'approvazione del bilancio d'esercizio o di situazioni patrimoniali;
- la gestione dei rapporti tra Soci, Revisori e Sindaci;
- la tenuta della contabilità generale e dei libri sociali;
- la redazione del bilancio di esercizio;
- la gestione di qualsivoglia adempimento in materia societaria quale, a titolo esemplificativo, la predisposizione di verbali e della documentazione da fornire all'Assemblea dei soci.

La presente sezione prevede l'espresso obbligo per coloro che rivestono un ruolo di vertice, principalmente gli amministratori, sindaci e i dirigenti preposti alla tenuta della contabilità, di conoscere e rispettare:

- i principi di ***Corporate Governance*** approvati dagli organi sociali di LumIT;
- le regole dettate in materia di controlli, procedure aziendali, documentazione e le disposizioni inerenti la ***struttura gerarchico-funzionale***, ***aziendale*** e ***organizzativa*** di LumIT e quelle richieste dal sistema di controllo di gestione;
- le normative interne inerenti al funzionamento del sistema informatico di LumIT.

Nell'ambito dei suddetti settori, è tassativamente imposto di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio di esercizio e delle altre comunicazioni sociali, al fine di fornire ai soci e ai

terzi un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della LumIT;

- tenere un comportamento corretto e trasparente, assicurando il pieno rispetto delle norme di legge e dei regolamenti, nonché delle procedure aziendali interne, nell'acquisizione, elaborazione e comunicazione dei dati e delle informazioni necessarie per consentire un fondato giudizio sulla situazione patrimoniale, economica e finanziaria della LumIT e sull'evoluzione delle relative attività;
- osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità e dell'effettività del patrimonio e del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in generale;
- assicurare il regolare e trasparente funzionamento della società e degli organi sociali, garantendo e agevolando ogni forma di controllo interno sulla gestione della società stessa;
- astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false e non corrette, idonee a provocare una sensibile distorsione dei risultati economici, patrimoniali e finanziari conseguiti da LumIT;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità, non frapponendo alcun ostacolo all'esercizio delle funzioni da queste esercitate.

Inoltre, è fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato considerate nella tabella sopra riportata;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire, di per sé, fattispecie di reato, possano potenzialmente diventarlo.

2.3.2. I Modelli

I reati previsti dall'art. 25-ter D.Lgs. 231/2001

a. False comunicazioni sociali (artt. 2621 e 2621-bis c.c.)

Sono puniti gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori che, nei bilanci, nelle relazioni o in altre comunicazioni sociali dirette ai soci o al pubblico, consapevolmente espongono fatti materiali rilevanti non rispondenti al vero oppure omettono fatti rilevanti la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società idoneo ad indurre altri in errore.

Sono altresì punite le falsità o le omissioni riguardanti beni posseduti o amministrati dalla società per conto di terzi.

I fatti possono essere valutati dal Giudice «di lieve entità» ai sensi dell'art. 2621-bis c.c. (con conseguente riduzione della sanzione per la persona fisica e giuridica), «tenuto conto della natura e delle dimensioni della società e delle modalità o degli effetti della condotta».

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

Del reato rispondono gli amministratori che ostacolano o impediscono mediante artifizi o raggiri (ad es. occultando documenti) lo svolgimento delle attività di controllo legalmente attribuite ai soci o ad altri organi sociali. Il reato sussiste unicamente nel caso in cui vi sia stato un danno nei confronti dei soci (comma 2): qualora sia configurabile un pregiudizio solo per la compagine sociale, la condotta integra gli estremi di un mero illecito amministrativo (senza responsabilità della società ai sensi del Decreto).

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

Il reato si configura allorquando si proceda, fuori dei casi di legittima riduzione del capitale sociale, alla restituzione, anche simulata, dei conferimenti ai soci o alla liberazione degli stessi dall'obbligo di eseguirli.

I soggetti attivi del reato sono gli amministratori, tuttavia anche i soci beneficiari della restituzione o della liberazione possono concorrere nel reato, ai sensi dell'art. 110 c.p., qualora abbiano svolto un'attività di determinazione o istigazione della condotta illecita degli amministratori.

d. Illegale ripartizione degli utili (art. 2627 c.c.)

