MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ai sensi del D.Lgs. 231/2001di ICTLA PA SRL

Testo approvato dall'Amminsitratore Unico di ICTLAB PA s.r.l. in data 11/06/2021

INDICE

Allegati:

- **Allegato1**: Elenco reati;
- **Allegato 2**: Codice Etico;
- **Allegato 3**: Organigramma di ICTLAB PA SRL;
- **Allegato 4**: Regolamento dell'Organismo di Vigilanza di ICTLAB PA SRL.

STATO DELLE REVISIONI

NUMERO E DATA REVISIONE	OGGETTO REVISIONE
24/03/2017	Prima versione (Lattanzio ICT Lab s.r.l.)
REV. 1 – 11/06/2021	Primo aggiornamento (ICTLAB PA s.r.l.)

1. INTRODUZIONE DI ICTLAB PA SRL

Le referenze in tutta Italia rendono **ICTLAB PA** una realtà unica al servizio delle Pubbliche Amministrazioni e delle PMI.

ICTLAB PA vanta un sistema di competenze specialistiche distintivo che consente ai clienti di cogliere appieno le opportunità dell'adozione delle nuove tecnologie, massimizzando il valore aggiunto dei percorsi di innovazione.

In particolare, ICTLAB PA offre i seguenti servizi:

- strategie e piani di innovazione per la diffusione dell'ICT nelle PA e nelle imprese
- sistemi di e-government.
- e – procurement
- cloud computing
- sistemi open data
- progettazione, studi di fattibilità e impatto, Project management, monitoraggio e valutazione dei progetti ICT
- progettazione e sviluppo sistemi informativi e portali web
- gestione applicativi, help desk
- supporto nel processo di acquisto ICT (fabbisogni, capitolati tecnici, selezione fornitore)

2. PREMESSA

2.1. Contesto Normativo di Riferimento

Il **Decreto legislativo 8 giugno 2001, n. 231**, avente ad oggetto la *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"* (qui di seguito denominato il "**D.Lgs. 231/2001**" o semplicemente il "**Decreto**"), ha introdotto per la prima volta nel nostro ordinamento la responsabilità degli Enti, per illeciti amministrativi dipendenti da reato.

Si tratta di una particolare forma di responsabilità definita "amministrativa" che, in realtà, si sostanzia in una responsabilità penale a carico degli enti, in quanto accertata dinnanzi al giudice penale.

Il Decreto costituisce un intervento di grande portata normativa e culturale in cui, alla responsabilità penale della persona fisica che ha commesso il reato, si aggiunge quella dell'Ente a vantaggio o nell'interesse del quale lo stesso reato è stato perpetrato.

Le disposizioni contenute nel Decreto ai sensi dell'articolo 1, comma 2, si applicano ai seguenti "Soggetti":

- enti forniti di personalità giuridica;
- società e associazioni anche prive di personalità giuridica.

Ai sensi del successivo comma 3, restano inveceesclusi dalla disciplina in oggetto:

- lo Stato;
- gli enti pubblici territoriali;
- gli altri enti pubblici non economici;
- gli enti che svolgono funzioni di rilievo costituzionale.

La responsabilità viene, quindi, attribuita all'Ente qualora i reati, indicati dal Decreto e riportati nell'elenco allegato al presente Modello (*cfr*. **Allegato n. 1 "Elenco Reati"**), siano commessi nel suo interesse o vantaggio da:

- soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale e coloro che esercitano di fatto la gestione ed il controllo dell'Ente (c.d. "soggetti apicali");
- soggetti sottoposti alla direzione o alla vigilanza di soggetti apicali (c.d. "soggetti in posizione subordinata").

Nell'ipotesi di reati commessi da soggetti in posizione apicale, la responsabilità dell'Ente è espressamente esclusa qualora quest'ultimo dimostri che il reato è stato commesso eludendo fraudolentemente i modelli di organizzazione e di gestione idonei a prevenire i reati della specie di quello verificatosi e che non vi sia stato, inoltre, omesso o insufficiente controllo da parte dell'Organismo di Vigilanza (di seguito "**O.d.V.**"), appositamente incaricato di vigilare sul corretto funzionamento e sull'effettiva osservanza del modello stesso.

A tal proposito, i modelli di organizzazione e gestione devono rispondere alle seguenti esigenze:

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

b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente;

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

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

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

Al contrario, nel caso di reato realizzato da soggetti in posizione subordinata, l'Ente sarà responsabile ove la commissione del reato sia stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza.

Diversamente, la responsabilità è espressamente esclusa laddove l'Ente abbia adottato, in relazione alla natura e alla dimensione dell'organizzazione nonché al tipo di attività svolta, "*misure idonee a garantire lo svolgimento dell'attività stessa nel rispetto della legge*" ed a verificare e a scoprire ed eliminare tempestivamente situazioni di rischio; nonché, laddove i suddetti soggetti abbiano agito "*nell'interesse esclusivo proprio o di terzi*" (art. 5, co. 2, D.Lgs. 231/01).

La responsabilità dell'Ente non scaturisce dalla commissione da parte dei soggetti sopra individuati di qualsivoglia fattispecie criminosa, ma è circoscritta alle ipotesi di reato previste originariamente dal Decreto e dalle successive modifiche, indicate nell'elenco allegato al presente Modello (*cfr*. Allegato n. 1 "Elenco Reati").

Ogni eventuale imputazione all'Ente di responsabilità derivanti dalla commissione di una o più delle fattispecie di cui al Decreto non vale ad escludere quella personale di chi ha posto in essere la condotta criminosa.

L'art. 9 comma 1 del Decreto individua **le sanzioni** che possono essere inflitte all'Ente, ovvero:

- le sanzioni pecuniarie;
- le sanzioni interdittive;
- la confisca;
- la pubblicazione della sentenza.

Le sanzioni pecuniarie variano da un minimo di 25.822 € ad un massimo di 1.549.370 € e sono fissate dal giudice tenendo conto:

- della gravità del fatto;
- del grado di responsabilità dell'Ente;
- dell'attività svolta dall'Ente per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti;
- delle condizioni economiche e patrimoniali dell'Ente.

Le sanzioni interdittive, la cui durata non può essere inferiore a tre mesi né superiore a due anni, sono:

- l'interdizione dall'esercizio delle attività;
- la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
- l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;
- il divieto di pubblicizzare beni o servizi;
- il commissariamento.

Le sanzioni interdittive sono applicabili, anche in via cautelare, esclusivamente se ricorre almeno una delle seguenti condizioni:

a) l'Ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso da soggetti in posizione apicale, ovvero da soggetti sottoposti all'altrui direzione e vigilanza quando la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;

b) in caso di reiterazione degli illeciti.

Le suesposte sanzioni possono essere applicate all'Ente esclusivamente dal Giudice penale e solo se sussistono tutti i requisiti oggettivi e soggettivi fissati dal Legislatore: la commissione di un determinato reato, nell'interesse o a vantaggio della società, da parte di soggetti qualificati (apicali o ad essi sottoposti) e la valutazione di non idoneità del modello organizzativo applicato o la sua mancata esecuzione.

La responsabilità degli enti si estende anche ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto, sempre che sussistano le particolari condizioni previste dal D.Lgs. 231/2001.

Infatti, con la Legge 146/2006, si è introdotto anche nell'ambito della disciplina della responsabilità amministrativa degli Enti il concetto di reato transnazionale.

Ai sensi dell'art. 3 della suddetta Legge si considera reato transnazionale "il reato punito con la pena della reclusione non inferiore nel massimo a 4 anni, qualora sia coinvolto un gruppo criminale organizzato, nonché:

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

La responsabilità amministrativa deriva dalla commissione di determinati reati (previsti *ex Lege*) consumati da soggetti apicali o dipendenti-collaboratori nell'interesse o a vantaggio dell'Ente;

Il Legislatore, all'art. 5 del D.Lgs. 231/2001, individua tali soggetti come segue:

a) "*persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche, di fatto, la gestione e il controllo degli stessi*" (cosiddetti soggetti apicali);
b) "*persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)" (cosiddetti sottoposti).*

L'interesse e il vantaggio dell'Ente, che la Legge prevede quali requisiti alternativi per la configurazione della responsabilità in parola, corrispondono a concetti da intendersi sussistenti in modo obbiettivo, quindi anche laddove non siano stati previsti dal soggetto agente che ha commesso il reato di cui al D.Lgs. 231/2001. Pertanto, non rileva l'atteggiamento o l'intento del soggetto che commette il reato, ma rileva il fatto che quel reato abbia comunque consentito un vantaggio per l'Ente. Differente è il caso in cui la commissione di un reato di cui al D.Lgs. 231/2001 comporti un vantaggio esclusivo per l'agente (o di un terzo rispetto all'Ente): in tale ipotesi non si configura la responsabilità amministrativa dell'Ente, versandosi in una situazione di estraneità dell'Ente al fatto reato.

La responsabilità dell'Ente è distinta e autonoma rispetto a quella di colui che ha commesso il reato (a titolo esemplificativo: l'amministratore della TIZIO S.R.L., che ha corrotto un ispettore del lavoro in favore della società per evitare un controllo, risponderà personalmente del reato di corruzione e la società TIZIO S.R.L. risponderà autonomamente - anche con il suo capitale - dell'illecito amministrativo commesso derivante dalla commissione del reato e mediante le dovute sanzioni).

Pertanto, la responsabilità dell'Ente si aggiunge a quella della persona fisica che ha commesso materialmente l'illecito, ed è autonoma rispetto ad essa, sussistendo anche quando l'autore del reato non è stato identificato o non è imputabile oppure nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

Ai fini dell'affermazione della responsabilità dell'Ente, oltre all'esistenza dei richiamati requisiti che consentono di collegare oggettivamente il reato all'ente (e quindi il fatto che una persona fisica dipendente/collaboratore dell'Ente, in posizione apicale o anche subordinata, abbia commesso un reato nell'interesse e a vantaggio dell'Ente), il Legislatore impone l'accertamento della colpevolezza dell'ente. Tale condizione si identifica con una "*colpa di organizzazione*", intesa come violazione di adeguate regole di diligenza autoimposte dall'Ente medesimo e volte a prevenire lo specifico rischio da reato.

In buona sostanza, l'Ente sarà chiamato a rispondere nel processo penale della sua colpa di organizzazione per non aver adottato un modello organizzativo capace di evitare la commissione del reato da parte dei dipendenti/collaboratori.

Specifiche disposizioni sono state dettate dal Legislatore per i casi di trasformazione, fusione, scissione e cessione d'azienda per i quali si rimanda, per maggiori dettagli, a quanto specificamente previsto dagli artt. 28>33 del D.Lgs. 231/2001.

Il D.Lgs. 231/2001, come successivamente modificato ed integrato[1], ha quindi introdotto la nuova disciplina della responsabilità amministrativa dell'Ente collettivo per taluni reati commessi nel proprio interesse o a proprio vantaggio da soggetti (e loro sottoposti) che esercitino (di diritto o di fatto) funzioni di rappresentanza, amministrazione e direzione.

La responsabilità dell'ente non scaturisce dalla commissione da parte dei soggetti appena individuati di qualsivoglia fattispecie criminosa, ma è circoscritta alle ipotesi di reato, previste originariamente dal Decreto e dalle successive modifiche (intervenute, da ultimo, con la Legge 19dicembre 2019, n. 159), di seguito elencate:

a) i reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24[2] e 25[3] del D.Lgs. 231/2001);
b) i reati in tema di falsità in monete, carte di pubblico credito e valori di bollo e in strumenti o segni di riconoscimento (art. 25-*bis* del D.Lgs. 231/2001)[4];
c) i reati societari (quelli previsti dall'art. 25-*ter* del D.Lgs. 231/2001)[5];
d) i reati con finalità di terrorismo o di eversione dell'ordine democratico (art. 25-*quater* del D.Lgs. 231/2001)[6];
e) i reati contro la personalità individuale (art. 25-*quinquies* del D.Lgs. 231/2001)[7] e i reati consistenti in pratiche di mutilazione degli organi genitali femminili (art. 25-*quater* 1 del D.Lgs. 231/2001)[8];
f) i reati di abuso di informazioni privilegiate e manipolazione del mercato (art. 25-*sexies* del D.Lgs. 231/2001)[9];
g) i reati commessi in violazione delle norme sullatutela della salute e della sicurezza nei luoghi di lavoro (art. 25-*septies* del D.Lgs. 231/2001)[10];
h) i reati così detti transnazionali[11] di cui alla Convenzione e ai Protocolli aggiuntivi delle Nazioni Unite contro il crimine organizzato (art. 10 della L. 16 marzo 2006, n. 146);
i) i reati di ricettazione (art. 648 c.p.), riciclaggio (art. 648-*bis* c.p.), impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.) e autoriciclaggio (art. 648-ter 1) (art. 25-*octies* 231/2001)[12];
j) i reati informatici (art. 24-*bis* del D.Lgs. 231/2001)[13];
k) i reati contro l'industria e il commercio (art. 25-*bis*. 1 del D.Lgs. 231/2001)[14];
l) i reati in materia di violazione del diritto d'autore (art. 25-*novies* del D.Lgs. 231/2001)[15];

---

[1] Interventi di modifica del D.Lgs. 231/2001: D.L. 25.09.2001, n. 350, convertito con L. 23.11.2001 n. 409 (art. 9); D.Lgs. 11.04.2002, n. 61 (art. 3); Leggi 14.01.2003, n. 7 (art. 3), 11.08.2003, n. 228 (art. 5), 18.04.2005, n. 62 (art. 9), 28.12.2005, n. 262 (artt. 31 e 39), 09.01.2006, n. 7 (art. 8), 06.02.2006, n. 38 (art. 10), 03.08.2007, n. 123 (art. 9) e dal D.Lgs. 21.11.2007, n. 231 (art. 63, c. 3), L. 18.03.2008, n. 48 (art. 7), L. 23.07.2009, n. 99 (art. 15) e D.Lgs. 07.07.2011 n. 121 (art. 2)D.Lgs. 16.07.2012, n. 109 (art. 2), L. 06.11.2012, n. 190 (art. 77), D.Lgs. 04.03.2014 n. 39, L. 15.12.2014, n. 186, L. 27.05.2015 n. 69, L. 20 novembre 2017, n. 167, L. 09.01.2019, n. 3, L. 03.05.2019, n. 39, L. 18.11.2019 n. 133, L. 19.12.2019, n. 157, D.Lgs. 14.07.2020, n. 75.

[2] Articolo modificato dall'articolo 5, comma 1, lettera a), numero 1), del D.Lgs. 14 luglio 2020, n. 75.

[3] Articolo modificato dall'art. 1, comma 9, lett. b) della L. 09.01.2019, n. 3 e successivamente modificato dall'articolo 5, comma 1, lettera b), numero 1), del D.Lgs. 14 luglio 2020, n. 75.

[4] Articolo aggiunto dall'art. 6, D.L. 25.09.2001 n. 350.

[5] Articolo aggiunto dall'art. 3, D.L. 11.04.2002 n. 61 e modificato dalla L. 27.05.2015 n. 69.

[6] Articolo aggiunto dall'art. 3, L. 14.01.2003 n. 7.

[7] Articolo aggiunto dall'art. 5, L. 11.08.2003 n. 228 e integrato dall'art. 3, D.Lgs. 04.03.2014 n. 39 per la fattispecie relativa all'adescamento di minori (art. 609-undecies c.p.), nonché dall'articolo 6, comma 1, della Legge 29 ottobre 2016, n. 199 per la fattispecie relativa all'intermediazione illecita e sfruttamento del lavoro.

[8] Articolo aggiunto dall'art. 8, L. 14.01.2003 n. 7.

[9] Articolo aggiunto dall'art. 9, L. 18.04.2005 n. 62.

[10] Articolo aggiunto dall'art. 9 L. 03.08.2007, n. 123 e successivamente modificato dall'art. 300 del D.Lgs. 81/2008 (Testo Unico Sicurezza Lavoro).

[11] I reati transazionali prevedono le seguenti caratteristiche:

- per il reato è prevista una pena maggiore di quattro (n. 4) anni;
- il reato è commesso in uno stato ma una parte della condotta deve essere avvenuta in un diverso stato;
- il reato vede implicato un gruppo criminale organizzato;
- il reato è commesso in uno stato ma ha effetti sostanziali in un diverso stato.

[12] Articolo aggiunto dall'art. 63, co. 3 del D.Lgs. 21.11.2007, n. 231 e integrato dall'art. 3 della L. 15.12.2014, n. 186 per la fattispecie dell'autoriciclaggio.

[13] Articolo aggiunto dall'art. 7 L. 18.03.2008, n. 48.

[14] Articolo aggiunto dall'art. 15 L. 23.07.2009, n. 99.

m) il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, come previsto *ex* art. 377-bis Codice Penale (art. 25-*decies* del D.Lgs. 231/2001);

n) i reati ambientali (art. 25-*undecies* del D.Lgs. 231/2001)[16];

o) il reato di impiego di cittadini di paesi terzi con soggiorno irregolare (art. 25-*duedecies* del D.Lgs. 231/2001)[17];

p) il reato di corruzione tra privati (art. 25-ter, I C., lettera S-*bis*) del D.Lgs. 231/2001)[18]

q) i delitti di criminalità organizzata (art. 24-ter del D.Lgs. 231/2001)[19];

r) i delitti di propaganda, istigazione ed incitamento alla violenza per motivi razziali, etnici, nazionali o religiosi (art. 25-terdecies del D.Lgs. 231/2001[20]);

s) le frodi in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25-quaterdecies del D.Lgs. 231/2001[21]);

t) i reati tributari (art. 25-quinquiesdecies del D.Lgs. 231/2001[22]);

u) contrabbando (art. 25-sexiesdeciesdel D.Lgs. 231/2001[23]).