Il reato si configura allorquando si proceda alla ripartizione di utili, o acconti sugli utili, non effettivamente conseguiti o destinati per legge a riserva, ovvero alla ripartizione di riserve, anche non costituite con utili, che per legge non possono essere distribuite.

La norma intende impedire:

- che la Società distribuisca utili che non si sono verificati, ovvero che, pur essendosi realizzati, siano vincolati per legge o per Statuto a riserva;
- che siano ripartite riserve intangibili *ex lege*.

Dal momento che le riserve e il capitale sociale rappresentano spesso l'unica forma di garanzia per i creditori e i soci, tale disposizione è dettata in particolar modo nel loro interesse, oltre che a difesa della società stessa.

Con la locuzione utili non effettivamente conseguiti, il legislatore ha inteso utili non reali, quindi prescindendo dal concetto di liquidità, di modo che la loro distribuzione rappresenta, negli effetti, una restituzione del capitale sociale o delle riserve.

Soggetti attivi del reato sono gli amministratori, tuttavia i soci beneficiari della ripartizione degli utili o delle riserve possono concorrere nel reato, ai sensi dell'art. 110 c.p., qualora abbiano svolto un'attività di determinazione o istigazione della condotta illecita degli amministratori.

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

La fattispecie di reato punisce gli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote sociali, cagionando una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

La stessa pena si applica agli amministratori che, fuori dei casi consentiti dalla legge, acquistano o sottoscrivono azioni o quote emesse dalla società controllante, cagionando una lesione del capitale sociale o delle riserve non distribuibili per legge.

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

Il reato si configura allorquando siano realizzate riduzioni di capitale sociale, fusioni con altre società o scissioni attuate in violazione delle disposizioni di legge e che cagionino danno ai creditori.

Soggetti attivi del reato sono gli amministratori.

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

Il reato si configura allorquando si proceda alla formazione o all'aumento in modo fittizio del capitale sociale tramite:

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

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

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

In caso di liquidazione dell'azienda, vengono puniti i liquidatori che ripartiscono i beni sociali tra i soci, piuttosto che soddisfare in via principale i creditori o accantonare somme necessarie a soddisfare questi ultimi, con conseguente danno per i creditori medesimi.

i. Corruzione tra privati (art. 2635, comma 3 c.c.)

Il richiamo operato dall'art. 25-ter D. Lgs. 231/2001 al solo comma 3 dell'art. 2635 c.c. configura l'illecito dell'ente solo in relazione alla condotta di chi, anche per interposta persona, offra, prometta o dia denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori di società o enti privati, per compiere o per omettere un atto in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà.

La *ratio* della norma è evidente: si vuole sanzionare l'ente unicamente nel caso in cui si ponga quale "corruttore". Non si è ritenuto di applicare alcuna sanzione nel caso in cui la Società sia il soggetto passivo e, quindi, assuma il ruolo del "corrotto": in tal caso, l'azienda verrebbe danneggiata dalla condotta del proprio amministratore, sicché non si configurerebbe un illecito posto in essere nell'interesse o a vantaggio dell'ente.

l. Istigazione alla corruzione tra privati (art. 2635-bis, comma 1 c.c.)

Tale delitto punisce chiunque offre o promette denaro o altra utilità non dovuti agli amministratori, ai direttori generali, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci e ai liquidatori, di società o enti privati, nonché a chi svolge in essi un'attività lavorativa con l'esercizio di funzioni direttive, affinché compia od ometta un atto in violazione degli obblighi inerenti al proprio ufficio o degli obblighi di fedeltà, qualora l'offerta non sia accettata.

Per quanto sia punibile anche il tentativo da parte del soggetto apicale, che sollecita vanamente la dazione o la promessa, in tale ipotesi non trova applicazione il Decreto (per le medesime ragioni appena viste: in questa ipotesi l'apicale agirebbe per definizione contro l'interesse della società).

m. Illecita influenza sull'assemblea (artt. 2636 c.c.)