Con riferimento ai reati sopra indicati in via generica, essi, al fine della miglior chiarezza, sono stati dettagliatamente indicati ed esplicati nell'Allegato 1.

Inoltre, nella Parte Speciale del modello, tali reati risultano ulteriormente descritti, ove, per ogni reato, è definita la sua struttura e la valutazione dei possibili rischi di accadimento nell'ambito societario.

Si pone l'attenzione sul fatto che la responsabilità amministrativa dell'Ente, inizialmente prevista solo per reati dolosi, oggi si può configurare anche in caso di reati colposi (dove non vi è l'intenzionalità del soggetto agente – es. infortunio sul lavoro da cui derivano lesioni gravi alla persona) o anche per reati contravvenzionali (come nel caso di alcuni reati ambientali) ove non ha rilevanza la valutazione della presenza del dolo o della colpa, ma il soggetto agente ne risponderà comunque e a prescindere.

È quindi sempre più opportuno considerare la rilevanza del Modello ai fini della miglior gestione della Società.

2.2. Struttura del Modello

Il Modello di organizzazione, gestione e controllo predisposto ed adottato da ICTLAB PA, si compone di:

- Una **Parte Generale** che fornisce una panoramica sul sistema complessivo di principi, regole organizzative e strumenti di controllo adottati da ICTLAB PA per prevenire la commissione, nell'ambito della propria attività, dei reati rilevanti ai sensi del D.Lgs. 231/01 e per garantire la trasparenza, la legalità, la correttezza e la coerenza delle proprie azioni. Una sezione della Parte Generale è dedicata **all'Organismo di Vigilanza (O.d.V.)**, ove ne vengono descritti i compiti, le funzioni ed i poteri, ed un'ulteriore sezione riguarda il **sistema sanzionatorio** da applicare in caso di commissione degli illeciti.
- Una **Parte Speciale** che si riferisce ai reati potenzialmente realizzabili all'interno della ICTLAB PA, nell'ambito della quale sono state focalizzate, per ciascuna categoria di reato, le aree sensibili, i destinatari ed i principi generali di comportamento ed i corrispondenti processi che tutti i soggetti, operanti nell'ambito di ICTLAB PA ovvero in rapporti con essa, sono tenuti ad osservare al fine di evitare l'insorgenza della responsabilità amministrativa della Società ed a prevenire, o almeno ridurre in maniera significativa, la probabilità di commissione dei reati rilevanti ai sensi del Decreto.

---

[15] Articolo aggiunto dall'art. 15 L. 23.07.2009, n. 99.
[16] Articolo aggiunto dall'art. 2 D.Lgs. 07.07.2011, n. 121 e integrato dall'art. 1 della L. 22.05.2015, n. 68.
[17] Articolo aggiunto dall'art. 2 D.Lgs. 16.07.2012, n. 109.
[18] Articolo aggiunto dall'art. 77 della L. 06.11.2012, n. 190.
[19] Articolo aggiunto dall'art. 2, co. 29, della L. 15.07.2009 n. 94.
[20] Articolo aggiunto dall'articolo 5, comma 2, della Legge 20 novembre 2017, n. 167 (Legge europea 2017).
[21] Articolo inserito dall'articolo 5, comma 1, della Legge 3 maggio 2019, n. 39.
[22] Articolo inserito dall'articolo 39, comma 2, del D.L. 26 ottobre 2019, n. 124, convertito con modificazioni dalla Legge 19 dicembre 2019, n. 157 e successivamente modificato dall'articolo 5, comma 1, lettera c), numero 1), del D.Lgs. 14 luglio 2020, n. 75.
[23] Articolo aggiunto dall'articolo 5, comma 1, lettera d), del D.Lgs. 14 luglio 2020, n. 75.

In allegato al Modello sono riportati:

- l'Elenco dei reati presupposto della responsabilità amministrativa delle società e degli enti ex D.Lgs. 231/2001;
- il Codice Etico;
- l'Organigramma della Società;
- il Regolamento dell'Organismo di Vigilanza.

L'Organo di Amministrazione (ad oggi, Amministratore Unico) di ICTLAB PA si impegna – su indicazione dell'OdV - ad integrare il Modello in caso di successivi interventi normativi che dovessero modificare le tipologie di reato o assumere rilevanza ai fini dell'applicazione della disciplina sulla responsabilità amministrativa degli enti ovvero nel caso di rilevanti modifiche dell'assetto organizzativo di ICTLAB PA.

2.3. Finalità del Modello

L'adozione del Modello costituisce un valido strumento di sensibilizzazione nei confronti dei dipendenti della Società e di tutti gli altri soggetti alla stessa cointeressati (clienti, fornitori, partner, collaboratori a diverso titolo), affinché seguano, nell'espletamento delle proprie attività, comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei reati contemplati nel Decreto.

La Società ha deciso di adottare il presente modello di organizzazione, gestione e controllo (di seguito il "**Modello**") con lo scopo di:

a) promuovere e valorizzare in misura ancora maggiore una cultura etica al proprio interno, in un'ottica di correttezza e trasparenza nella gestione delle attività, responsabilizzando tutti coloro che operano in nome e per conto di ICTLAB PA, nelle aree di attività a rischio;

b) introdurre un meccanismo che consenta di istituire un processo permanente, seppur da aggiornare periodicamente, di analisi delle attività aziendali, volto ad individuare le aree nel cui ambito possano astrattamente configurarsi i reati indicati dal Decreto;

c) introdurre principi di controllo a cui il sistema organizzativo debba conformarsi, così da poter prevenire nel concreto il rischio di commissione dei reati indicati dal Decreto nelle specifiche attività emerse a seguito dell'attività di analisi delle aree sensibili.

2.4. Destinatari del Modello

Le regole contenute nel presente Modello si applicano a tutti coloro che svolgono, anche di fatto, funzioni di gestione, amministrazione, direzione o controllo nella Società, ai dipendenti, nonché ai consulenti, collaboratori, procuratori e, in generale, a tutti i terzi che agiscono per conto di ICTLAB PA nell'ambito delle attività emerse come "a rischio".

I soggetti ai quali il Modello si rivolge sono tenuti, pertanto, a rispettarne puntualmente tutte le disposizioni, anche in adempimento dei doveri di lealtà, correttezza e diligenza che scaturiscono dai rapporti giuridici instaurati con ICTLAB PA.

2.5. Approvazione, modifica ed integrazione del Modello

I modelli di organizzazione e di gestione costituiscono, ai sensi e per gli effetti dell'articolo 6 comma 1, lettera a), del Decreto, atti di emanazione del Vertice aziendale. Pertanto, l'approvazione del presente Modello e dei suoi elementi costitutivi costituisce prerogativa e responsabilità esclusiva dell'Organo di Amministrazione (ad oggi, Amministratore Unico) di ICTLAB PA. La formulazione di eventuali modifiche ed integrazioni del Modello è responsabilità in via esclusiva dello stesso Amministratore Unico, anche su segnalazione dell'Organismo di Vigilanza, per i seguenti elementi:

- modifica della configurazione o dei compiti dell'Organismo di Vigilanza;
- l'inserimento, la modifica o l'integrazione di principi del Codice Etico;
- modifiche o integrazioni al Sistema disciplinare;
- l'adeguamento ad eventuali modifiche dell'assetto della società tali da incidere sulla mappatura delle aree di rischio o sulla configurazione delle misure di prevenzione del rischio di commissione di illeciti di cui al d.lgs. n. 231/01;
- aggiornamento, integrazione o comunque modifica della mappatura delle attività sensibili;

- modifica delle procedure aziendali e relativi riferimenti di cui alla Parte Speciale del presente documento tali da incidere sulla mappatura di cui al punto che precede, o alle conseguenti misure di prevenzione del rischio di commissione di illeciti di cui al d.lgs. n. 231/01;
- l'aggiornamento delle misure di prevenzione del rischio di commissione di illeciti di cui al d.lgs. n. 231/01 derivante da evoluzione degli strumenti di protezione della società o della normativa di riferimento, così come le modifiche conseguenti ad eventuali evoluzioni della disciplina di cui al d.lgs. n. 231/01, o a quella ivi richiamata.

2.6. Attuazione del Modello

L'adozione del presente Modello costituisce il punto di partenza del processo di conduzione dinamica del Modello stesso.

Per la fase di attuazione del Modello, l'Amministratore Unico e i Dirigenti/Responsabili, supportati dall'Organismo di Vigilanza, sono responsabili, per i rispettivi ambiti di competenza, dell'implementazione dei vari elementi del Modello, ivi comprese le procedure operative.

In ogni caso, ICTLAB PA ribadisce che la corretta attuazione ed il controllo sul rispetto delle disposizioni aziendali e, quindi, delle regole contenute nel presente Modello, costituiscono un obbligo ed un dovere di tutto il personale della Società e, in particolare, di ciascun Responsabile di funzione cui è demandata, nell'ambito della propria competenza, la responsabilità primaria sul controllo delle attività, specialmente di quelle a rischio.

3. PARTE GENERALE

3.1. Sistema organizzativo della Società

Il Sistema organizzativo di ICTLAB PA è stato impostato in modo da essere sufficientemente formalizzato e chiaro, soprattutto per quanto attiene all'attribuzione di responsabilità, alle linee di dipendenza gerarchica e alla descrizione dei compiti, con specifica previsione di principi di controllo quali, ad esempio, la contrapposizione di funzioni.

L'adeguatezza di tale sistema organizzativo è stata verificata sulla base dei seguenti criteri:

- formalizzazione del sistema;
- chiara definizione delle responsabilità attribuite e delle linee di dipendenza gerarchica;
- esistenza della contrapposizione di funzioni;
- corrispondenza tra le attività effettivamente svolte e quanto previsto dalle missioni e responsabilità della società.

La struttura organizzativa di ICTLAB PA è formalizzata e rappresentata graficamente in un *organigramma* (cfr. **Allegato n. 3 "Organigramma della Società"**), il quale definisce con chiarezza le linee di dipendenza gerarchica ed i legami funzionali tra le diverse posizioni di cui si compone la struttura stessa.

Si precisa che, per la gestione delle attività caratteristiche, ICTLAB PA può avvalersi anche di aziende partner attraverso appositi contratti di servizio. In particolare le seguenti funzioni sono:

- Gare e contratti: Lattanzio KIBS
- Assistenza tecnica e informatica: IAD s.r.l.
- Amministrazione, bache e fornitori: Company's Advisors s.r.l.

L'Organigramma e tutti i documenti ad esso connessi sono oggetto di costante e puntuale aggiornamento all'esito degli eventuali cambiamenti nella struttura organizzativa.

L'esatta individuazione dei compiti di ciascun soggetto e la loro assegnazione in modo chiaro e trasparente consente il rispetto del principio di separazione dei ruoli, necessario al fine di arginare il rischio della commissione di reati passibili di sanzione *ex* D. Lgs. 231/2001.

3.2. Sistema dei Controlli Interni

Il sistema dei controlli interni è costituito da un sistema procedurale, di governance e da norme più strettamente operative che regolamentano i processi aziendali, le attività ed i relativi controlli con l'obiettivo di:

- assicurare il rispetto delle strategie aziendali;
- assicurare l'efficacia ed efficienza dei processi;
- assicurare l'affidabilità e l'integrità delle informazioni contabili e gestionali;
- assicurare la conformità delle operazioni con la legge, i piani, i regolamenti e le procedure aziendali interne;
- assicurare il livello di conformità alle norme UNI EN ISO 9001;
- porre a disposizione della direzione un'informazione puntuale, organica, strutturata e quantitativa, che consenta di verificare e confrontare nel tempo l'evoluzione del livello qualitativo raggiunto.

Il sistema dei controlli interni è periodicamente soggetto a monitoraggio ed adeguamento in relazione all'evoluzione dell'operatività aziendale e al contesto normativo di riferimento.

Il sistema adottato da ICTLAB PA si compone dei seguenti principali elementi:

- l'organizzazione aziendale formalizzatache definisce struttura, ruoli, responsabilità, poteri autorizzativi e dipendenze gerarchiche;
- l'insieme delle procedure riferite ai diversi processi aziendali;
- gli ordini di servizio ed i regolamenti interni che disciplinano lo svolgimento delle attività interne ed assicurano la tracciabilità e documentabilità delle operazioni e dei controlli effettuati, nel rispetto del principio di separazione delle funzioni e di garanzia che ogni transazione o azione sia verificabile, documentata, coerente e congrua;
- un sistema di gestione delle risorse finanziarie e dei pagamenti;

- un sistema di formazione ed informazione, volto alla sensibilizzazione e diffusione a tutti i livelli aziendali dei principi etici e delle regole comportamentali, delle procedure emanate e dei contenuti del Modello di organizzazione, gestione e controllo;
- il Codice Etico, che racchiude i principi etici che devono essere osservati al fine di prevenire o ridurre i rischi di commissione di reato previsti dalla legge;
- un sistema disciplinare che interviene in caso di inosservanza delle disposizioni del Codice Etico, delle procedure operative e del Modello di organizzazione, gestione e controllo.

La funzione aziendale responsabile dell'audit presidia l'adeguatezza e l'affidabilità del Sistema dei Controlli Interni dell'azienda e supporta l'OdV.

3.3. Processo di analisi dei Rischi

Al fine di fornire la società del presidio costituito da un efficiente ed efficace Modello di organizzazione, gestione e controllo, sono state effettuate una serie di attività di analisi, a loro volta suddivise in differenti fasi dirette alla costruzione di un sistema di prevenzione e gestione dei rischi conforme con le disposizioni del Decreto Legislativo n. 231/2001.

Di seguito si descrive l'approccio metodologico utilizzato per individuare le aree a rischio e rilevare l'attuale sistema dei presidi e dei controlli finalizzato alla prevenzione dei reati.

Il processo di analisi si è articolato secondo i seguenti passaggi operativi:

1. mappatura dei processi sensibili
2. definizione e analisi dei rischi potenziali per singolo processo
3. analisi, valutazione e adeguamento del sistema di controllo preventivo (c.d. protocolli)

3.3.1 Mappatura dei processi sensibili

In tale fase del processo è stata effettuata un'analisi della realtà aziendale al fine di censire le aree interessate alle potenziali casistiche di reato ed individuare i soggetti interessati all'attività di controllo e monitoraggio.

In particolare, il lavoro di identificazione dei processi sensibili è iniziato con l'esame della documentazione aziendale disponibile (organigramma, procedure, comunicazioni interne e disposizioni di servizio, sistema di deleghe e procure, bilancio annuale), al fine di comprendere il contesto di riferimento in cui ICTLAB PA opera.

Dalla combinazione delle informazioni rilevate e dall'analisi critica della documentazione acquisita, è stata elaborata la mappatura dei processi ed una prima identificazione delle aree sensibili a rischio di commissione di reati, meglio identificate nella Parte Speciale del presente Modello.

3.3.2 Definizione e analisi dei rischi potenziali per singolo processo

Con riferimento alle aree sensibili individuate in precedenza, al contesto operativo interno di ICTLAB PA, sono state identificate le possibili modalità attuative dei reati.

Tale attività ha permesso di individuare i principali rischi aziendali che sono stati riepilogati nella **Parte Speciale** del presente documento, ove sono ripartite, per ciascuna fattispecie di reato, le aree sensibili e gli accorgimenti da adottare per evitare la commissione dei singoli reati.

3.3.3 Analisi, valutazione e adeguamento del sistema di controllo preventivo

Sulla base dei principali rischi aziendali rilevati, al fine di individuare tutte le misure preventive idonee a limitare il verificarsi degli stessi, in relazione alla singola area/attività "sensibile", sono state analizzate le procedure ed i controlli in essere al fine di valutare l'adeguatezza dei processi esistenti, ossia la loro attitudine a prevenire comportamenti illeciti (o comunque a ridurne il rischio ad un livello accettabile) e ad evidenziarne l'eventuale commissione.

In particolare, per ciascuna categoria di reato, potenzialmente realizzabile all'interno della ICTLAB PA, sono stati definiti i seguenti elementi:

1. le aree sensibili;
2. i destinatari;
3. i principi generali di comportamento e processi aziendali.

Lo scopo di tale valutazione è stato quello di ridurre ad un livello accettabile il rischio di commissione di reato identificato.

Come anzi detto, nella Parte Speciale del presente documento, sono ripartite per ciascuna area sensibile, le fattispecie di reato che presentano un più sensibile rischio di commissione in relazione alle specificità operative rispettivamente emergenti, e gli accorgimenti conseguenti da adottare per evitare la commissione degli stessi.

3.4. Codice Etico

L'adozione di principi etici rilevanti ai fini della prevenzione dei reati di cui al D. Lgs 231/2001 rappresenta un obiettivo del presente Modello. In tale ottica, l'adozione di un Codice Etico quale utile strumento di *governance* costituisce un elemento essenziale del sistema di controllo preventivo. Il Codice Etico, infatti, mira a raccomandare, promuovere o vietare determinati comportamenti a cui possono essere collegate sanzioni proporzionate alla gravità delle eventuali infrazioni commesse.

Il Codice Etico adottato dalla Società ai sensi del D. Lgs. 231/2001 è allegato al presente Modello e ne costituisce parte integrante (cfr. **Allegato n. 2 "Codice Etico"**).

Il Codice Etico di ICTLAB PA è rivolto all'Amministratore Unico, ai Dirigenti/Responsabili ed ai dipendenti, ma si estende anche a consulenti, collaboratori, procuratori e terzi che agiscono per conto della Società. L'efficacia applicativa del Codice è, pertanto, direttamente applicabile anche a quei soggetti nei cui confronti il rispetto dei principi etici può essere contrattualmente pattuito. È responsabilità dell'Organismo di Vigilanza individuare e valutare, con il supporto dei consulenti esterni, l'opportunità dell'inserimento di specifiche clausole contrattuali nei contratti che regolamentano il rapporto con detti soggetti alla luce delle attività aziendali potenzialmente esposte alla commissione dei reati di cui al citato Decreto.

Eventuali dubbi sull'applicazione dei principi e delle regole contenute nel Codice Etico, devono essere tempestivamente discussi con l'Organismo di Vigilanza.

Chiunque venga a conoscenza di violazioni ai principi del Codice o di altri eventi suscettibili di alterarne la portata e l'efficacia, è tenuto a darne pronta segnalazione all'Organismo di Vigilanza.

L'inosservanza dei principi e delle regole di condotta contenute nel Codice comporta l'applicazione delle misure sanzionatorie contemplate nel Sistema Disciplinare aziendale previsto dal Modello.

3.5. Formazione e Comunicazione

3.5.1. Formazione

La formazione interna costituisce uno strumento imprescindibile per un'efficace implementazione del Modello e per una diffusione capillare dei principi di comportamento e di controllo adottati dalla Società, al fine di una ragionevole prevenzione dei reati, da cui il Decreto fa scaturire la responsabilità amministrativa.

Tale attività formativa ha luogo successivamente all'adozione del Modello da parte dell'Amministratore Unico della Società, attraverso l'esposizione dei criteri fondamentali della responsabilità amministrativa dell'Ente, i reati presi in considerazione dal decreto, nonché la tipologia di sanzioni previste e le metodologie d'analisi adottate. L'Organismo di Vigilanza verifica che la formazione del personale, in merito all'applicazione del Modello di Organizzazione, Gestione e Controllo, sia adeguata e coerente con le disposizioni normative, nonché con le previsioni del Modello stesso. I programmi formativi vengono condivisi con l'Organismo di Vigilanza.

I requisiti del programma di formazione sono i seguenti:

- adeguatezza rispetto alla posizione ricoperta dai soggetti all'interno dell'organizzazione (neo-assunto, impiegato, quadro, dirigente, ecc.);
- differenziazione dei contenuti in funzione dell'attività svolta dal soggetto all'interno dell'azienda (attività a rischio, attività di controllo, attività non a rischio, ecc.);
- periodicità definita in funzione (i) del grado di cambiamento cui è soggetto l'ambiente esterno in cui si colloca l'agire aziendale, (ii) della capacità di apprendimento del personale e (iii) del grado di committment del management a conferire autorevolezza all'attività formativa svolta;
- selezione di relatori competenti e autorevoli, al fine di assicurare la qualità dei contenuti trattati, nonché di evidenziare l'importanza che la formazione in oggetto riveste per la Società e per le strategie che la stessa vuole perseguire;
- obbligatorietà della partecipazione (con appositi meccanismi di controllo per monitorare la presenza dei soggetti);
- controllo e verifica del grado di apprendimento dei partecipanti.

La formazione può essere classificata in *generale* o *specifica*. In particolare, la **formazione generale**, attuata secondo le modalità ritenute più idonee ed efficaci, interessa tutti i livelli dell'organizzazione, al fine di consentire ad ogni individuo di venire a conoscenza:

- dei precetti contenuti nel D. Lgs. 231/2001 in tema di responsabilità amministrativa degli Enti, dei reati e delle sanzioni ivi previste;
- dei principi di comportamento previsti dal Codice Etico;
- del Sistema disciplinare;
- delle linee guida e dei principi di controllo contenuti nelle procedure operative interne e degli standard di comportamento;
- dei poteri e compiti dell'Organismo di Vigilanza;
- del sistema di reporting interno riguardante l'Organismo di Vigilanza.

La **formazione specifica** interessa, invece, tutti quei soggetti che per via della loro attività, o comunque della loro posizione in azienda, necessitino di specifiche competenze al fine di gestire le peculiarità dell'attività stessa (i.e. il personale che opera nell'ambito di attività segnalate come potenzialmente a rischio di commissione di taluni illeciti ai sensi del Decreto). Questi sono destinatari di una formazione sia generale sia specifica. La formazione specifica è strutturata in modo tale da consentire al soggetto di:

- avere consapevolezza dei potenziali rischi associabili alla propria attività, nonché degli specifici meccanismi di controllo da attivare al fine di monitorare l'attività stessa;
- acquisire la capacità d'individuare eventuali anomalie e segnalarle nei modi e nei tempi utili per l'implementazione di possibili azioni correttive.

Anche i soggetti preposti al controllo interno cui spetta il monitoraggio delle attività risultate potenzialmente a rischio sono destinatari di una formazione specifica, al fine di renderli consapevoli delle loro responsabilità e del loro ruolo all'interno del sistema del controllo interno, nonché delle sanzioni cui vanno incontro nel caso disattendano tali responsabilità e tale ruolo.

In caso di modifiche e/o aggiornamenti rilevanti del Modello sono organizzati dei moduli d'approfondimento mirati alla conoscenza delle variazioni intervenute.

3.5.2 Comunicazione

In linea con quanto disposto dal D.Lgs. 231/2001, la Società dà piena pubblicità al presente Modello, al fine di assicurare che tutto il personale sia a conoscenza di tutti i suoi elementi.

La comunicazione è sempre capillare, efficace, chiara e dettagliata, con aggiornamenti periodici connessi ai mutamenti del Modello.

In particolare, la comunicazione:

- è sufficientemente dettagliata in rapporto al livello gerarchico di destinazione;
- utilizza i canali di trasmissione più appropriati e facilmente accessibili ai destinatari della comunicazione al fine di fornire le informazioni in tempi utili e permettendo al personale destinatario di usufruire della comunicazione stessa in modo efficace ed efficiente;
- è di qualità in termini di contenuti (comprende tutte le informazioni necessarie), tempestiva, aggiornata (deve contenere l'informazione più recente) e accessibile.

Il piano effettivo di comunicazione relativo alle componenti essenziali del presente Modello viene sviluppato, in coerenza ai principi sopra definiti, con comunicazione a tutto il personale tramite i mezzi di comunicazione aziendali ritenuti più idonei, quali, ad esempio, l'utilizzo di e-mail, pubblicazione sul sitointranet aziendale (cruscotto), ed invio personalizzato di apposita comunicazione a quadri e dirigenti.

3.6. Organismo di Vigilanza

Ai sensi dell'art. 6 del D.Lgs. 231/2001, una delle condizioni necessarie affinché la Società non risponda dei reati commessi dal proprio personale o dai propri incaricati è l'aver affidato il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello ad un apposito Organismo, dotato di autonomi poteri di iniziativa e di controllo.

3.6.1 Composizione, funzione e poteri

Sulla base del D. Lgs. 231/2001, l'Organo a cui affidare il compito di vigilare sul Modello, deve avere i seguenti requisiti:

- **Autonomia ed indipendenza**: l'OdV deve garantire l'autonomia dell'iniziativa di controllo da ogni forma di interferenza o condizionamento da parte di qualunque componente della società. Tali requisiti possono considerarsi soddisfatti prevedendo un'attività di reporting al massimo vertice aziendale, ovvero all'Amministratore Unico. Al fine di garantire tali requisiti, inoltre, ad esso non devono essere attribuiti compiti operativi che ne minerebbero l'obiettività di giudizio nell'esercizio delle sue funzioni. Al fine di svolgere in assoluta indipendenza le proprie funzioni, l'OdV dispone di autonomi poteri di spesa sulla base di un preventivo annuale, approvato dall'Amministratore Unico su proposta dell'Organismo stesso; in tal modo quest'ultimo potrà disporre di una dotazione adeguata di risorse finanziarie per ogni esigenza necessaria al corretto svolgimento dei compiti ed a coprire il compenso dei componenti dell'Organismo. A salvaguardia del principio di autonomia ed indipendenza è esclusa la possibilità di far parte dell'Organismo di Vigilanza a coloro i quali si trovano in situazioni di:
  - conflitto di interesse, anche potenziale, con la Società tali da pregiudicare l'indipendenza richiesta dal ruolo e dai compiti che si andrebbero a svolgere;
  - di relazioni di parentela, di coniugio o affinità entro il IV grado con componenti dell'Organo Amministrativo, soggetti apicali in genere, sindaci della società e revisori incaricati dalla Società di revisione con componenti degli organi sociali e con il vertice.
- **Onorabilità:** adeguati requisiti di "onorabilità" devono essere posseduti sin dal momento della nomina a componente dell'OdV; in base a tale principio non possono essere eletti a componenti dell'OdV coloro i quali:
  - si trovano nelle condizioni previste dall'art. 2382 c.c. (interdizione, inabilitazione, fallimento, condanna alla pena accessoria dell'interdizione, anche temporanea, dai pubblici uffici o dell'incapacità ad esercitare uffici direttivi)
  - siano stati condannati con sentenza irrevocabile o con sentenza non definitiva anche se a pena condizionalmente sospesa, fatti salvi gli effetti della riabilitazione, per uno dei reati tra quelli cui è applicabile il D. Lgs. n. 231/2001 o reati la cui pena edittale massima sia superiore a 5 anni. Per sentenza di condanna si intende anche la sentenza resa ex art. 444 c.p.p.;
  - abbiano rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, anche con provvedimento non definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;
  - abbiano subito l'applicazione delle sanzioni amministrative accessorie previste dall'art. 187 quater del D. Lgs. n. 58/1998.
- **Professionalità:** per svolgere efficacemente le funzioni affidategli, l'OdV deve possedere, un bagaglio di conoscenze, strumenti e tecniche specialistiche proprie di chi svolge attività ispettiva e consulenziale di analisi dei sistemi di controllo (organizzazione aziendale, finanza, analisi di procedure, ecc.) e di tipo giuridico. Tali tecniche possono essere utilizzate:
  - in via preventiva, per indicare eventuali ed opportune modifiche del Modello, al fine di adottare le misure più idonee a prevenire la commissione di reato;
  - in via continuativa, per verificare il rispetto dei comportamenti codificati con l'effettiva operatività;

Relativamente alle competenze giuridiche, ed in particolare alla disciplina penale, al fine di poter svolgere l'attività di prevenzione per la realizzazione dei reati, l'OdV deve conoscere la struttura e le modalità realizzative dei reati sia tramite l'utilizzo di risorse aziendali interne e/o di consulenza esterna.

- **Continuità d'azione:** al fine di garantire un'efficace e costante attuazione del modello, è necessaria la presenza di una struttura dedicata all'attività di vigilanza sul Modello, priva di mansioni operative che possa portarla ad assumere decisioni che abbiano effetti economico-finanziari; tale struttura può comunque fornire pareri consultivi sulla costruzione del modello, in fase di redazione dello stesso.

Il conferimento dell'incarico all'OdV e la revoca del medesimo sono atti di competenza dell'Amministratore Unico. La revoca di tale incarico sarà ammessa, oltre che per giusta causa (intendendosi a tal riguardo l'interdizione o l'inabilitazione, ovvero una grave infermità che renda il componente dell'Organismo di Vigilanza inidoneo a svolgere le proprie funzioni di vigilanza, o un'infermità che, comunque, comporti la sua assenza dal luogo di lavoro per un periodo superiore a sei mesi e non ovviabile attraverso alter modalità telematiche) anche nei casi in cui vengano meno i requisiti di indipendenza, onorabilità, assenza di conflitti di interessi e di relazioni di parentela con gli Organi Sociali ovvero in caso di un grave inadempimento dei doveri propri dell'Organismo di Vigilanza.

Nello specifico, i compiti assegnati all'OdV sono:

- verificare costantemente l'efficienza, l'efficacia e l'adeguatezza del Modello organizzativo adottato nel prevenire e contrastare la commissione degli illeciti, anche futuri ai quali è applicabile il D.Lgs. 231/2001, formulando eventuali proposte di aggiornamento a seguito di significative violazioni delle prescrizioni del Modello, di rilevanti mutamenti organizzativi o novità normative;
- monitorare l'applicazione ed il rispetto del Codice Etico;
- assicurare il costante aggiornamento della mappatura delle aree ritenute sensibili ai fini del D.Lgs. 231/2001;
- elaborare un programma di ispezioni teso a verificare l'osservanza da parte dell'Organizzazione, delle modalità operative e delle procedure previste dal Modello, al fine di vigilare sull'effettività del modello, rilevando la coerenza e gli eventuali scostamenti dei comportamenti attuati, tramite l'analisi dei flussi informativi e le segnalazioni alle quali sono tenuti i responsabili delle varie funzioni aziendali;
- predisporre un efficace sistema di comunicazione interna per consentire la trasmissione all'OdV di notizie rilevanti ai fini del D.Lgs. 231/2001, garantendo la tutela e la riservatezza del segnalante;
- mantenere un collegamento costante con la società di revisione, salvaguardandone la necessaria indipendenza e con gli altri consulenti coinvolti nelle attività di attuazione del Modello;
- segnalare all'Amministratore Unico le violazioni accertate che possono comportare una responsabilità della società al fine di porre in essere gli opportuni provvedimenti;
- verificare e valutare l'idoneità del sistema disciplinare ai sensi e per gli effetti del D.lgs. 231/2001;
- assicurare costantemente i previsti flussi informativi verso gli Organi Sociali relativamente alle attività di verifica e controllo svolte;
- promuovere e monitorare iniziative per favorire la conoscenza del Modello, la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello;
- formulare e sottoporre all'Amministratore Unico la previsione di spesa per la propria attività;
- fornire chiarimenti in merito all'applicazione delle previsioni del presente Modello.

È da precisare che le attività poste in essere dall'OdV non possono essere sindacate da altro organo interno. L'OdV, nello svolgimento dei suoi compiti, ha libero accesso a tutta la documentazione presso tutte le funzioni aziendali al fine di ottenere tutte le informazioni e dati utili e può avvalersi dell'ausilio di strutture interne della società o di consulenti esterni.

3.6.2 Controlli periodici

Oltre all'attività di vigilanza continua sull'effettiva applicazione del Modello e sulla sua adeguatezza, periodicamente l'OdV svolge specifiche verifiche sulla reale capacità del Modello di prevenire i reati, eventualmente avvalendosi anche di soggetti terzi aventi adeguate caratteristiche di professionalità ed indipendenza.

Periodicamente, soprattutto nell'ambito delle aree di attività sensibili, l'OdV effettua verifiche, anche mediante tecniche campionarie, mirate su determinate operazioni o specifici atti posti in essere da ICTLAB PA, i cui risultati devono essere riepilogati in un apposito report da trasmettere agli Organi Sociali deputati.Inoltre effettua ricognizioni sulle attività aziendali ai fini dell'aggiornamento della mappatura delle attività a rischio.

In particolare, relativamente alla verifica dell'osservanza del Modello, l'OdV verifica:

- l'esistenza di idonee iniziative per la diffusione della conoscenza e della comprensione dei principi del Modello;
- l'effettiva operatività posta in essere nelle aree delle attività "sensibili";
- le presunte violazioni delle prescrizioni del Modello e del Codice Etico.

L'OdV elabora annualmente il programma di vigilanza, in coerenza con i principi e i contenuti del Modello, e ne coordina l'effettiva attuazione verificando periodicamente la risoluzione delle situazioni di non conformità rilevate. Qualora lo ritenga necessario, l'OdV potrà inoltre svolgere interventi non programmati in aree specifiche.

Per le verifiche, l'OdV si avvale del supporto di altre funzioni interne che, di volta in volta, si rendano a tal fine necessarie. Al termine di tali verifiche viene elaborato un report che ne riepiloga gli esiti ed i miglioramenti da attuare in caso di emersione di criticità.

3.6.3 Attività di Reporting

In riferimento all'attività di reporting, l'OdV riferisce all'Amministratore Unico in merito all'attuazione del Modello e all'emersione di eventuali criticità attraverso due tipologie di reporting:

- la prima, semestrale, all'Amministratore Unico in cui vengono rendicontate le attività di verifica svolte e l'esito delle stesse;
- la seconda, annuale, tramite la quale viene illustrata all'Amministratore Unico l'attività svolta nell'anno in corso, unitamente al piano delle attività per l'anno successivo.

In caso di situazioni straordinarie (quali ad esempio modifiche legislative in materia di responsabilità amministrative degli enti, significative modifiche organizzative, ricezione di segnalazioni che rivestono carattere di urgenza), l'OdV informerà immediatamente l'Amministratore Unico.

Qualora l'OdV rilevi una violazione del Modello riferibile all'Amministratore Unico, effettua una segnalazione da destinarsi prontamente ai soci (o al collegio sindacale qualora rpesente), o procede alla convocazione di una assemblea.

Gli interventi dell'OdV devono essere verbalizzati e le copie dei verbali devono essere conservati.

L'OdV si riunisce almeno ogni trimestre e delle riunioni viene redatto apposito verbale.

L'OdV ha la facoltà di richiedere di confrontarsi con qualunque esponente aziendale, dirigente, dipendente, per acquisire informazioni o chiedere chiarimenti ecc e, per motivi urgenti, la convocazione dell'Amministratore Unico; questi, in qualsiasi momento,ha la medesima facoltà di convocare l'OdV.

3.6.4 Obblighi di informazione

L'OdV deve essere informato, mediante apposite segnalazioni effettuate dagli Organi Sociali, dai dipendenti,,dai consulenti, collaboratori, dai partner, dai fornitori e da tutti coloro che hanno contatti/relazione/interdipendenze con ICTLAB PA in merito ad eventi che potrebbero ingenerare responsabilità di ICTLAB PA ai sensi del D.Lgs. 231/01.

In particolare, devono essere segnalate senza ritardo:

- le notizie relative alla commissione o alla ragionevole convinzione di commissione degli illeciti da parte di dipendenti ICTLAB PA, distaccati, collaboratori, consulenti, partner e fornitori per reati previsti nel D.Lgs. n. 231/2001;
- le violazioni delle regole di comportamento o procedurali contenute nel presente Modello e nel Codice Etico da parte di dipendenti ICTLAB PA, distaccati, consulenti, partner e fornitori.