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

2.4. Reati di ricettazione, riciclaggio, impiego di denaro beni utilità di provenienza illecita e Autoriciclaggio

Tabella - I reati previsti dall'art. 25-octies D.Lgs. 231/2001

Reato	Sanzione per la persona giuridica	Misura interdittiva per la persona giuridica	Oggetto materiale della condotta
RICETTAZIONE (ART. 648 CP)	Da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengano da delitto per il quale sia stabilita la pena della reclusione superiore nel massimo a cinque anni, si applica la sanzione da 400 a 1000 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art. 9, comma 2, D. Lgs. 231 del 2001) per la durata non superiore a due anni,	Ricezione, occultamento, acquisto di denaro o cose provenienti da qualsiasi delitto, da parte di chi non ha avuto alcun ruolo nella commissione di tale delitto
RICICLAGGIO (ART. 648 BIS CP)	Da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengano da delitto per il quale sia stabilita la pena della reclusione superiore nel massimo a cinque anni, si applica la sanzione da 400 a 1000 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio;	Sostituzione o trasferimento di denaro, beni o altra utilità provenienti da delitto non colposo, oppure compimento di altre operazioni in modo da ostacolare l'identificazione della provenienza delittuosa, da parte di chi non ha avuto alcun ruolo nella

		esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art. 9, comma 2, D. Lgs. 231 del 2001) per la durata non superiore a due anni.	commissione di tali delitti.
IMPIEGO DI DENARO, BENI O ALTRA UTILITÀ DI PROVENIENZA ILLECITA (ART. 648 TER CP)	Da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengano da delitto per il quale sia stabilita la pena della reclusione superiore nel massimo a cinque anni, si applica la sanzione da 400 a 1000 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio; esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art. 9, comma 2, D. Lgs. 231 del 2001) per la durata non superiore a due anni.	Impiego in attività economiche e finanziarie di denaro di provenienza illecita, da parte di chi non ha avuto alcun ruolo negli illeciti presupposti
AUTORICICLAGGIO (ART. 648-TER.1 CP)	Da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengano da delitto per il quale sia stabilita la pena della reclusione superiore nel massimo a cinque anni, si applica la sanzione da 400 a 1000 quote.	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di contrattare con la P.A., salvo che per ottenere le prestazioni di un pubblico servizio;	Viene punito chiunque, avendo commesso o concorso a commettere un delitto non colposo, compie atti di riciclaggio in relazione a tale delitto.

		esclusione da agevolazioni, finanziamenti, contributi o sussidi, e l'eventuale revoca di quelli già concessi; divieto di pubblicizzare beni e servizi (art 9, comma 2, D. Lgs. 231 del 2001) per la durata non superiore a due anni.	

2.4.1. Introduzione

a. La normativa antiriciclaggio in generale

L'art. *25-octies* è stato inserito nel *corpus* del D. Lgs. 231/2001 da parte del D. Lgs. 231/2007 (cd. "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione").

Per quanto il cd. "decreto antiriciclaggio" sia finalizzato a prevenire operazioni di riciclaggio da parte degli operatori finanziari, la responsabilità delle persone giuridiche è configurabile anche in relazione a qualsiasi tipo di società in applicazione del principio del c.d. *risk based approach*, che impone l'individuazione, oltre alle consuete aree di rischio, anche delle specifiche operazioni che possono far presumere l'utilizzo di denaro o altre utilità provenienti da attività illecite. I Modelli, pertanto, dovranno dettare delle stringenti regole ispirate ai canoni della rintracciabilità del rischio e della trasparenza.

Infine, merita di essere evidenziata la particolare natura di questi illeciti, i quali, nella maggior parte dei casi, non vedono coinvolti unicamente soggetti appartenenti alla Società, ma altresì figure estranee. Per questo motivo, la Confindustria (con le Linee Guida del 2014) ha sollecitato le imprese ad estendere le misure di controllo anche ai soggetti terzi (fornitori e clienti) che entrano in contatto con queste.

b. Principi generali destinati a prevenire i delitti di riciclaggio

Ai fini della prevenzione dei reati sopra rubricati, LumIT prevede l'espresso divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato di riferimento;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Inoltre, è fatto obbligo ai destinatari di conoscere e rispettare:

- i principi *di Corporate Governance* approvati dal CdA che rispecchiano le normative applicabili e le pratiche internazionali in relazione alla prevenzione del riciclaggio;
- le procedure aziendali, la documentazione e le disposizioni inerenti alla struttura gerarchico-funzionale, aziendale ed organizzativa della Società ed il sistema di controllo di gestione;
- le norme inerenti al sistema amministrativo, contabile, finanziario, di *reporting*;
- le norme interne inerenti all'uso e il funzionamento del sistema informativo di LumIT.