Il dipendente, il distaccato o il collaboratore che intende segnalare una violazione (o presunta violazione) del Modello la comunica all'OdV, informandone il proprio superiore diretto responsabile se lo ritiene opportuno..

L'indirizzo cui inoltrare le segnalazioni è il seguente:

Organismo di Vigilanza

Salita del Grillo, 10

00184 Roma

riportando sulla busta la dicitura RISERVATA

Ovvero inviare una mail all'indirizzo di posta elettronica appositamente costituito dalla gestione aziendale (*odv@ictlabpa.it*).

Gli obblighi di segnalazione da parte dei Collaboratori, dei Consulenti,dei Clienti, dei Fornitori e dei Partner devono essere specificati in apposite clausole inserite nei contratti che legano tali soggetti a ICTLAB PA.

L'Organismo di Vigilanza provvederà preliminarmente a porre in essere tutte le valutazioni e i controlli ritenuti necessari e, ove la segnalazione sarà ritenuta fondata, provvederà a mettersi in contatto con le Autorità competenti.

ICTLAB PA garantisce i segnalanti da qualsiasi forma di ritorsione, discriminazione o penalizzazione ed assicura in ogni caso la massima riservatezza circa la loro identità, fatti salvi gli obblighi di legge e la tutela dei diritti della ICTLAB PA.

Oltre alle segnalazioni relative a violazioni di carattere specifico, i responsabili di funzione devono tempestivamente trasmettere all'OdV le informazioni concernenti:

- le richieste di assistenza legale inoltrate dai Dipendenti in caso di avvio di procedimento giudiziario per i Reati di cui al D.Lgs. n. 231/2001;
- i rapporti preparati dai responsabili di altre funzioni aziendali nell'esercizio delle proprie funzioni e dai quali potrebbero emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del Decreto;
- le notizie relative ai procedimenti sanzionatori svolti e alle eventuali misure irrogate (ivi compresi i provvedimenti verso i dipendenti/distaccati) ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora essi siano legati a commissione di Reati o violazione delle regole di comportamento o procedurali del Modello;
- prospetti riepilogativi relativi a commesse attribuite da Enti pubblici
- informazioni in merito a decisioni relative alla richiesta, erogazione o utilizzo di contributi pubblici

In tale contesto, l'OdV definisce le responsabilità, le modalità, i contenuti e la frequenza degli ulteriori flussi informativi che devono pervenire allo stesso.

Con la periodicità stabilità dall'OdV i responsabili delle funzioni aziendali coinvolte nei processi "sensibili" ai sensi del D.Lgs. 231/2001, mediante un processo di autodiagnosi sull'attività svolta, attestano con dichiarazione scritta, il livello di attuazione del Modello con particolare attenzione al rispetto dei principi di controllo e comportamento e delle norme operative, segnalando le eventuali criticità ed i comportamenti significativamente difformi da quelli descritti nel processo e le motivazioni che hanno reso necessario od opportuno tale scostamento dalle indicazioni dettate dal Modello o più ingenerale dall'impianto normativo, nonché l'adeguatezza delle azioni risolutive adottate. Le attestazioni periodiche vengono trasmesse all'OdV.

Ogni informazione, segnalazione, report previsti nel Modello sono conservati presso l'ufficio del Presidente dell'OdV ed accessibili a tutti i componenti dell'OdV per un periodo di 5 anni.

3.7. Sistema sanzionatorio

Per l'efficacia del modello di organizzazione, gestione e controllo è fondamentale prevedere, per i casi di violazione dei principi etici e delle prescrizioni e procedure previste dal modello stesso, un adeguato sistema sanzionatorio, conforme al CCNL applicabile e all'art. 7 dello Statuto dei lavoratori.

È da precisare che, in caso di violazioni del Modello e del Codice Etico, l'applicazione del sistema disciplinare e delle relative sanzioni da parte del datore di lavoro è indipendente dallo svolgimento e dall'esito del procedimento penale eventualmente avviato dall'autorità giudiziaria a carico dell'autore materiale della condotta criminosa.

3.7.1 Sanzioni per personale dipendente o distaccato non dirigente

In caso di violazione del modello da parte di personale dipendente non dirigente, o anche da parte di personale non dirigente distaccato presso ICTLAB PA, si applicheranno i seguenti provvedimenti disciplinari, previsti dall'art. 225 del Contratto Collettivo Nazionale di Lavoro del terziario, della distribuzione e dei servizi:

a) biasimo inflitto verbalmente per le mancanze lievi;

b) biasimo inflitto per iscritto nei casi di recidiva delle infrazioni di cui al precedente punto a);

c) multa in misura non eccedente l'importo di 4 ore della normale retribuzione;

d) sospensione dalla retribuzione e dal servizio per un massimo di giorni 10;

e) licenziamento disciplinare senza preavviso e con le altre conseguenze di ragione e di legge.

ICTLAB PA applicherà i provvedimenti di cui alle precedenti lettere a), b), c), d) ed e) a seconda della gravità della condotta, ovvero in relazione alla entità delle mancanze e alle circostanze che le accompagnano.

In particolare, l'applicazione delle sanzioni deve ispirarsi al principio della proporzionalità previsto dall'art. 2106 del c.c., cioè deve essere graduata in ragione della gravità oggettiva del fatto costituente infrazione disciplinare.

A tal fine si terrà conto:

- dell'intenzionalità del comportamento o del grado della colpa;
- del comportamento complessivo del dipendente con particolare riguardo alla sussistenza o meno di precedenti disciplinari;
- del livello di responsabilità e autonomia del dipendente autore dell'illecito disciplinare;

- della gravità degli effetti del medesimo con ciò intendendosi il livello di rischio cui la società ragionevolmente può essere stata esposta – ai sensi e per gli effetti del D.Lgs.231/2001 – a seguito della condotta censurata;
- delle altre particolari circostanze che accompagnano l'illecito disciplinare.

L'eventuale adozione di un provvedimento disciplinare sarà comunicata al dipendente non dirigente, da parte di ICTLAB PA, con lettera raccomandata entro 15 giorni dalla scadenza del termine assegnato al lavoratore stesso per presentare le sue controdeduzioni, così come previsto dall'art. 227 del CCNL di riferimento.

3.7.2 Sanzioni per personale dipendente con qualifica di dirigente

In caso di violazione o di adozione di comportamenti non conformi alle prescrizioni del Modello da parte dei Dirigenti, sebbene oggi non presenti nella struttura aziendale, risultano ad essi applicabili le misure disciplinari conformi a quanto previsto dal Contratto Collettivo Nazionale di Lavoro di riferimento e compatibilmente con i principi sanciti dal Codice Civile, nonché dalle eventuali ulteriori normative speciali applicabili.

In particolare, nel caso in cui la violazione del Modello Organizzativo dovesse portare il venir meno del rapporto fiduciario con la Società, verranno verificate le sanzioni con riferimento alle potenziali violazioni delle regole e dei principi contenuti nel Modello organizzativo e nel Codice Etico, nel rispetto dei generali principi di gradualità e proporzionalità delle sanzioni, e dunque:

- della gravità delle violazioni poste in essere;
- delle funzioni del lavoratore, e della intensità del vincolo fiduciario sotteso al rapporto di lavoro;
- della prevedibilità dell'evento;
- della intenzionalità del comportamento o del grado di negligenza, imprudenza o imperizia del dirigente;
- del comportamento complessivo tenuto in azienda dal dirigente, con particolare riguardo alla sussistenza o meno di precedenti disciplinari in capo al medesimo, nei limiti consentiti dalla legge;
- di tutte quelle altre circostanze che caratterizzano il concreto comportamento del lavoratore.

3.7.3 Sanzioni per i collaboratori ed i consulenti

Conformemente a quanto previsto al paragrafo 3.7.5, in caso di violazione accertata del modello da parte di un collaboratore, ICTLAB PA potrà considerare tale comportamento contrario alle regole della correttezza e quindi l'esecuzione del contratto di collaborazione potrà essere considerata non secondo buona fede, in violazione delle disposizioni contenute negli artt. 1175 e 1375 c.c..

Nei casi più gravi, pertanto, ICTLAB PA potrà decidere di recedere dal contratto di collaborazione.

In caso di recesso anticipato dal contratto, ICTLAB PA sarà tenuta esclusivamente al pagamento del compenso per l'attività svolta e per le spese sostenute sino al momento del recesso, con riserva di richiedere il risarcimento del dannoqualora dal comportamento tenuto derivino danni concreti alla Società.

3.7.4 Sanzioni per i componenti degli Organi sociali

In caso di violazione delle prescrizioni del Modello da parte dell'Amministratore Unico, l'OdV informa l'Assemblea dei Soci e, ove nominato, il Collegio Sindacale, il quale adotta le misure più idonee tra quelle previste dalla legge come ad esempio il richiamo in forma scritta, la previsione di meccanismi di sospensione temporanea e revoca di deleghe eventualmente conferite. In caso di condanne nei confronti dell'Organo Amministrativo può essere disposta la decadenza/revoca della carica sociale ricoperta (questa dovrà comunque essere rimessa ad una deliberazione dell'Assemblea dei Soci che potrà anche non ravvisarne l'utilità e la necessità).

3.7.5 Sanzioni per partner, fornitori ed altri soggetti terzi

I principi e i contenuti del Modello 231 sono portati a conoscenza di tutti coloro con i quali la Società intrattiene relazioni contrattuali. L'impegno all'osservanza della legge e dei principi di riferimento del Modello 231 da parte dei terzi aventi rapporti contrattuali con ICTLAB PA è previsto da apposita clausola del relativo contratto ed è oggetto di accettazione da parte del terzo contraente.

Conformemente a quanto previsto al paragrafo 3.7.3, ogni violazione dei principi e delle prescrizioni del Modello da parte dei partner, dei fornitori, dei consulenti e altri soggetti con cui ICTLAB PA entri in contatto, è sanzionata secondo quanto previsto nelle specifiche clausole contrattuali inserite nei relativi contratti.

ICTLAB PA potrà comunqueriservarsi di adottare tutte le misure necessarie qualora i comportamenti che integrano violazioni dei principi di comportamento o delle prescrizioni previste dal Modello 231 risultino contrari alle regole della correttezza e della buona fede e quindi l'esecuzione dei contratti risulti contraria ai canoni civilistici, in violazione delle disposizioni contenute negli artt. 1175 e 1375 c.c..

Resta salva l'eventuale richiesta di risarcimento qualora dal comportamento tenuto derivino danni patrimoniali o non patrimoniali alla Società.

4. PARTE SPECIALE

Come esplicato nella parte generale del presente Modello, la disciplina della responsabilità amministrativa degli enti prevede che la Società possa risultare responsabile non per tutti i reati previsti dal nostro Ordinamento, ma solo per determinati di questi.

Infatti, il Decreto legislativo n. 231/2001 individua esattamente quali fattispecie penali siano suscettibili di generare la responsabilità degli Enti.

Ai fini di massima chiarezza, posto che la materia di cui si tratta è parte della scienza del diritto e possono occorrere validi strumenti e determinate informazioni/dati per comprendere le diverse fattispecie di reato di cui all'Allegato1della Parte Generale del Modello Organizzativo, in questa Parte Speciale, si espongono sinteticamente le caratteristiche dei c.d. reati "presupposto", indicandone la rilevanza ai fini della disciplina della responsabilità degli enti e si evidenziano determinati principi generali del diritto e varie nozioni scientifiche (quale ad esempio la nozione di Pubblica Amministrazione) utili ai fini di una effettiva comprensione inerente le condotte criminose che si desidera evitare nell'ambito dell'attività aziendale.

Forniti gli strumenti ritenuti necessari per comprendere effettivamente le varie tipologie di fattispecie di reato sensibili ai sensi del Decreto legislativo n. 231/2001, mediante un'analisi delle diverse ipotesi di reato e una valutazione delle funzioni svolte nell'ambito delle varie aree decisionali di ICTLAB PA, della documentazione aziendale, dei rilevati flussi informativi e delle interviste effettuate, si individuano nel modo più preciso possibile le aree di rischio di commissione di reato e si indicano i vari presidi utili per evitare la commissione dei reati da parte di dipendenti/collaboratori di ICTLAB PA nel suo interesse e/o a suo vantaggio.

4.1 Fattispecie di reato

La Parte Speciale si riferisce ai reati potenzialmente realizzabili all'interno della ICTLAB PA di cui di seguito si descrivono brevemente, per una completa informativa, le singole fattispecie contemplate nel D.Lgs. 231/2001.

REATI CONTRO LA PUBBLICA AMMINISTRAZIONE (ai sensi degli artt. 24 e 25 del D.Lgs. 231/2001)

La nozione di Pubblica Amministrazione

La prima tipologia di Reati astrattamente applicabili e rilevanti per la Società è costituita dai reati contro la Pubblica Amministrazione disciplinati dagli artt. 24 e 25 del Decreto (di seguito, "Reati contro la P.A.").

L'analisi dei Reati contro la P.A., ai fini della costruzione del Modello, presuppone, innanzitutto, una chiara definizione dei termini "Pubblica Amministrazione" (di seguito, "P.A."), "Pubblico Ufficiale" (di seguito, "P.U.") ed "Incaricato di Pubblico Servizio" (di seguito, "I.P.S.").

Per P.A. si intende l'insieme di enti e soggetti pubblici (Stato, Ministeri, Regioni, Province, Comuni, etc.) e talora privati (organismi di diritto pubblico, concessionari, amministrazioni aggiudicatrici, S.p.A. miste, etc.) e tutte le altre figure che svolgono in qualche modo la funzione pubblica, nell'interesse della collettività e quindi nell'interesse pubblico.

L'art. 22, comma 1, lett. e), della Legge n. 241/1990 ha ridefinito il concetto di Pubblica Amministrazione ricomprendendovi "*tutti i soggetti di diritto pubblico e i soggetti di diritto privato limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o comunitario*".

La nozione di P.U. è fornita direttamente dal legislatore all'art. 357 del c.p., il quale identifica il "pubblico ufficiale" in "*chiunque eserciti una pubblica funzione legislativa, giudiziaria o amministrativa*", specificando 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*". L'elemento che caratterizza il P.U. è l'*esercizio di una funzione pubblica* e, pertanto, rientrano in tale nozione:

a. i soggetti che concorrono a formare la volontà dell'ente pubblico, ovvero lo rappresentano all'esterno;
b. tutti coloro che sono muniti di poteri autoritativi;
c. tutti coloro che sono muniti di poteri di certificazione.

I poteri pubblici in rilievo sono il *potere legislativo*, quello *giudiziario* e, da ultimo, quello riconducibile alla *pubblica funzione amministrativa*.

Il *potere legislative* trova la sua esplicazione nell'attività normativa vera e propria ovvero in tutte quelle accessorie e/o preparatorie di quest'ultima. È ritenuto P.U., in quanto svolge la *pubblica funzione legislativa*, chiunque, al livello nazionale e comunitario, partecipi all'esplicazione di tale potere. I soggetti pubblici a cui normalmente può ricondursi l'esercizio di tale tipo di funzione sono: il Parlamento, il Governo (limitatamente alle attività legislative di sua competenza, quali decreti legge e decreti delegati), le Regioni, le Province (queste ultime per quanto attiene alla loro attività normativa) e le Istituzioni dell'Unione Europea.

Il *potere giudiziario* trova la sua esplicazione nell'attività dello *ius dicere*, inteso in senso lato. E' ritenuto P.U., in quanto svolge la *pubblica funzione giudiziaria* non solo chi, a livello nazionale e comunitario, svolga una attività diretta all'esplicazione di tale potere, ma anche chi svolge tutta l'attività afferente l'amministrazione della giustizia, collegata ed accessoria alla prima. Svolgono tale tipo di funzione, pertanto, tutti coloro che, a livello nazionale e comunitario, partecipano sia alla vera e propria attività dello *ius dicere*, sia a quella amministrativa collegata allo stesso, ovvero i magistrati (compresi i pubblici ministeri), i cancellieri, i segretari, i membri della Corte di Giustizia e della Corte dei Conti Comunitarie, i funzionari e gli addetti allo svolgimento dell'attività amministrativa collegata allo *ius dicere* della Corte di Giustizia e della Corte dei Conti Comunitarie, etc.

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

- il *potere deliberative* della P.A. è quello relativo alla "*formazione e manifestazione della volontà della Pubblica Amministrazione"*. Tale definizione comprende qualsiasi attività che concorra in qualunque modo ad estrinsecare il potere deliberativo della Pubblica Amministrazione; in tale prospettiva, sono stati qualificati come '*pubblici ufficiali*', non solo le persone istituzionalmente preposte ad esplicare tale potere ovvero i soggetti che svolgono le attività istruttorie o preparatorie all'*iter* deliberativo della Pubblica Amministrazione, ma anche i loro collaboratori, saltuari ed occasionali;
- il *potere autoritativo* della P.A. consiste nel potere della Pubblica Amministrazione di realizzare i propri fini mediante veri e propri comandi, rispetto ai quali il privato si trova in una situazione di soggezione. Questo ruolo di supremazia della P.A. è, ad esempio, facilmente individuabile nel potere della stessa di rilasciare concessioni ai privati. Possono essere qualificati come '*pubblici ufficiali*' tutti i soggetti preposti ad esplicare tale potere;
- il *potere certificativo* della P.A. consiste nel potere di rappresentare come certa una determinata situazione sottoposta alla cognizione di un 'pubblico agente'.

La giurisprudenza più recente ha esteso la qualifica di P.U. anche al c.d. funzionario di fatto, ovvero colui che eserciti una funzione pubblica pur senza formale o regolare "investitura", con la tolleranza o acquiescenza dell'Amministrazione.

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

Si considera I.P.S. colui il quale presta un '*pubblico servizio*' a qualunque titolo. Si intendono attività di pubblico servizio:

a) le attività di produzione di beni e servizi di interesse generale e assoggettate alla vigilanza di un'autorità pubblica;
b) le attività volte a garantire i diritti della persona alla vita, alla salute, alla libertà, alla previdenza e assistenza sociale, all'istruzione, alla libertà di comunicazione, in regime di concessione e/o di convenzione.