2.4.2. I modelli

I reati previsti dall'art. 25-octies D.Lgs. 231/2001

a. Ricettazione (art. 648 c.p.)

È punito chi, fuori dai casi di concorso nel reato, al fine di procurare a sé o ad altri un profitto, acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto, o comunque si intromette nel farle acquistare, ricevere od occultare.

b. Riciclaggio (art. 648-bis c.p.)

Risponde di questo reato chiunque, fuori dai casi di concorso nel reato, sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo, ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa.

c. Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.)

Viene punito chi, fuori dai casi di concorso nel reato e dei casi previsti dagli artt. 648 e 648-bis cp, impiega in attività economiche o finanziarie denaro, beni o altre utilità provenienti da delitto.

d. Autoriciclaggio (art. 648-ter1 c.p.)

La fattispecie in oggetto, di recente introduzione, costituisce un cd. reato proprio, e dunque può essere posto in essere esclusivamente da colui che ha partecipato alla commissione del delitto non colposo, da cui è derivato il provento oggetto di reinvestimento.
In particolare, tale fattispecie di reato è integrata da chi, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa.
Ai fini dell'integrazione dell'illecito in esame possono essere poste in essere tre diverse tipologie di condotte, aventi come oggetto denaro o altre utilità provenienti dalla commissione di un delitto non colposo, ossia:

- la sostituzione: attività dirette a separare la condotta da ogni possibile collegamento con il reato;
- il trasferimento: attività di spostamento dei valori di provenienza delittuosa da un soggetto ad un altro o da un luogo ad un altro, in maniera tale da farne perdere traccia, relativamente all'origine e alla provenienza;
- l'impiego: attività con il quale la Società potrebbe reinvestire il denaro o le altre utilità provenienti da delitto; svolgere operazioni di ricapitalizzazione ecc.

La pena è diminuita fino alla metà per chi si sia efficacemente adoperato per evitare che le condotte siano portate a conseguenze ulteriori o per assicurare le prove del reato e l'individuazione dei beni, del denaro e delle altre utilità provenienti dal delitto.

2.5. Reati informatici

Tabella 1 - I reati previsti dall'art. 24-bis D. Lgs 231/2001

Reato	Sanzione per la persona giuridica	Misura interdittiva per la persona giuridica	Oggetto materiale della condotta
ACCESSO ABUSIVO A SISTEMA INFORMATICO E TELEMATICO (ART. 615 TER CP)	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. a, b ed e, D. Lgs. 231 del 2001)	Accedere abusivamente ad un sistema informatico o telematico, o mantenersi al suo interno contro la volontà di chi ha il diritto di escluderlo.
INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUATER CP)	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. a, b ed e, D. Lgs. 231 del 2001)	Intercettare, impedire o interrompere comunicazioni informatiche.
INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617-QUINQUIES CP)	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. a, b ed e, D. Lgs. 231 del 2001)	Installare apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635-BIS CP)	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. a, b ed e, D. Lgs. 231 del 2001)	Distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici altrui.
DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI UTILIZZATI DALLO STATO O DA ALTRO ENTE PUBBLICO O COMUNQUE DI PUBBLICA UTILITÀ (ART. 635-TER CP)	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. a, b ed e, D. Lgs. 231 del 2001)	Distruggere, deteriorare, cancellare, alterare o sopprimere, informazioni, dati o programmi informatici utilizzati dallo Stato o da enti pubblici.
DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635-QUATER CP)	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. a, b ed e, D. Lgs. 231 del 2001)	Distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici.
DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (ART. 635-QUINQUIES CP)	Da 100 a 500 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. a, b ed e, D. Lgs. 231 del 2001)	Distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici utilizzati dallo Stato o da enti pubblici

DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615-QUATER CP)	Fino a 300 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. a, b ed e, D. Lgs. 231 del 2001)	Procurarsi o diffondere abusivamente codici di accesso a sistemi informatici.
DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (ART. 615-QUINQUIES CP)	Fino a 300 quote	Interdizione dall'esercizio dell'attività; sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. a, b ed e, D. Lgs. 231 del 2001)	Diffondere apparecchiature, dispositivi o programmi diretti a danneggiare un sistema informatico o telematico

Tabella 2 - Il reato previsto dall'art. 1, comma 11 D.L. 105/2019, convertito con modificazione dalla L. 133/2019

Reato	Sanzione per la persona giuridica	Misura interdittiva per la persona giuridica	Oggetto materiale della condotta
VIOLAZIONE DELLE DISPOSIZIONI CONTENUTE NEI COMMA 2, LETT. B), 6 LETT. A) E 6 LETT. C) DELL'ART. 1 DEL D.L. 105/2019 (ART. 1, COMMA 11 DEL D.L. 105/2019)	Fino a 400 quote	Nessuna	In attesa di compiuta definizione con D.M. da parte del Ministro delle Infrastrutture, in relazione a condotte attinenti alla sicurezza nazionale cibernetica

2.5.1. Introduzione

a. I reati informatici in generale

La responsabilità delle persone giuridiche in relazione ai reati informatici (i c.d. *cybercrime*) è prevista dall'art. 24-*bis*, D. Lgs. 231/2001.

All'inizio degli anni Novanta, in linea con la crescente diffusione degli apparecchi informatici, è sorta l'esigenza di regolamentare le nuove realtà tecnologiche, anche sul piano penalistico. Il legislatore si è posto l'obiettivo di prevenire e reprimere una moltitudine di nuove condotte criminose emerse nella società; tuttavia, il raggiungimento di tale obiettivo si è rivelato particolarmente difficoltoso, poiché i reati di cui trattasi ledono (o quantomeno mettono in pericolo) una serie di beni giuridici estremamente differenti tra di loro (solo approssimativamente riassumibili nei concetti di "*riservatezza informatica*" e "*sicurezza informatica*").

La riservatezza informatica

Si tratta del bene giuridico tutelato dai reati informatici per antonomasia.

Da un lato, la riservatezza informatica assurge al rango di diritto fondamentale della persona, da intendersi quale diritto ad uno spazio informatico esclusivo che, a prescindere dai contenuti che vi siano presenti, deve essere lasciato *libero da intrusioni* e da *manomissioni* di terzi; pertanto è strumento essenziale per la piena realizzazione della persona nell'odierna vita individuale e sociale, che neppure l'Autorità Pubblica può violare o comprimere, se non nei casi e modi previsti tassativamente dalla legge e con le garanzie del controllo giudiziario (come diffusamente sostenuto dalla Dir. 2012/29/UE). Dall'altro lato, si distingue dalla *privacy* in senso stretto, che indica il più specifico diritto alla tutela dei propri "dati personali", ovunque e da chiunque siano trattati, richiedendo complesse discipline di tutela, finalizzate a garantire la possibilità di controllo da parte della persona cui si riferiscono le informazioni, ed il bilanciamento con la contrapposta esigenza di circolazione e di accessibilità anche da parte di terzi, in quanto elementi spesso essenziali per infinite attività e servizi in ogni settore della

società contemporanea. Le tecnologie informatiche ne hanno infatti determinato, per un verso, la grande estensione e facilità di raccolta e trattamento, per altro verso, l'importanza fondamentale per lo svolgersi di molteplici attività e rapporti.
Il rilievo di questo bene giuridico e la fragilità a cui è esposto, rispetto ad offese dalle quali il titolare non può autonomamente difendersi in modo adeguato, rende necessario un efficace intervento pubblico di protezione che, in mancanza di sufficiente capacità preventiva di sanzioni soltanto civilistiche e amministrative, da valutare anche dal punto di vista degli strumenti di ricerca e raccolta delle prove, deve necessariamente includere anche misure penali.