L'effettiva ricorrenza dei requisiti richiesti per l'I.P.S. deve essere verificata, caso per caso, in ragione della concreta ed effettiva possibilità di ricondurre l'attività di interesse alle richiamate definizioni, essendo certamente ipotizzabile anche che soggetti appartenenti alla medesima categoria, ma addetti ad espletare differenti *funzioni* o *servizi*, possano essere diversamente qualificati proprio in ragione della non coincidenza dell'attività da loro in concreto svolta. Pertanto, anche un privato o il dipendente di una società privata può essere qualificato quale I.P.S. quando svolge attività finalizzate al perseguimento di uno scopo pubblico e alla tutela di un interesse pubblico.

La qualifica di I.P.S. spetta anche a chi, senza un regolare e/o formale atto di nomina ma comunque non abusivamente, svolga di fatto un pubblico servizio.

Con la Legge n. 300/2000, la qualifica di P.U. e di I.P.S. è stata estesa anche ai membri degli organi della Comunità Europea ed ai funzionari della Comunità Europea e di Stati esteri (art. 322-*bis* c.p.).

I REATI

Gli articoli 24 e 25 del D.Lgs. n. 231/2001 prevedono ipotesi di reato del codice penale riguardanti le seguenti fattispecie:

- malversazione ai danni dello Stato (art. 316-*bis* C.P.);
- indebita percezione di erogazioni a danno dello Stato (art. 316-*ter* C.P.);
- truffa in danno dello Stato o di un ente pubblico (anche comunitario) per il conseguimento di erogazioni pubbliche (artt. 640 II c. n. 1 – 640-*bis* C.P.);
- frode informatica in danno dello Stato o di un ente pubblico (anche comunitario – art. 640-*ter* C.P.);
- concussione (art. 317 C.P.);
- induzione indebita a dare o promettere utilità (art. 319-*quater* C.P.);
- corruzione (artt. 318, 319 e 319-*ter* C.P.);
- istigazione alla corruzione (art. 322 C.P.);
- concussione, corruzione e istigazione alla corruzione di membri di organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322-*bis* C.P.);
- traffico di influenze illecite (art. 346-*bis* C.P.);
- frode nelle pubbliche forniture (art. 356 C.P.);
- frode ai danni del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale (art. 2 L. 898/1986);
- peculato (art. 314, comma 1 C.P.);
- peculato mediante profitto dell'errore altrui (art. 316 C.P.);
- abuso d'ufficio (art. 323 C.P.).

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del D.Lgs. 231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal Decreto. A tal fine, riportiamo qui di seguito una breve descrizione dei reati richiamati dagli artt. 24 e 25 del D.Lgs. 231/2001.

CONCUSSIONE (art. 317 c.p.)

Tale ipotesi di reato si perfeziona quando un pubblico ufficiale o un incaricato di un pubblico servizio, abusando della propria posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli. Questo reato è suscettibile di un'applicazione meramente residuale in questa sede ai fini della individuazione dell'ambito di incidenza delle fattispecie considerate dal D.Lgs. 231/2001; in particolare, tale forma di reato potrebbe ravvisarsi, nell'ambito di applicazione del D.Lgs. 231/2001 stesso, nell'ipotesi in cui un dipendente od un agente della Società concorra nel reato del pubblico ufficiale, il quale, approfittando di tale qualità, richieda a terzi prestazioni non dovute (sempre che, da tale comportamento, derivi in qualche modo un vantaggio per la Società).

LE FATTISPECIE DI CORRUZIONE (artt. 318 e ss. c.p.)

Il reato di corruzione consiste, in generale, in un accordo criminoso avente ad aggetto il mercimonio, il baratto dell'attività funzionale della pubblica amministrazione, a fronte della dazione di una somma di danaro od altra utilità da parte del privato, nei confronti del pubblico ufficiale. E' sufficiente a configurare il reato in esame, anche la sola accettazione della promessa inerente la suddetta dazione.

Il codice distingue innanzitutto la corruzione propria dalla corruzione impropria. Il criterio discretivo è dato dalla contrarietà ai doveri d'ufficio: la corruzione è propria se il mercimonio dell'ufficio concerne un atto contrario ai doveri di ufficio; la corruzione è impropria se la compravendita ha per oggetto un atto conforme ai doveri di ufficio.

La corruzione poi si scinde in antecedente e susseguente: la prima si ha se la retribuzione è pattuita anteriormente al compimento dell'atto e al fine di compierlo; la seconda si configura se la retribuzione concerne un atto già compiuto. Nel caso di corruzione impropria susseguente, l'art. 321 esclude la punibilità del corruttore.

Segnatamente, la fattispecie prevista dall'art. 318 c.p. (corruzione per un atto d'ufficio) si realizza quando il pubblico ufficiale, per compiere un atto del suo ufficio, riceve, per sé o per un terzo, in denaro od altra utilità, una retribuzione che non gli è dovuta o ne accetta la promessa.

La fattispecie di cui all'art. 319 c.p. (corruzione per un atto contrario ai doveri d'ufficio) si realizza quando il pubblico ufficiale per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve per sé o per altri danaro od altra utilità o ne accetta la promessa.

Le disposizioni dell'articolo 319 c.p. si applicano anche se il fatto è commesso da persona incaricata di un pubblico servizio; quelle di cui all'articolo 318 c.p. si applicano anche alla persona incaricata di un pubblico servizio, quale definito dall'art. 358 c.p., ma solo qualora rivesta la qualità di pubblico impiegato.

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

La nozione di pubblico ufficiale e di incaricato di pubblico servizio

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

Sebbene non esista nel codice penale una definizione di Pubblica Amministrazione, in base a quanto stabilito nella relazione Ministeriale allo stesso codice, la Pubblica Amministrazione comprende, in relazione ai reati in esso previsti, "tutte le attività dello Stato e degli altri enti pubblici".

Si rileva che non tutte le persone fisiche che agiscono nella sfera e in relazione ai suddetti enti siano soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie criminose richiamate dal D.lgs. 231/2001.

In particolare, le figure che assumono rilevanza a tal fine sono soltanto quelle dei "pubblici ufficiali" e degli "incaricati di pubblico servizio".

Pubblico Ufficiale

Ai sensi dell'art. 357 c.p., è considerato pubblico ufficiale "agli effetti della legge penale" colui che "*esercita una pubblica funzione legislativa, giudiziaria o amministrativa.*

Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi".

Incaricato Di Pubblico Servizio

Ai sensi dell'art. 358 c.p. *"sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio.*

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

Sulla definizione di entrambe le figure, la giurisprudenza ha chiarito quanto segue.

Al fine di individuare se l'attività svolta da un soggetto possa essere qualificata come pubblica, ai sensi e per gli effetti di cui agli art. 357 e 358 c.p., ha rilievo esclusivo la natura delle funzioni esercitate, che devono essere inquadrabili tra quelle della p.a. Non rilevano invece la forma giuridica dell'ente e la sua costituzione secondo le norme del diritto pubblico, né lo svolgimento della sua attività in regime di monopolio, né tanto meno il rapporto di lavoro subordinato dell'agente con l'organismo datore di lavoro. Nell'ambito dei soggetti che svolgono pubbliche funzioni, la qualifica di pubblico ufficiale è poi riservata a coloro che formano o concorrano a formare la volontà della p.a. o che svolgono tale attività per mezzo di poteri autoritativi o certificativi, mentre quella di incaricato di pubblico è assegnata dalla legge in via residuale a coloro che non svolgono pubbliche funzioni ma che non curino neppure mansioni di ordine o non prestino opera semplicemente materiale.

Al fine di individuare se l'attività svolta da un soggetto possa essere qualificata come pubblica, ai sensi e per gli effetti di cui agli art. 357 e 358 c.p., è necessario verificare se essa sia o meno disciplinata da norme di diritto pubblico, quale che sia la connotazione soggettiva del suo autore, distinguendosi poi - nell'ambito

dell'attività definita pubblica sulla base del detto parametro oggettivo - la pubblica funzione dal pubblico servizio per la presenza (nell'una) o la mancanza (nell'altro) dei poteri tipici della potestà amministrativa, come indicati dal comma 2 dell'art. 357 predetto.

CORRUZIONE PER UN ATTO D'UFFICIO O CONTRARIO AI DOVERI D'UFFICIO (Artt. 318-319 C.P.)

Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale, ovvero un incaricato di pubblico servizio (per estensione, in virtù del disposto dell'art. 320 c.p.) riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del suo ufficio (determinando un vantaggio in favore dell'offerente).

L'attività del pubblico ufficiale, ovvero dell'incaricato di un pubblico servizio, potrà estrinsecarsi sia in un atto dovuto (ad esempio: velocizzare una pratica la cui evasione è di propria competenza), sia in un atto contrario ai suoi doveri (ad esempio: pubblico ufficiale che accetta denaro per garantire l'aggiudicazione di una gara).

Tale ipotesi di reato si differenzia dalla concussione, in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale o dell'incaricato di un pubblico servizio.

CORRUZIONE IN ATTI GIUDIZIARI (art. 319-ter)

Tale ipotesi di reato si configura nel caso in cui un soggetto, parte di un procedimento giudiziario, al fine di ottenere un vantaggio nel procedimento stesso corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario).

INDUZIONE INDEBITA A DARE O PROMETTERE UTILITÀ (art. 319-quater C.P.)

Commette il delitto di induzione a dare o promettere utilità (art. 319-quater c.p.), salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio il quale, abusando della sua qualità o dei suoi poteri, induce taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.

Nei casi suindicati è punito anche chi dà o promette denaro o altra utilità al pubblico ufficiale o all'incaricato di pubblico servizio.

ISTIGAZIONE ALLA CORRUZIONE (art. 322 c.p.)

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale rifiuti l'offerta illecitamente avanzatagli.

CONCUSSIONE, CORRUZIONEE ISTIGAZIONE ALLA CORRUZIONE DI MEMBRI DI ORGANI DELLE COMUNITÀ EUROPEE E DI FUNZIONARI DELLE COMUNITÀ EUROPEE E DI STATI ESTERI (art. 322-bis c.p.)

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

Ciò premesso, va detto che l'art. 322-*bis* c.p. incrimina altresì – e questo è d'interesse per i privati che abbiano a che fare con i soggetti sopra elencati – tutti coloro che compiano le attività colpite dagli artt. 321 e 322 c.p. (cioè attività corruttive) nei confronti delle persone medesime, e non solo i soggetti passivi della corruzione. Inoltre, l'art. 322-*bis* c.p. incrimina anche l'offerta o promessa di denaro o altra utilità *"a persone che esercitano funzioni o attività corrispondenti aquelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri* [diversi da quelli dell'Unione Europea] *o organizzazioni pubbliche internazionali, qualora ilfatto sia commesso per procurare a sé o altri un indebito vantaggio in operazioni economicheinternazionali" (art. 322-bis.2.2)*.

MALVERSAZIONE A DANNO DELLO STATO O DELL'UNIONE EUROPEA (art. 316-bis c.p.)

Tale ipotesi di reato si perfeziona nel caso in cui un soggetto, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate.La condotta, infatti, consiste nell'avere distratto, anche parzialmente, la somma ottenuta, senza che rilevi che l'attività programmata si sia comunque svolta.

Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

INDEBITA PERCEZIONE DI EROGAZIONI IN DANNO DELLO STATO O DELL'UNIONE EUROPEA (art. 316-ter c.p.)

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

In questo caso, contrariamente a quanto visto in merito al punto precedente (art. 316-bis c.p.), a nulla rileva l'uso che venga fatto delle erogazioni, poiché il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va evidenziato che tale ipotesi di reato è residuale rispetto alla fattispecie della truffa ai danni dello Stato, nel senso che si configura solo nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

TRUFFA IN DANNO DELLO STATO, DI ALTRO ENTE PUBBLICO O DELL'UNIONE EUROPEA (art. 640, comma 2 n. 1, c.p.)

Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea).

Tale reato può realizzarsi ad esempio nel caso in cui, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non veritiere (ad esempio supportate da documentazione artefatta) al fine di ottenere l'aggiudicazione della gara stessa.

TRUFFA AGGRAVATA PER IL CONSEGUIMENTO DI EROGAZIONI PUBBLICHE (art. 640-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche.

Tale fattispecie può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

FRODE INFORMATICA IN DANNO DELLO STATO O DI ALTRO ENTE PUBBLICO (art. 640-ter c.p.)

Tale ipotesi di reato si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danno a terzi. In concreto, può integrarsi il reato in esame qualora, una volta ottenuto un finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

TRAFFICO DI INFLUENZE ILLECITE (art. 346-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, fuori dei casi di concorso nei reati di cui agli articoli 319 e 319-ter, sfruttando relazioni esistenti con un pubblico ufficiale o con un incaricato di un pubblico servizio, si ottiene indebitamente denaro o altro vantaggio patrimoniale, come 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.

FRODE NELLE PUBBLICHE FORNITURE (art. 356 c.p.)

Tale ipotesi di reato si configura nel caso in cuisi commette frode nella esecuzione dei contratti di fornitura o nell'adempimento degli altri obblighi contrattuali conclusi con lo Stato, o con un altro ente pubblico, ovvero con un'impresa esercente servizi pubblici o di pubblica necessità.

FRODE AI DANNI DEL FONDO EUROPEO AGRICOLO DI GARANZIA E DEL FONDO EUROPEO AGRICOLO PER LO SVILUPPO RURALE (art. 2 L. 898/1986)

Tale ipotesi di reato si configura nel caso in cui, mediante l'esposizione di dati o notizie falsi, si consegue indebitamente, per se' o per altri, aiuti, premi, indennità, restituzioni, contributi o altre erogazioni a carico totale o parziale del Fondo europeo agricolo di garanzia e del Fondo europeo agricolo per lo sviluppo rurale.

PECULATO (art. 314, comma 1 c.p.)

Tale ipotesi di reato si configura nel caso in cui, il pubblico ufficiale o l'incaricato di un pubblico servizio, che, avendo per ragione del suo ufficio o servizio il possesso o comunque la disponibilità di denaro o di altra cosa mobile altrui, se ne appropria.

PECULATOMEDIANTE PROFITTO DELL'ERRORE ALTRUI (art. 316 c.p.)

Tale ipotesi di reato si configura nel caso in cui, il pubblico ufficialeol'incaricato di un pubblico servizionell'esercizio delle funzioni o del servizio, giovandosi dell'errore altrui,riceveo ritiene indebitamente, per sé o per un terzo, denaroodaltrautilità.

ABUSO D'UFFICIO (art. 323 c.p.)

Tale ipotesi di reato si configura nel caso in cui, il pubblico ufficialeo l'incaricato di pubblico servizio, nello svolgimento delle funzioni o del servizio, in violazione di norme di legge o di regolamento, ovvero omettendo di astenersi in presenza di un interesse proprio o di un prossimo congiunto o negli altri casi prescritti, intenzionalmente procura a sé o ad altri un ingiusto vantaggio patrimoniale ovvero arreca ad altri un danno ingiusto.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia *quivi* in esame è sicuramente presente.

Ciò è deducibile in funzione della natura della stessa società, della rilevanza e della tipologia dell'attività svolta dall'ente, del costante contatto tra funzionari della P.A. centrale (ad esempio funzionari dei Ministeri) e della PA locale (ad esempio funzionari della Regione) e le figure apicali e i dipendenti di ICTLAB PA.

REATI IN TEMA DI FALSITÀ IN MONETE, CARTE DI PUBBLICO CREDITO E VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO (ai sensi degli artt. 25-bis del D.Lgs. 231/2001)

In linea generale, occorre tener presente che la *falsificazione* può essere definita come una situazione non corrispondente al vero, ma capace di presentarsi all'apparenza come veritiera, traendo in inganno chi ci viene in contatto. Peraltro, non è suscettibile di sanzione qualsiasi falso, ma solo quello capace di ingannare una moltitudine indeterminata di soggetti.

I REATI

L'art. 25-*bis* del D.Lgs. n. 231/2001 prevede ipotesi di reato del codice penale contenuti nel titolo VII, ad oggetto i "Delitti contro la fede pubblica", in cui l'interesse tutelato è la fede pubblica, garantita attraverso la difesa della regolarità della circolazione monetaria.

In particolare, il suddetto art. 25-*bis* prevede alcuni dei reati contenuti nei capi I e II del titolo VII, riguardanti, rispettivamente:

1. la "falsità in monete, in carte di pubblico credito e in valori di bollo";
2. la "falsità in sigilli o strumenti o segni di autenticazione, certificazione o riconoscimento".

I primi tutelano oggetti ben individuati, ossia:

- monete aventi corso legale: la moneta è un bene economico utilizzato a fini si scambio, come misura di valore o mezzo di pagamento; ha corso legale la moneta che lo Stato impone come ordinario strumento di pagamento, in base al valore ad essa conferito;
- carte di pubblico credito: ricomprendono le monete aventi corso legale, le carte o cedole al portatore di emanazione governativa e tutte le altre emesse da organi a ciò deputati ed aventi corso legale;

- valori di bollo: carte bollate, francobolli ed altri valori dello stesso genere disciplinati da leggi speciali.
- La previsione di tali reati, in relazione alla responsabilità degli enti, deriva sostanzialmente dal processo di unificazione monetaria europeo.
- Le ipotesi di reato previste dal D.Lgs. n. 231/2001 nell'ambito di tale capo sono le seguenti:
- falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate;
- alterazione di monete;
- spendita e introduzione nello Stato, senza concerto, di monete falsificate;
- spendita di monete falsificate ricevute in buona fede;
- falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati;
- contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo;
- fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata;
- uso di valori di bollo contraffatti o alterati.