La sicurezza informatica

Non meno importante è il nuovo bene giuridico della "sicurezza informatica", che non è soltanto strumentale alla protezione degli altri interessi e diritti della persona meritevoli di tutela nel *cyberspace* (a cominciare dalla riservatezza informatica e dalla *privacy*, appena menzionate), ma è, a sua volta, meritevole di un'autonoma ed efficace protezione giuridica, compresa quella penale, in quanto svolge una funzione di garanzia "preventiva" di tutti gli altri interessi e diritti che emergono e si esercitano nello spazio cibernetico. Data la sua notevole rilevanza, a certe condizioni, diviene addirittura indisponibile per gli stessi titolari dei sistemi informatici, allorché tale sistema sia collettivamente condiviso. A titolo esemplificativo, si pensi ai gestori di registri informatici in uso nelle PA: se si permettesse loro di poter operare liberamente si rischierebbe di sacrificare una serie di diritti appartenenti ad un'ampia sfera di soggetti (per esempio la violazione del citato diritto alla *privacy*). Infatti, la vulnerabilità della protezione di un qualsivoglia sistema, inestricabilmente connesso con gli altri, si riverbera necessariamente sulla sicurezza di tutti.

b. Principi generali dei modelli destinati prevenire la commissione dei reati informatici

Ai fini della prevenzione dei reati oggetto della presente Sezione, LumIT prevede l'espresso divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato enucleate;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Pertanto, è fatto obbligo ai destinatari di conoscere e rispettare:

- i principi di *Corporate Governance* approvati dal CdA che rispecchiano le normative applicabili e le pratiche internazionali in relazione alla prevenzione dei reati informatici;
- le procedure aziendali, la documentazione e le disposizioni inerenti alla struttura gerarchico-funzionale, aziendale ed organizzativa della Società ed il sistema di controllo di gestione;
- le norme inerenti al sistema amministrativo, contabile, finanziario, di *reporting*;
- le norme interne inerenti all'uso e il funzionamento del sistema informativo di LumIT;
- in generale, la normativa applicabile.

2.5.2. I modelli

I reati previsti dall'art. 25-bis D.Lgs. 231/2001

a. Accesso abusivo a sistema informatico e telematico (art. 615-ter c.p.)

Il reato può essere commesso da 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.
La pena è aumentata allorché il fatto sia 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; oppure se il colpevole per commettere il fatto usa

violenza sulle cose o alle persone, ovvero se è palesemente armato; o ancora, se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.
La pena è ulteriormente aumentata se i fatti sono commessi avverso 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.

b. Detenzione e diffusione abusiva di codici di accesso e sistemi informatici o telematici (art. 615-quater c.p.)

Incorre in questo illecito penale 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.
La pena è aumentata se ricorrono le circostanze aggravanti di cui all'art. 617-*quater* c.p.

c. Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)

Il reato è commesso da 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.

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

Questa fattispecie può essere commessa da chiunque fraudolentemente intercetti comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa. Sono altresì puniti coloro che rivelino, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni.
Il reato è aggravato allorché il fatto sia 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; oppure 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.

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

Viene punito chiunque distrugga, deteriori, cancelli, alteri o sopprima informazioni, dati o programmi informatici altrui; allorché il fatto sia commesso con violenza alla persona o minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

f. 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.)

L'art. 615-ter sanziona chiunque commetta 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; inoltre, se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è aumentata.
La pena è altresì aumentata allorquando il fatto sia commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema.

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

È punito chiunque, mediante le condotte di cui alla lettera E), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugga, danneggi, renda in tutto o in parte inservibili sistemi informatici o telematici altrui o ne ostacoli gravemente il funzionamento. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

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

È punito chi commette il fatto di cui alla lettera precedente al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

La pena è aumentata 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;
- il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema.

Per completezza, si segnala che con il D. L. 21 settembre 2019, n. 105, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 (Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica), è stata prevista una nuova ipotesi di responsabilità della persona giuridica. Tuttavia, in attesa di una compiuta definizione delle condotte di reato da parte del Ministro delle Infrastrutture, all'epoca dell'ultimo aggiornamento dei presenti MOGC tale ipotesi è di fatto non operativa.

2.6. Reati tributari

Tabella - I reati previsti dall'art. 25-quinquiesdecies D. Lgs. 231/2001

Reato	Sanzione per la persona giuridica	Misura interdittiva per la persona giuridica	Oggetto materiale della condotta
DICHIARAZIONE FRAUDOLENTA MEDIANTE FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI (ART. 2, COMMI 1 E 2-BIS, L. 74/2000)	Da 100 a 500 quote, Se, in seguito alla commissione dei delitti indicati, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di 1/3. Se l'ammontare degli elementi passivi fittizi è inferiore a € 100.000 la sanzione è da 100 a 400 quote.	Divieto di contrattare con la p.a.; esclusione dalle agevolazioni, concessioni e finanziamenti; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. c, d ed e, D. Lgs. 231 del 2001).	Indicare in una delle dichiarazioni relative ai redditi o all'imposta sul valore aggiunto elementi passivi fittizi, avvalendosi di fatture o altri documenti per operazioni inesistenti.
DICHIARAZIONE FRAUDOLENTA MEDIANTE ALTRI ARTIFICI (ART. 3, L. 74/2000)	Da 100 a 500 quote, Se, in seguito alla commissione dei delitti indicati, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di 1/3.	Divieto di contrattare con la p.a.; esclusione dalle agevolazioni, concessioni e finanziamenti; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. c, d ed e, D. Lgs. 231 del 2001).	Indicare in una delle dichiarazioni relative ai redditi o all'imposta sul valore aggiunto elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi diversi dalle fatture o di altri mezzi fraudolenti.
EMISSIONE DI FATTURE O ALTRI DOCUMENTI PER OPERAZIONI INESISTENTI	Da 100 a 500 quote, Se, in seguito alla commissione dei delitti indicati, l'ente ha conseguito un profitto di rilevante entità, la	Divieto di contrattare con la p.a.; esclusione dalle agevolazioni, concessioni e finanziamenti; divieto di pubblicizzare beni e servizi (art. 9, comma 2,	Emettere o rilasciare fatture o altri documenti per operazioni inesistenti, al fine di consentire a terzi l'evasione delle imposte

(ART. 8, COMMI 1 E 2-BIS, L. 74/2000)	sanzione pecuniaria è aumentata di 1/3. Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta è inferiore a € 100.000 la sanzione è da 100 a 400 quote.	lett. c, d ed e, D. Lgs. 231 del 2001).	sui redditi o sul valore aggiunto.
OCCULTAMENTO O DISTRUZIONE DI DOCUMENTI CONTABILI (ART. 10, L. 74/2000)	Da 100 a 400 quote	Divieto di contrattare con la p.a.; esclusione dalle agevolazioni, concessioni e finanziamenti; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. c, d ed e, D. Lgs. 231 del 2001).	Occultare o distruggere in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.
SOTTRAZIONE FRAUDOLENTA AL PAGAMENTO DI IMPOSTE (ART. 11, L. 74/2000)	Da 100 a 400 quote	Divieto di contrattare con la p.a.; esclusione dalle agevolazioni, concessioni e finanziamenti; divieto di pubblicizzare beni e servizi (art. 9, comma 2, lett. c, d ed e, D. Lgs. 231 del 2001).	Vendere simulatamente o compiere altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva delle imposte sui redditi o sul valore aggiunto. Indicare nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori.

2.6.1. Introduzione

a. Il "nuovo" art. 25-quinquiesdecies

Questa Sezione della Parte Speciale si riferisce ai comportamenti dei Destinatari coinvolti nei Processi Sensibili nel cui ambito possono essere commessi reati tributari.

Si precisa che il recente legislatore, nell'introdurre il nuovo art. 25-quinquiesdecies del Decreto, ha inteso limitare la responsabilità della persona giuridica solo alle ipotesi di reati tributari considerate più gravi tra quelle previste D. Lgs. 10 marzo 2000, n. 74 ("Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della legge 25 giugno 1999, n. 205").

b. Principi generali dei modelli destinati prevenire la commissione dei reati tributari

Ai fini della prevenzione dei reati oggetto della presente Sezione, LumIT prevede l'espresso divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato enucleate;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Pertanto, è fatto obbligo ai destinatari di conoscere e rispettare:

- i principi di *Corporate Governance* approvati dal CdA che rispecchiano le normative applicabili e le pratiche internazionali in relazione alla prevenzione dei reati tributari;
- le procedure aziendali, la documentazione e le disposizioni inerenti alla struttura gerarchico-funzionale, aziendale ed organizzativa della Società ed il sistema di controllo di gestione;
- le norme inerenti al sistema amministrativo, contabile, finanziario, di *reporting*;
- le norme interne inerenti all'uso e il funzionamento del sistema informativo di LumIT;

- in generale, la normativa applicabile.