I secondi tutelano, invece, beni genericamente indicati come marchi, segni distintivi, brevetti, disegni o modelli industriali.

I reati previsti dal D.Lgs. n. 231/2001, rientranti in questo secondo capo, sono i seguenti:

- contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni;
- introduzione nello Stato e commercio di prodotti con segni falsi.

✓ **RILEVANZA**

Per quanto attiene l'attività di ICTLAB PA, le ipotesi delittuose di cui all'art. 25-*bis*, allo stato, non paiono ipotizzabili.

I reati di falso sopra indicati non dovrebbero essere immaginabili nell'ambito delle condotte dei dipendenti/collaboratori di ICTLAB PA e come la società non risulti, ad oggi, svolgere alcuna azione a mezzo della quale o in occasione della quale tali reati possano venir perpetrati.

REATI SOCIETARI (ai sensi degli artt. 25-ter e 25-sexies del D.Lgs. 231/2001)

Si riporta, qui di seguito, una breve descrizione dei reati richiamati dall'art. 25-*ter* (Reati societari) del D.Lgs. 231/2001, anche in questo caso funzionale a coglierne le più dirette potenziali ricadute rispetto alle specificità operative e di assetto organizzativo della società ICTLAB PA.

FALSE COMUNICAZIONI SOCIALI (art. 2621 c.c.)

Salvo quanto previsto dall'articolo 2622, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazione ovvero omettono informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, sono puniti con l'arresto fino a due anni.

La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene.

La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.

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

Nei casi previsti dai commi terzo e quarto, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.

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

Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, i quali, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, esponendo fatti materiali non rispondenti al vero ancorché oggetto di valutazione, ovvero omettendo informazioni la cui comunicazione è imposta dalla legge sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, cagionano un danno patrimoniale alla società, ai soci o ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

Si procede a querela anche se il fatto integra altro delitto, ancorché aggravato a danno del patrimonio di soggetti diversi dai soci e dai creditori, salvo che sia commesso in danno dello Stato, di altri enti pubblici o delle Comunità Europee.

Nel caso di società soggette alle disposizioni della parte IV, titolo III, capo II, del testo unico di cui al Decreto legislativo 24 febbraio 1998, n. 58 e successive modificazioni, la pena per i fatti previsti al primo comma è da uno a quattro anni e il delitto è procedibile d'ufficio.

La pena è da due a sei anni se, nelle ipotesi di cui al terzo comma, il fatto cagiona un grave nocumento ai risparmiatori.

Il nocumento si considera grave quando abbia riguardato un numero di risparmiatori superiore allo 0,1 per mille della popolazione risultante dall'ultimo censimento ISTAT ovvero se sia consistito nella distruzione o riduzione del valore di titoli di entità complessiva superiore allo 0,1 per mille del prodotto interno lordo.

La punibilità per i fatti previsti dal primo e terzo comma è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi.

La punibilità per i fatti previsti dal primo e terzo comma è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene.

La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5 per cento o una variazione del patrimonio netto non superiore all'1 per cento.

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

Nei casi previsti dai commi settimo e ottavo, ai soggetti di cui al primo comma sono irrogate la sanzione amministrativa da dieci a cento quote e l'interdizione dagli uffici direttivi delle persone giuridiche e delle imprese da sei mesi a tre anni, dall'esercizio dell'ufficio di amministratore, sindaco, liquidatore, direttore generale e dirigente preposto alla redazione dei documenti contabili societari, nonché da ogni altro ufficio con potere di rappresentanza della persona giuridica o dell'impresa.

FALSITÀ NELLE RELAZIONI O NELLE COMUNICAZIONI DELLE SOCIETÀ DI REVISIONE (art. 2624 c.c.)

I responsabili della revisione i quali, al fine di conseguire per sé o per altri un ingiusto profitto, nelle relazioni o in altre comunicazioni, con la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni, attestano il falso od occultano informazioni concernenti la situazione economica, patrimoniale o finanziaria della società, ente o soggetto sottoposto a revisione, in modo idoneo ad indurre in errore i destinatari delle comunicazioni sulla predetta situazione, sono puniti, se la condotta non ha loro cagionato un danno patrimoniale, con l'arresto fino a un anno.

Se la condotta di cui al primo comma ha cagionato un danno patrimoniale ai destinatari delle comunicazioni, la pena è della reclusione da uno a quattro anni.

Si precisa che:

- soggetti attivi sono i responsabili della società di revisione; sicché i componenti degli organi di amministrazione e di controllo e i dipendenti della società revisionata possono essere coinvolti solo a titolo di concorso nel reato commesso dal revisore;
- deve sussistere la consapevolezza della falsità e l'intenzione di ingannare i destinatari delle comunicazioni;
- la condotta deve essere idonea ad indurre in errore i destinatari delle comunicazioni;
- la condotta deve essere rivolta a conseguire per sé o per altri un ingiusto profitto;
- la sanzione è più grave se la condotta ha cagionato un danno patrimoniale ai destinatari delle comunicazioni.

IMPEDITO CONTROLLO (art. 2625 c.c.)

Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo o di revisione legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione, sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 euro.

Se la condotta ha cagionato un danno ai soci, si applica la reclusione fino ad un anno e si procede a querela della persona offesa.

La pena è raddoppiata se si tratta di società con titoli quotati in mercati regolamentati italiani o di altri Stati dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al Decreto legislativo 24 febbraio 1998 n. 58.

INDEBITA RESTITUZIONE DEI CONFERIMENTI (artt. 2626 c.c.)

Gli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscono, anche simulatamente, i conferimenti ai soci o li liberano dall'obbligo di eseguirli, sono puniti con la reclusione fino ad un anno.

ILLEGALE RIPARTIZIONE DEGLI UTILI O DELLE RISERVE (art. 2627 c.c.)

Tale condotta criminosa consiste nel ripartire utili o acconti sugli utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartire riserve, anche non costituite con utili, che non possono per legge essere distribuite.

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

ILLECITE OPERAZIONI SULLE AZIONI O QUOTE SOCIALI O DELLA SOCIETÀ CONTROLLANTE (art. 2628 c.c.)

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, sono puniti con la reclusione fino ad un anno.

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.

Se il capitale sociale o le riserve sono ricostituiti prima del termine previsto per l'approvazione del bilancio relativo all'esercizio in relazione al quale è stata posta in essere la condotta, il reato è estinto.

OPERAZIONI IN PREGIUDIZIO DEI CREDITORI (art. 2629 c.c.)

La fattispecie si perfeziona con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori.

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

OMESSA COMUNICAZIONE DEL CONFLITTO DI INTERESSE (art. 2629-bis c.c.)

L'amministratore o il componente del consiglio di gestione di una società con titoli quotati in mercati regolamentati italiani o di altro Stato dell'Unione europea o diffusi tra il pubblico in misura rilevante ai sensi dell'articolo 116 del testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58 e successive

modificazioni, ovvero di un soggetto sottoposto a vigilanza ai sensi del testo unico di cui al decreto legislativo 1° settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998 della legge 12 agosto 1982, n. 576 o del decreto legislativo 21 aprile 1993, n. 124 che viola gli obblighi previsti dall'articolo 2391, primo comma, è punito con la reclusione da uno a tre anni, se dalla violazione siano derivati danni alla società o a terzi.

Art. 2391 c.c. (Interessi degli amministratori)

L'amministratore deve dare notizia agli altri amministratori e al collegio sindacale di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della società, precisandone la natura, i termini, l'origine e la portata; se si tratta di amministratore delegato, deve altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale, se si tratta di amministratore unico, deve darne notizia anche alla prima assemblea utile.

Nei casi previsti dal precedente comma la deliberazione del Consiglio di Amministrazione deve adeguatamente motivare le ragioni e la convenienza per la società dell'operazione.

Nei casi di inosservanza a quanto disposto nei due precedenti commi del presente articolo ovvero nel caso di deliberazioni del consiglio o del comitato esecutivo adottate con il voto determinante dell'amministratore interessato, le deliberazioni medesime, qualora possano recare danno alla società, possono essere impugnate dagli amministratori e dal Collegio Sindacale entro novanta giorni dalla loro data; l'impugnazione non può essere proposta da chi ha consentito con il proprio voto alla deliberazione se sono stati adempiuti gli obblighi di informazione previsti dal primo comma. In ogni caso sono salvi i diritti acquistati in buona fede dai terzi in base ad atti compiuti in esecuzione della deliberazione.

L'amministratore risponde dei danni derivati alla società dalla sua azione od omissione.

L'amministratore risponde altresì dei danni che siano derivati alla società dalla utilizzazione a vantaggio proprio o di terzi di dati, notizie o opportunità di affari appresi nell'esercizio del suo incarico.

FORMAZIONE FITTIZIA DEL CAPITALE (art. 2632 c.c.)

Gli amministratori e i soci conferenti che, anche in parte, formano od aumentano fittiziamente il capitale sociale mediante attribuzioni di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale, sottoscrizione reciproca di azioni o quote, sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione, sono puniti con la reclusione fino ad un anno.

INDEBITA RIPARTIZIONE DEI BENI SOCIALI DA PARTE DEI LIQUIDATORI (art. 2633 c.c.)

I liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, cagionano danno ai creditori, sono puniti, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

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

CORRUZIONE TRA PRIVATI (art. 2635 c.c.)

Con la legge 6 novembre 2012, n. 190, è stato introdotto, tra i reati-presupposto previsti e puniti dal D.Lgs. 231/2001, il reato di "*Corruzione tra privati*", di cui all'art. 2635 c.c., che sanziona, salvo che il fatto costituisca più grave reato, gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori, che, a seguito della dazione o della promessa di denaro o altra utilità, per sé o per altri, compiono od omettono atti, in violazione degli obblighi inerenti al loro ufficio o degli obblighi di fedeltà, cagionando nocumento alla società, prevedendo una pena più lieve se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma. È imputabile, insieme al corrotto anche il corruttore, ovvero chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma.

ILLECITA INFLUENZA SULL'ASSEMBLEA (art. 2636 c.c.)

Chiunque, con atti simulati o fraudolenti, determina la maggioranza in assemblea, allo scopo di procurare a sé o ad altri un ingiusto profitto, è punito con la reclusione da sei mesi a tre anni.

AGGIOTAGGIO (art. 2637 c.c.)

Chiunque diffonde notizie false, ovvero pone in essere operazioni simulate o altri artifici concretamente idonei a provocare una sensibile alterazione del prezzo di strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato, ovvero ad incidere in modo significativo sull'affidamento che il pubblico ripone nella stabilità patrimoniale di banche o di gruppi bancari, è punito con la pena della reclusione da uno a cinque anni.

OSTACOLO ALL'ESERCIZIO DELLE FUNZIONI DELLE AUTORITÀ PUBBLICHE DI VIGILANZA (art. 2638 c.c.)

La condotta criminosa si realizza attraverso l'esposizione nelle comunicazioni alle Autorità di vigilanza previste dalla legge, al fine di ostacolarne le funzioni, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazione, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza, ovvero con l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA, la possibilità che si verifichino reati appartenenti alla tipologia *quivi* in esame è sicuramente presente. Ciò è deducibile in funzione della natura della stessa società, della rilevanza e della tipologia dell'attività svolta dall'ente.

REATI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO (ai sensi dell'art. 25-quater del D.Lgs. 231/2001)

L'art. 25-*quater* è stato introdotto dal legislatore con la Legge n. 7/2003 in ossequio agli obblighi non solo scaturenti dalla Convenzione Internazionale per la repressione del finanziamento del terrorismo, stipulata a New York in data 8 dicembre 1999, ma anche da tutti gli altri strumenti internazionali (Risoluzione del Consiglio di Sicurezza delle Nazioni Unite, convenzioni internazionali ed europee, etc.) adottati nel periodo immediatamente successivo agli attacchi di matrice terroristica del settembre 2001 a New York.

Le relative norme sono state formulate anche nell'ambito del nostro codice penale mediante l'introduzione degli articoli dal 270-*bis* al 270-*sexies*, l'art. 280, gli articoli 280-*bis*, 289-*bis* e 302.

In buona sostanza, trattasi di condotte inerenti all'organizzazione dell'associazione terroristica e di eversione dell'ordine democratico (assistenza, arruolamento addestramento, etc.) ed esecutive del progetto delittuoso (atti di terrorismo, attentati, sequestri di persona, etc.).

- ✓ **RILEVANZA**

Le ipotesi delittuose di cui all'art. 25-*quater* (delitti con finalità di terrorismo ed eversione dell'ordine democratico) risultano ipotizzabili a carico della Società solo astrattamente ed in linea strettamente teorica, atteso che la società non risulta, allo stato, svolgere alcuna azione a mezzo o in occasione della quale gli stessi possano venir perpetrati.

Si aggiunga che mediante tali delitti appare di difficile compimento un vantaggio societario, così come risulta evidente una carenza di interesse in tal senso.

REATI CONSISTENTI IN PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI E REATI CONTRO LA PERSONALITÀ INDIVIDUALE (ai sensi dell'art. 25-quater.1 del D.Lgs. 231/2001)

I reati consistenti in pratiche di mutilazione degli organi genitali femminili sono stati introdotti della Legge n. 7 del 9.01.2006, normativa emanata in attuazione degli articoli 2, 3, 32 della nostra Costituzione, dei principi contenuti nella Dichiarazione e dal Programma di azioni adottati a Pechino il 15 settembre 1995, nonché nella quarta Conferenza mondiale delle Nazioni Unite.

La Comunità Internazionale, infatti, si è sempre occupata delle problematiche relative alle pratiche di mutilazione e maltrattamenti perpetrate ai danni delle donne in quelle culture che non riconoscono la parità di diritti a entrambi i sessi, con particolare attenzione alla condizione delle bambine all'interno di queste società.

I principi fondamentali sanciti nella Dichiarazione universale dei diritti dell'uomo adottata nel 1948 vietano le discriminazioni sessuali nonché la pratica di trattamenti inumani e degradanti.

Il nostro ordinamento ha quindi recepito tramite l'introduzione dell'art. 583-bis del codice penale il divieto di pratiche di mutilazione degli organi genitali femminili.

I delitti contro la personalità individuale sono stati introdotti come reati presupposto ai fini della responsabilità di cui al Decreto n. 231 dal 2003.

Le fattispecie delittuose contro la personalità individuale che implicano la responsabilità dell'ente sono di vario tipo: fattispecie in tema di schiavitù (riduzione o mantenimento in schiavitù; acquisto e alienazione di schiavi; tratta di persone), in materia di prostituzione minorile e di pornografia minorile.

- ✓ **RILEVANZA**

L'analisi dell'attività tipica di ICTLAB PA porta a ritenere che non possano concretizzarsi le sopra citate fattispecie di reato.

REATI DI ABUSO DI INFORMAZIONI PRIVILEGIATE E MANIPOLAZIONE DEL MERCATO (ai sensi dell'art. 25-sexies del D.Lgs. 231/2001)

Tali reati vengono inseriti nell'ambito del Decreto in funzione della direttiva comunitaria 2003/6/CE del Parlamento Europeo e del Consiglio del 28.01.2003. In virtù dei relativi precetti, sono stati inseriti nel Decreto Legislativo n. 58 del 24.02.1998 (Testo Unico della Finanza) gli articoli 184 e 185 disciplinanti i delitti di "abuso di informazioni privilegiate" e di "manipolazione del mercato".

La realizzazione delle due fattispecie delittuose, alternativamente, implica la responsabilità dell'art. 25-*sexies* del Decreto.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame è in linea astratta presente esclusivamente per il reato di "aggiotaggio finanziario" (art. 185 T.U.F.).

La condotta di tale reato si può sostanziare nella diffusione, ovverosia nella propalazione ad un numero esteso di destinatari, individuati o non individuabili, della "notizia" che non deve avere necessariamente contenuto economico, ma costituire un dato oggettivo connesso alle sorti della società emittente o del relativo strumento finanziario, comprendendo anche le smentite di un fatto vero.

ICTLAB PA, per quanto si tratti di un'ipotesi estremamente improbabile (sia per le dimensioni societarie e dei relativi rapporti, sia per la natura degli ordinari rapporti societari con soggetti terzi, sia anche per la difficoltà di perseguire un vantaggio dalla commissione del reato), potrebbe comunque diffondere notizie sensibili, nel senso sopra esposto, in relazione ad attività negoziali con società quotate.

In ogni caso appare arduo poter rilevare un interesse aziendale e o un vantaggio in favore di ICTLAB PA nell'ambito di un'ipotesi del genere.

REATI COMMESSI IN VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E DELLA SICUREZZA NEI LUOGHI DI LAVORO (ai sensi dell'art. 25-septies del D.Lgs. 231/2001)

Con l'approvazione della L. 3 agosto 2007 n. 123, in vigore dal successivo 25 agosto, è operativa l'estensione della responsabilità dell'ente ai reati di omicidio colposo (art. 589 c.p.) e lesioni colpose gravi e gravissime (art. 590, co. 3, c.p.) commesse in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e salute nel luogo di lavoro.

L'articolo 9 prevede, infatti, l'inserimento dell'articolo 25-*septies* che estende la responsabilità amministrativa degli enti a tali fattispecie di reato e prevede per l'ente sanzioni pecuniarie ed interdittive.

L'impatto di tale intervento normativo è stato senz'altro significativo, considerando, soprattutto, che per la prima volta è stata prevista la punibilità degli enti (tra l'altro anche con sanzioni interdittive) per delitti perseguibili a titolo colposo mentre sino ad oggi tutti i reati presupposto prevedevano la sussistenza del dolo (coscienza e volontarietà dell'azione criminosa).

Lesioni colpose ed omicidio colposo

La lesione è considerata grave (art. 583 c.p., co. 1) nei seguenti casi:

"1) se dal fatto deriva una malattia che metta in pericolo la vita della persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni;

2) se il fatto produce l'indebolimento permanente di un senso o di un organo."