2.6.2. I modelli

I reati previsti dall'art. 25-quinquiesdecies D.Lgs. 231/2001

a. Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, commi 1 e 2-bis)

È punito chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, avvalendosi di fatture o altri documenti per operazioni oggettivamente o anche solo soggettivamente inesistenti, indica in una delle dichiarazioni relative a dette imposte elementi passivi fittizi.
Il fatto si considera commesso avvalendosi di fatture o altri documenti per operazioni inesistenti quando tali fatture o documenti sono registrati nelle scritture contabili obbligatorie, o sono detenuti a fine di prova nei confronti dell'amministrazione finanziaria.
La pena è ridotta se l'ammontare degli elementi passivi fittizi è inferiore a euro centomila, così come è ridotta la sanzione per la persona giuridica.

b. Dichiarazione fraudolenta mediante altri artifici (art. 3)

Fuori dai casi previsti nel paragrafo precedente, è punito chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, compiendo operazioni simulate oggettivamente o soggettivamente ovvero avvalendosi di documenti falsi o di altri mezzi fraudolenti idonei ad ostacolare l'accertamento e ad indurre in errore l'amministrazione finanziaria, indica in una delle dichiarazioni relative a dette imposte elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi o crediti e ritenute fittizi. La condotta è punibile solo qualora siano congiuntamente superate le seguenti soglie di punibilità:

- l'imposta evasa è superiore, con riferimento a taluna delle singole imposte, a euro trentamila;
- l'ammontare complessivo degli elementi attivi sottratti all'imposizione, anche mediante indicazione di elementi passivi fittizi, è superiore al cinque per cento dell'ammontare

complessivo degli elementi attivi indicati in dichiarazione, o comunque, è superiore a euro un milione cinquecentomila, ovvero qualora l'ammontare complessivo dei crediti e delle ritenute fittizie in diminuzione dell'imposta, è superiore al cinque per cento dell'ammontare dell'imposta medesima o comunque a euro trentamila.

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

Non costituiscono mezzi fraudolenti la mera violazione degli obblighi di fatturazione e di annotazione degli elementi attivi nelle scritture contabili o la sola indicazione nelle fatture o nelle annotazioni di elementi attivi inferiori a quelli reali.

c. Emissione di fatture o altri documenti per operazioni inesistenti (art. 8, commi 1 e 2-bis)

È punito chiunque, al fine di consentire a terzi l'evasione delle imposte sui redditi o sul valore aggiunto, emette o rilascia fatture o altri documenti per operazioni inesistenti.

L'emissione o il rilascio di più fatture o documenti per operazioni inesistenti nel corso del medesimo periodo di imposta si considera come un solo reato.

Se l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo d'imposta, è inferiore a euro centomila, si applica una pena ridotta (e, correlativamente, una sanzione meno incisiva per la persona giuridica).

d. Occultamento o distruzione di documenti contabili (art. 10)

È punito chiunque, al fine di evadere le imposte sui redditi o sul valore aggiunto, ovvero di consentire l'evasione a terzi, occulta o distrugge in tutto o in parte le scritture contabili o i documenti di cui è obbligatoria la conservazione, in modo da non consentire la ricostruzione dei redditi o del volume di affari.

e. Sottrazione fraudolenta al pagamento di imposte (art. 11)

È punito chiunque, al fine di sottrarsi al pagamento di imposte sui redditi o sul valore aggiunto ovvero di interessi o sanzioni amministrative relativi a dette imposte di ammontare complessivo superiore ad euro cinquantamila, aliena simulatamente o compie altri atti fraudolenti sui propri o su altrui beni idonei a rendere in tutto o in parte inefficace la procedura di riscossione coattiva. Se l'ammontare delle imposte, sanzioni ed interessi è superiore ad euro duecentomila la pena è aumentata, rimanendo invece invariata la cornice edittale prevista per la sanzione applicabile alla persona giuridica.

È punito altresì chiunque, al fine di ottenere per sé o per altri un pagamento parziale dei tributi e relativi accessori, indica nella documentazione presentata ai fini della procedura di transazione fiscale elementi attivi per un ammontare inferiore a quello effettivo od elementi passivi fittizi per un ammontare complessivo superiore ad euro cinquantamila. Se l'ammontare di cui al periodo precedente è superiore ad euro duecentomila la pena è aumentata, rimanendo invece invariata la cornice edittale prevista per la sanzione applicabile alla persona giuridica.