La lesione è considerata invece gravissima se dal fatto deriva (art. 583 c.p., co. 2):

"1) una malattia certamente o probabilmente insanabile;

2) la perdita di un senso;

3) 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;

4) la deformazione, ovvero lo sfregio permanente del viso."

Il reato di omicidio colposo è previsto dall'art. 589 del Codice Penale: *"Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. [...]"*

Le norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

Le norme antinfortunistiche, dirette alla tutela della salute, della sicurezza e dell'igiene nei luoghi di lavoro richiamate dagli articoli del Codice Penale trovano, nella legislazione vigente, fondamentale regolamentazione nel D.Lgs. 9 aprile 2008, n. 81 in attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123 (di seguito "Testo Unico" o, semplicemente "T.U."). Il D. Lgs. 81/2008 individua nel Documento di Valutazione Rischi (di seguito "DVR") il perno attorno a cui ruota il sistema di sicurezza dell'impresa. Il DVR è il documento in cui deve essere formalizzata l'attività di valutazione di "*tutti rischi per la salute e la sicurezza dei lavoratori*" (ivi compresi quelli riguardanti gruppi di lavoratori particolari) (art. 28 comma 1 del T.U.), che il datore di lavoro, unitamente agli ulteriori soggetti identificati dalla normativa in parola, deve effettuare.

Il processo di valutazione rischi richiesto dal Testo Unico deve riguardare tutti i rischi per la sicurezza e la salute dei lavoratori, ivi compresi quelli riguardanti gruppi di lavoratori esposti a rischi particolari, tra cui anche quelli collegati allo stress lavoro-correlato, e quelli riguardanti le lavoratrici in stato di gravidanza. Detto documento impone l'ulteriore obbligo di individuazione ed attuazione di specifiche misure preventive di tutela, nonché la predisposizione di idonei Dispositivi di Protezione Individuale (di seguito "DPI").

Il Modello organizzativo con riferimento ai reati di cui all'art. 25-septies

L'art. 5 del D.Lgs. 231/01 richiede, per la configurabilità della responsabilità dell'ente, che il reato sia stato commesso nell'"interesse o a vantaggio" dell'ente stesso.

Avuta considerazione della natura colposa dei reati di cui alla presente sezione, che sono caratterizzati dalla mancanza di volontà dell'evento da parte del soggetto agente (e peraltro escludendosi la possibilità che sussista un interesse diretto della Società all'accadimento dell'evento infortunistico), si ritiene che il vantaggio per l'ente si possa ravvisare nel risparmio di costi e/o tempi che si possa conseguire nel non dare piena attuazione ai presidi richiesti dalle norme a tutela della salute e sicurezza dei dipendenti.

Ulteriormente, la causa di esclusione della responsabilità per l'ente di cui all'art. 6 del D. Lgs. 231/2001 deve essere valutata in relazione alla struttura colposa del reato. Per i reati dolosi risulta coerente, a norma dell'art. 6 citato, considerare "incolpevole" l'ente che dimostra che il reato è stato posto in essere aggirando fraudolentemente il sistema di controlli posto in essere al fine di prevenire detta tipologia di reati. Diversamente, in un reato colposo dove la volontarietà è limitata alla condotta e non anche all'evento, non si potrà dimostrare che l'agente ha perseguito l'evento aggirando fraudolentemente i presidi posti dalla Società.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame è in linea astratta presente, seppur in misura sensibilmente ridotta.

L'attività non produttiva/industriale in senso proprio, ma di fornitura di servizi, nonché l'attenzione prestata dalla Società alle problematiche sulla sicurezza dei lavoratori, consentono di valutare del tutto marginale il rischio di commissione di tali reati.

REATI COSÌ DETTI TRANSNAZIONALI DI CUI ALLA CONVENZIONE E AI PROTOCOLLI AGGIUNTIVI DELLE NAZIONI UNITE CONTRO IL CRIMINE ORGANIZZATO (ai sensi dell'art. 10 della L. 16.3.2006 n. 146)

Per quel che riguarda i reati transnazionali, la L. 16.3.2006 n. 146, che ha ratificato ed eseguito la Convenzione e i Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale adottati dall'assemblea generale il 15.11.2000 e il 31.05.2001, ha previsto un ulteriore ampliamento del catalogo delle fattispecie che possono determinare la responsabilità amministrativa da reato.

In particolare, introduce le fattispecie interessate nell'ordinamento italiano e prevede, come condizione di realizzazione di tali reati, il coinvolgimento di un gruppo criminale organizzato.

Si evince, infatti, dal dettato normativo dell'art. 3 della citata Legge che è da considerarsi "transnazionale" il reato di:

- associazione di tipo mafioso;
- associazione per delinquere, anche finalizzata al contrabbando di tabacchi lavorati esteri o al traffico illecito di sostanze stupefacenti o psicotrope;
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- favoreggiamento personale;
- traffico di migranti;

purché risponda alle seguenti condizioni:

- punito con la pena della reclusione non inferiore - nel massimo - a quattro anni;
- in cui sia coinvolto un gruppo criminale organizzato;

nonché:

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

✓ RILEVANZA

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame, seppur astrattamente possibile, appare remota.

Si è comunque valutato che il rischio "231" inerente i reati transnazionali potrebbe eventualmente considerarsi rispetto a una fattispecie di reato già giudicata sensibile (seppur in via minimale) nell'ambito nazionale e cioè all'ipotesi di reato di cui all'art. 377-*bis* C.P. che prevede l'"*induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria*".

Ad ogni buon conto, posto che la configurazione del reato transnazionale prevede tra i suoi elementi essenziali il coinvolgimento di un "gruppo criminale organizzato", si può considerare tale rischio limitato a tal punto da poterne valutare l'esclusione.

REATI DI RICETTAZIONE, RICICLAGGIO, IMPIEGO DI DENARO, BENI O UTILITÀ DI PROVENIENZA ILLECITA (ai sensi dell'art. 25-octies del D.Lgs. 231/2001)

L'art. 25-*octies* del Decreto è stato inserito nel *corpus* "231" ad opera dell'art. 63, Decreto Legislativo 21.11.2007 n. 231. La responsabilità amministrativa degli enti, può quindi essere invocata anche con riferimento ai delitti di "ricettazione" (art. 648 C.P.), "riciclaggio" (art. 648-*bis* C.P.) e "impiego di denaro, beni o utilità di provenienza illecita" (art. 648-*ter* C.P.) commessi nell'interesse o a vantaggio dell'ente.

Il Decreto n. 231 del 2007 ha visto la luce in attuazione della c.d. III direttiva antiriciclaggio (direttiva n. 2005/60/CE), concernente la prevenzione dell'utilizzo del sistema finanziario per finalità di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

La norma introdotta ha completato il quadro normativo del Decreto che, già in funzione dell'introduzione dei reati transnazionali, aveva previsto la responsabilità degli enti per i delitti di cui agli articoli 648-*bis* e 648-*ter* C.P..

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame è in linea generale presente, seppur in misura sensibilmente ridotta.

In effetti, i flussi economici e patrimoniali aziendali risultano integralmente tracciati e giustificati, ciò anche in funzione delle metodiche adottate da ICTLAB PA in relazione alle sue certificazioni.

Non vi è utilizzo del contante se non in misura inferiore anche al nuovo limite di trasferimento del contante per i pagamenti di € 1.000,00.

REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ai sensi dell'art. 24-bis del D.Lgs. 231/2001)

La Legge n. 48 del 18 marzo 2008, "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno" ha apportato significative modifiche al Codice Penale e al D.Lgs. n. 231/2001.

Tra le principali modifiche si segnalano:

- l'eliminazione della diversità nella definizione di "documento informatico" tra il diritto civile e il diritto penale;
- l'introduzione del delitto di false dichiarazioni al Certificatore (art. 495-*bis* C.P.); la modifica dell'art. 615 - *quinquies* (diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico);
- la rivisitazione del danneggiamento di dati, programmi, e dei sistemi informatici, anche di pubblica utilità, con l'introduzione della punibilità a querela del danneggiamento di dati "privati";
- l'introduzione di una nuova fattispecie di frode informatica, commessa dal soggetto che presta servizi di certificazione di firma elettronica;
- l'estensione ai reati "informatici" della responsabilità amministrativa degli enti, di cui al D.Lgs. n. 231/2001.

I REATI:

1) Falsità in documenti informatici (art. 491-*bis* del codice penale);
2) Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* del codice penale);
3) Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* del codice penale);
4) Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* del codice penale);
5) Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* del codice penale);
6) Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* del codice penale);
7) Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* del codice penale);
8) Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-*ter* del codice penale);
9) Danneggiamento di sistemi informatici o telematici (art. 635-*quater* del codice penale);
10) Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* del codice penale).

Di seguito una breve analisi dei reati informatici:

FALSITÀ IN DOCUMENTI INFORMATICI (art. 491-bis c.p.)

Tutti i delitti relativi alla falsità in atti, tra i quali rientrano le ipotesi di falso materiale e ideologico, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo bensì un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali. Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (D.Lgs. 82/2005 e succ. modifiche ed integrazioni).

A titolo esemplificativo, integrano il delitto di falsità in documenti informatici la condotta di fraudolento inserimento di dati falsi nelle banche dati pubbliche, oppure la condotta dell'addetto alla gestione degli archivi informatici che proceda, deliberatamente, alla modifica di dati in modo da falsificarli.

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (art. 615-ter c.p.)

Tale reato si perfeziona quando un soggetto si introduce abusivamente 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.

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema, oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

Il delitto potrebbe essere commesso da parte di qualunque dipendente della Società accedendo abusivamente ai sistemi informatici di proprietà di terzi (*outsider hacking*), ad esempio, per prendere cognizione di dati riservati di un partner commerciale (ad esempio, appaltatore o subappaltatore) o un consulente. Ancora, il delitto di accesso abusivo a sistema informatico si considera integrato nel caso in cui un soggetto accede abusivamente ad un sistema informatico e procede alla stampa di un documento contenuto nell'archivio del PC altrui, pur non effettuando alcuna sottrazione materiale di file (accesso abusivo in copiatura), oppure procedendo solo alla visualizzazione di informazioni (accesso abusivo in sola lettura).

DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (art. 615 - quater c.p.)

Tale ipotesi di reato si perfeziona quando un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Questo delitto si perfeziona tanto nel caso in cui il soggetto che sia legittimamente in possesso dei dispositivi di cui sopra (ad esempio, un operatore di sistema) li comunichi senza autorizzazione a terzi, quanto nel caso in cui un soggetto faccia illecitamente uso di questi dispositivi.

L'art. 615 - quater, inoltre, punisce chi rilascia delle istruzioni o indicazioni che rendano possibile la ricostruzione del codice di accesso oppure il superamento delle misure di sicurezza.

Risponde, ad esempio, del delitto di diffusione abusiva di codici di accesso, il dipendente di una società autorizzato ad un certo livello di accesso al sistema informatico che ottenga il livello di accesso superiore, procurandosi codici o altri strumenti di accesso mediante lo sfruttamento della propria posizione all'interno della Società, oppure carpisca in altro modo fraudolento o ingannatorio il codice di accesso.

DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (art. 615-quinquies c.p.)

Tale ipotesi di reato si concretizza qualora taluno, 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 allo scopo di favorire l'interruzione totale o parziale, o l'alterazione del funzionamento del detto sistema, procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Questo delitto si configura, ad esempio, nel caso in cui un soggetto inserisca un virus, idoneo a danneggiare un sistema informatico, nel sistema stesso o qualora produca o utilizzi delle smart card che consentono il danneggiamento di apparecchiature o di dispositivi.

Questi fatti sono punibili solo nel caso in cui il soggetto persegua lo scopo di danneggiare un sistema informatico o telematico, le informazioni, i dati oppure i programmi in essi contenuti o ancora al fine di favorire l'interruzione parziale o totale o l'alterazione del funzionamento dei sistemi o dei dati. Ciò si verifica, ad esempio, qualora un dipendente di una società introduca un virus nel sistema informatico di un concorrente o di un fornitore, in modo da danneggiarlo od interromperne il funzionamento.

INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (art. 617 - quater c.p.)

Tale fattispecie di reato è integrata qualora taluno, fraudolentemente, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, nonché nel caso in cui qualcuno riveli, parzialmente o integralmente, il contenuto delle comunicazioni mediante qualsiasi mezzo di informazione al pubblico.

La fraudolenza consiste nella modalità occulta di attuazione dell'intercettazione, all'insaputa del soggetto che invia o cui è destinata la comunicazione.

Attraverso tecniche di intercettazione è possibile, durante la fase della trasmissione, prendere cognizione del contenuto di comunicazioni tra sistemi informatici o modificarne la destinazione: l'obiettivo dell'azione è tipicamente quello di violare la riservatezza dei messaggi, o comprometterne l'integrità, ritardarne o impedirne l'arrivo a destinazione.

Il reato si perfeziona, ad esempio, con il vantaggio concreto dell'ente, nel caso in cui un dipendente esegua attività di sabotaggio industriale mediante l'intercettazione fraudolenta delle comunicazioni di un concorrente.

INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE O INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (art. 617- quinquies c.p.)

Questo reato si realizza quando qualcuno, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

La semplice installazione di apparecchiature idonee alla intercettazione, pertanto, viene punita poiché rende probabile la commissione del reato di intercettazione.

La fattispecie di reato in questione si considera integrata, con vantaggio dell'ente, nel caso in cui, ad esempio, un dipendente, direttamente o mediante conferimento di incarico ad un investigatore privato, si introduca fraudolentemente presso la sede di un concorrente o di un cliente insolvente al fine di installare apparecchiature idonee all'intercettazione di comunicazioni informatiche o telematiche.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (art. 635-bis c.p.)

Tale fattispecie di reato si perfeziona quando taluno distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui. La sanzione è più grave se il fatto è commesso con abuso della qualità di operatore del sistema.

Costituisce danneggiamento di informazioni, dati e programmi informatici ai sensi dell'art. 635-bis c.p., ad esempio, la condotta di chi proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare di questi dati. Il fatto del danneggiamento potrebbe essere commesso in vantaggio dell'ente laddove, ad esempio, l'eliminazione o l'alterazione dei file o di un programma informatico appena acquistato siano poste in essere al fine di far venire meno la prova del credito da parte del fornitore dell'ente o al fine di contestare il corretto adempimento da parte del fornitore.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI UTILIZZATI DALLO STATO O DA ALTRO ENTE PUBBLICO O COMUNQUE DI PUBBLICA UTILITÀ (art. 635-ter c.p.)

Tale ipotesi di reato si configura quando taluno commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità. Il reato è aggravato se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, o se il fatto è commesso con abuso della qualità di operatore di sistema.

Questo delitto si distingue da quello contemplato dall'articolo 635 – bis c.p. poiché in questo caso il danneggiamento ha ad oggetto beni dello Stato o di altro ente pubblico o, comunque, di pubblica utilità; ne deriva che il delitto sussiste anche nel caso in cui si tratti di dati, informazioni o programmi di proprietà di privati ma destinati alla soddisfazione di un interesse di natura pubblica.

Perché il reato si perfezioni è sufficiente che l'autore tenga una condotta finalizzata al deterioramento o alla soppressione dei dati.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (art. 635-quater c.p.)

Questo reato si perfeziona quando taluno, mediante le condotte di cui all'art. 635-bis c.p. (danneggiamento di dati, informazioni e programmi informatici), ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento. La pena è aumentata se il fatto è commesso con abuso della qualità di operatore di sistema.

Si tenga conto che, qualora l'alterazione dei dati, delle informazioni o dei programmi renda inservibile o ostacoli gravemente il funzionamento del sistema, si integrerà il delitto di danneggiamento di sistemi informatici e non quello di danneggiamento dei dati previsto dall'art. 635 – bis c.p..

Costituisce ipotesi di danneggiamento di sistemi informatici o telematici, ad esempio, il danneggiamento o cancellazione di dati o programmi contenuti nel sistema, effettuati direttamente o indirettamente (per esempio attraverso l'inserimento nel sistema di un virus).

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (art. 635-quinquies c.p.)

Questa fattispecie criminosa si configura quando il fatto descritto dall'art. 635-quater c.p. è diretto a distruggere, danneggiare, rendere, in tutto o in parte inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento. La sanzione è significativamente aggravata se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se lo stesso è reso, in tutto o in parte, inservibile, nonché nelle ipotesi in cui il fatto sia stato commesso con abuso della qualità di operatore di sistema.

Nel delitto di danneggiamento di sistemi informatici o telematici di pubblica utilità (noto come attentato al sistema), diversamente dal delitto di danneggiamento di dati, informazioni e programmi di pubblica utilità (art. 635 – ter c.p.), quel che rileva è che il sistema sia utilizzato per il perseguimento della pubblica utilità, indipendentemente dalla proprietà privata o pubblica del sistema. Ne consegue che il danneggiamento di un sistema informatico di proprietà di un ente pubblico, non utilizzato per il perseguimento di una pubblica utilità, non sarà sanzionabile ai sensi dell'art. 635 – quinquies c.p., ma, piuttosto, ai sensi dell'art. 634 – quater c.p., considerandosi il sistema informatico di proprietà pubblica alla stregua di qualsiasi altro sistema informatico.

Costituisce fattispecie di reato rilevante ai sensi del Decreto, ad esempio, la condotta del dipendente addetto al sistema informatico di un cliente (sistema che deve perseguire uno scopo di pubblica utilità) che, in sede di esecuzione di un contratto di appalto con la Pubblica Amministrazione o con persone incaricate di pubblico servizio, danneggi una parte del sistema medesimo al fine di occultare un inadempimento contrattuale della società dalla quale dipende.

- ✓ **RILEVANZA**

Per la natura dei servizi offerti dalla Società, ICTLAB PA risulta potenzialmente esposta al rischio di commissione dei reati informatici; la consumazione di tali reati è legata ad una potenziale non corretta configurazione e gestione della propria infrastruttura di Information Technology e ai rapporti con soggetti terzi nell'ambito della gestione dei dati e della manutenzione dei prodotti.

DELITTI DI CRIMINALITÀ ORGANIZZATA (ai sensi dell'art. 24-ter del D.Lgs. 231/2001)

La Legge n. 94 del 15 luglio 2009 ha previsto l'aggiunta dell'art. 24-*ter* nell'ambito del *corpus* del Decreto Legislativo n. 231 - 8 giugno 2001.

Il citato provvedimento normativo ha introdotto nell'alveo dei reati che prevedono la responsabilità amministrativa degli enti anche i reati associativi previsti dall'art. 10 L. n. 146/2006 di ratifica della Convenzione ONU sulla lotta alla criminalità organizzata.

Fino a tale provvedimento i reati comportanti la responsabilità amministrativa dell'ente potevano essere considerati un numero chiuso; l'art. 24 *ter* sanziona vari reati:

1) Associazione a delinquere (art. 416 C.P.).
2) Associazioni di tipo mafioso anche straniere (art. 416 *bis* C.P.).
3) Scambio elettorale politico-mafioso (art. 416 *ter* C.P.).
4) Sequestro di persona a scopo di estorsione (art. 630 C.P.).

5) I delitti in materia di stupefacenti (art. 74 D.P.R. n. 309/1990).
6) I delitti in materia di armi (come indicati all'art. 407 II c., lett. a - n. 5 C.P.P.).
7) I delitti commessi avvalendosi delle condizioni previste dal predetto art. 416-*bis* C.P. ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo.

Quest'ultima norma è quella che ha visto nel sistema "231" una modifica di rotta al fine della determinazione dei reati presupposto; infatti, tale norma implica una clausola "aperta" che lascia spazio all'ingresso di tutti quei reati commessi in ambito associativo mafioso e di sostegno alle associazioni mafiose.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichi un sodalizio criminale di natura associativa è presente, seppur in misura ridotta.

DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO (ai sensi dell'art. 25-bis.1 del D.Lgs. 231/2001)

La Legge n. 99 del 23 luglio 2009 recante: "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia", ha ampliato notevolmente il novero dei c.d. "reati presupposto" alla responsabilità amministrativa degli enti, di cui al Decreto Legislativo n. 231 8 giugno 2001, attraverso l'introduzione dell'art. 25-*bis.*1. L'elencazione di cui all'articolo *de quo*, che comprende la gamma dei reati previsti dagli artt. 513 e ss. del codice penale, risponde al bisogno di tutela, avvertito dal Legislatore, dell'ordine economico e del normale e corretto svolgimento delle attività produttive ad esso inerenti.

Nel dettaglio, la responsabilità degli enti è stata estesa anche alle seguenti ipotesi di reato:

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

- ✓ **RILEVANZA**

ICTLAB PA non svolge alcuna attività di produzione di beni materiali o di natura industriale e non ha interessi all'utilizzo di privative e/o titoli di proprietà industriale, nonché marchi e/o segni distintivi di soggetti terzi. In merito alla possibile rilevanza di condotte implicanti profili di responsabilità inerenti la proprietà intellettuale e il diritto d'autore, tale valutazione viene svolta nell'ambito dell'analisi dei delitti in materia di diritto d'autore.

DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE (ai sensi dell'art. 25-novies del D.Lgs. 231/2001)

La Legge n. 99 del 23 luglio 2009 recante: "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia", ha introdotto nell'alveo dei cosiddetti "reati presupposto" del *corpus* legislativo del Decreto Legislativo n. 231 del 2001 la categoria dei delitti in materia di violazione del diritto d'autore.

Tale ampliamento risponde in *primis* ad una più ampia prospettiva di armonizzazione, dettata dalla Commissione Europea, risalente alla Direttiva del 24 giugno 2006, nella quale si afferma la necessità di realizzare, a livello europeo, una sostanziale armonizzazione delle sanzioni penali irrogabili alle persone fisiche e giuridiche che hanno commesso o sono responsabili di violazioni intenzionali di un diritto di proprietà intellettuale commesse su scala commerciale. Ponendosi in una prospettiva prettamente nazionale, l'introduzione di tali ipotesi di reato formalizza l'*intellectual property* quale fattore di rischio

dell'impresa, conferendo la dovuta elevazione a tutti quei contenuti immateriali, strumentali e fondamentali per l'attività d'impresa.

Le ipotesi di reato di cui all'articolo 25-*novies* del Decreto sono quelle previste dagli articoli 171 I comma, lettera a-*bis* e III comma, 171-*bis*, 171-*ter*, 171-*septies* e 171-*octies* della Legge n. 633, del 22 aprile 1941, recante disposizioni in materia di "Protezione del diritto d'autore e di altri diritti connessi al suo esercizio" (LDA).

La normativa in materia di diritto d'autore, funzionale alla tutela delle creazioni intellettuali in vari settori, quali quello della musica, della letteratura, del teatro e, più in generale, di tutti i settori artistici, è stata scelta dal Legislatore anche ai fini della tutela dei programmi per elaboratore, ritenuti anch'essi creazione intellettuale dell'autore.

Tale scelta ha implicato vari e intensi confronti in dottrina e in giurisprudenza, poiché spesso valutata criticamente per la sua lieve efficacia di tutela.

In buona sostanza, il dibattito ha riguardato la possibilità di una scelta più radicale legata a un'opzione brevettuale; ad oggi, risulta comunque in vigore la tutela del diritto d'autore e, tra l'altro, i programmi per elaboratori, il c.d. *software*, possono ottenere una protezione relativa alla paternità e alla data di creazione del prodotto mediante un'apposita registrazione presso gli uffici della S.I.A.E..

Le condotte, con riferimento alle quali si configura la responsabilità dell'ente, riguardano, in generale, l'abusiva riproduzione, pubblicazione, traduzione, trasformazione, modificazione, vendita e distribuzione delle opere intellettuali.

Un'ulteriore ipotesi sensibile ai sensi del Decreto è quella attinente la protezione dei contenuti delle Banche Dati.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame appare remota. La tipologia dell'attività di ICTLAB PA, allo stato, non pare collegarsi in alcun modo con attività sensibile in materia di reati di violazione del diritto d'autore.

DELITTI DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITÀ GIUDIZIARIA, COME PREVISTO EX ART. 377-BIS CODICE PENALE (ai sensi dell'art. 25-decies del D.Lgs. 231/2001)

Il reato di "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" è stato introdotto nel novero degli illeciti penali per i quali vi è responsabilità amministrativa dell'ente nell'agosto del 2009 (con Legge 03 agosto 2009 n. 116) in funzione della ratifica ed esecuzione della Convenzione dell'Organizzazione delle Nazioni Unite contro la corruzione adottata dall'Assemblea generale dell'ONU il 31 ottobre 2003 con risoluzione n. 58/4 firmata dallo Stato italiano il 09 dicembre 2003.

Per errore di procedura normativa il reato era stato introdotto con il riferimento dell'art. 25-*novies*, medesimo riferimento dei reati in materia di violazione del diritto d'autore (anch'essi precedentemente previsti enunciati dall'art. 25-*novies* del Decreto Legislativo n. 231/2001).

Il Decreto Legislativo n. 231/2001 conteneva quindi due art. 25-*novies* con una diversa rubrica e un differente contenuto.

Mediante il Decreto Legislativo n. 121 del 07.07.2011 il Legislatore è intervenuto, correggendo l'erronea numerazione.

Oggi il reato di "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" risulta regolarmente rubricato all'art. 25-*decies* del Decreto Legislativo n. 231/2001.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichi tale reato è senz'altro presente.Pertanto,nell'Allegato 4 - Tabella di correlazione attività sensibili si è evidenziata la presenza di rischi per la commissione di tali reati.

REATI AMBIENTALI (ai sensi dell'art. 25-undecies del D.Lgs. 231/2001)

Dal 16 agosto 2011, con l'entrata in vigore del Decreto Legislativo n. 121 del 07.07.2011, i reati ambientali sono parte di quegli illeciti per cui anche l'Ordinamento italiano ha previsto la responsabilità amministrativa dell'ente.

L'inserimento dei reati ambientali nel novero degli illeciti di cui al D.Lgs. n. 231/2001, da tempo annunciato a seguito del recepimento delle Direttive europee CE 2008/99/CE e 2009/123/CE (in materia di inquinamento provocato dalle navi) prevede nuove misure di tutela penale e un ampliamento delle pene in termini di quote o sanzioni interdittive per molti reati e violazioni già previsti dall'Ordinamento penale.

Peculiare è il fatto che la responsabilità dell'ente sia stata prevista anche nell'ambito dei reati contravvenzionali.

Di seguito vengono indicati esattamente i reati ambientali di cui al decreto:

- norme poste a tutela delle specie animali e vegetali protette e di habitat all'interno dei siti protetti (art.727-bis c.p.);
- norme in materia di scarichi di acque reflue e gestione dei rifiuti previste dal Testo Unico Ambientale (D.Lgs. n. 152/2006);
- attività di gestione di rifiuti non autorizzata (art. 256, commi 1, 3, 5 e 6 primo periodo, D.Lgs. n. 152/2006);
- omessa bonifica dei siti in conformità al progetto approvato dall'autorità competente (art. 257, commi 1 e 2 D.Lgs. n. 152/2006);
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 comma 4, secondo periodo, D.Lgs. n. 152/2006);
- traffico illecito di rifiuti (art. 259, comma 1, D.Lgs. 152/2006);
- attività organizzate per il traffico illecito di rifiuti (art. 260, commi 1 e 2, D.Lgs. n. 152/2006);
- falsità ideologica del certificato di analisi dei rifiuti, anche utilizzato nell'ambito del SISTRI – Area Movimentazione, e falsità ideologica e materiale della scheda SISTRI – Area Movimentazione (art. 260-bis, commi 6, 7, secondo e terzo periodo e 8 D.Lgs. n. 152/2006);
- superamento dei valori limite di emissione che determinano il superamento dei valori limite di qualità dell'aria (Art. 279, comma 5, D.Lgs. n. 152/2006);
- norme a tutela dell'ozono stratosferico (art. 3 L. n. 549/1993);
- norme sul commercio internazionale delle specie animali e vegetali in via di estinzione (L. n. 150/1992);
- falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni previste dall'art. 16, par. 1, lett. a), c), d), e), ed l) del Regolamento CE n. 338/97 e ss. mm. ii. (art. 3-bis, L. n. 150/1992);
- detenzione di esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e per l'incolumità pubblica (art. 6, L. n. 150/1992);
- norme finalizzate alla prevenzione dell'inquinamento provocato dalle navi (D.Lgs. n. 202/2007).

La Legge 22 Maggio 2015, n. 68, ha modificato l'art 25-*undecies* del D.Lgs. 231/01, aggiungendo tra i reati presupposto il delitto di inquinamento ambientale (art. 425-*bis* c.p.), il delitto di disastro ambientale (art. 452-*quater* c.p.), i delitti colposi contro l'ambiente (art.452-*quinquies* c.p.), i delitti associativi aggravati ai sensi dell'articolo 452-*octies*, il delitto di traffico e abbandono di materiale ad alta radioattività (art. 452-*sexies* c.p.) prevedendo per tale violazione la sanzione pecuniaria da duecentocinquanta a seicento quote.

✓ RILEVANZA

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame appare probabile; vi è quindi la presenza di rischi per la commissione di reati ambientali.

REATI IN MATERIA DI IMMIGRAZIONE (ai sensi dell'art. 25-duodecies del D.Lgs. 231/2001)

È entrato in vigore il 09.08.2012 il Decreto Legislativo 16.07.2012, n. 109 recante norme in attuazione della direttiva 2009/52/CE sulle norme minime relative a sanzioni e provvedimenti nei confronti di datori di lavoro che impiegano cittadini di paesi terzi il cui soggiorno è irregolare.

L'articolo 2 del Decreto Legislativo n. 109/2012 recita:

Al decreto legislativo 8 giugno 2001, n. 231, dopo l'articolo "25-*undecies*" e' inserito il seguente:

"25-*duodecies* (Impiego di cittadini di paesi terzi il cui soggiorno è irregolare).

1. In relazione alla commissione del delitto di cui all'articolo 22, comma 12-bis, del Decreto Legislativo 25 luglio 1998, n. 286, si applica all'ente la sanzione pecuniaria da 100 a 200 quote, entro il limite di 150.000 euro".

In particolare, le fattispecie a cui si riferisce la norma sono, per quanto attiene la responsabilità degli enti, quelle previste dall'ipotesi di reato aggravato di cui al comma 12-*bis* dell'art 22 e risultano limitate a tre condotte tipiche:

1) se i lavoratori occupati sono in un numero superiore a tre;
2) se i lavoratori occupati sono minori in età non lavorativa;
3) se i lavoratori occupati sono sottoposti alle altre condizioni lavorative di particolare sfruttamento di cui al terzo comma dell'art. 603-*bis* del codice penale.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame, risulta presente in misura ridotta, sia per le fattispecie in esame, sia per la presenza di procedure aziendali di assunzione (predisposte nel rispetto della normativa giuslavorista vigente).

DELITTI DI PROPAGANDA, ISTIGAZIONE ED INCITAMENTO ALLA VIOLENZA PER MOTIVI RAZZIALI, ETNICI, NAZIONALI O RELIGIOSI (ai sensi dell'art. 25-terdecies del D.Lgs. 231/2001)

L'art. 5 della Legge n. 167/2017 ha ampliato il catalogo dei reati presupposto contenuto nel D.Lgs. 231/2001, introducendo l'art. 25-terdecies, rubricato "razzismo e xenofobia".

Con la suddetta disposizione divengono rilevanti, ai fini della responsabilità penale dell'Ente, tutte le fattispecie di propaganda di idee fondate sulla superiorità o sull'odio razziale o etnico ovvero di istigazione o incitamento a compiere atti di discriminazione per motivi razziali, etnici, nazionali o religiosi.

In questo modo viene dunque estesa la responsabilità amministrativa derivante da reato dell'Ente, a cui, in caso di commissione dei reati sopracitati, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, D.Lgs. 231/2001, per una durata non inferiore a un anno.

Qualora la propaganda, l'istigazione o l'incitamento si fondino in tutto o in parte sulla negazione della Shoah o dei crimini di genocidio, dei crimini contro l'umanità e dei crimini di guerra, si applica la sanzione pecuniaria da duecento a ottocento quote.

Se infine l'Ente è stabilmente utilizzato allo scopo unico o prevalente di consentire o agevolare la commissione dei delitti sopra indicati, si applica la sanzione dell'interdizione definitiva dall'esercizio dell'attivitàai sensi dell'articolo 16, comma 3, D.Lgs. 231/2001.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame appare remota, sia per le fattispecie in esame, sia per la presenza di procedure aziendali a presidio dei processi a rischio di commissione dei reati in commento.

FRODI IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O DI SCOMMESSA E GIOCHI D'AZZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI (ai sensi dell'art. 25-quaterdecies del D.Lgs. 231/2001)

La Legge 3 maggio 2019 n. 39, recante la "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulle manipolazioni sportive, sottoscrittaa Magglingen il 18 settembre 2014*", ha esteso la responsabilità degli enti ai reati di frode in competizioni sportive e di esercizio abusivo di attività di giuoco o di scommesse.

Viene quindi introdotto nel D.Lgs. 231/2001 l'art. 25-*quaterdecies*, a tenore del quale:

"*1. In relazione alla commissione dei reati di cui agli articoli 1 e 4 della legge 13 dicembre 1989, n. 401, si applicano all'ente le seguenti sanzioni pecuniarie: Per i delitti, la sanzione pecuniaria fino a cinquecento quote; Per le contravvenzioni, la sanzione pecuniaria fino a duecentosessanta quote.*

2. Nei casi di condanna per uno dei delitti indicati nel comma 1, lettera a), del presente articolo, si applicano le sanzioni interdittive previste dall'art. 9, comma 2, per una durata non inferiore a un anno".

Nello specifico, il delitto di frode sportiva (art. 1 L. 401/1989) incrimina "*chiunque offre o promette denaro o altra utilità o vantaggio a taluno dei partecipanti ad una competizione sportiva organizzata dalle federazioni riconosciute, al fine di raggiungere un risultato diverso da quello conseguente al corretto e leale svolgimento della competizione, ovvero compie altri atti fraudolenti volti al medesimo scopo*" nonché "*il partecipante alla competizione che accetta il denaro o altra utilità o vantaggio, o ne accoglie la promessa*".

L'art. 4 dello stesso articolato normativo contempla, invece, diverse fattispecie connesse all'esercizio, organizzazione, vendita di attività di giochi e scommesse in violazione di autorizzazioni o concessioni amministrative.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame appare remota.

REATI TRIBUTARI (ai sensi dell'art. 25-quinquiesdecies del D.Lgs. 231/2001)

La riforma dei reati tributari introdotta con la L. 19 dicembre 2019, n. 157, di conversione del D.L. 26 ottobre 2019, n. 124 (c.d. decreto fiscale), ha inserito l'art. 25 *quinquiesdecies*al D.Lgs. 231/2001, interpolandolo ulteriormente.

L'intervento normativo si innesta nel contesto di una costante estensione della responsabilità amministrativa da reato dell'ente, determinata anche da un intervento europeo in tal senso (la direttiva UE 17/1371) e da un clima politico, in materia penale, estremamente rigorista nei confronti dei reati dei c.d. "grandi evasori".

L'art.25*quinquiesdecies*del d.lgs. 231/2001 indica per quali reati tributari (previsti cioè nel novellato D.Lgs. 74/2000) commessi per interesse o vantaggio dell'ente possa determinarsi la responsabilità amministrativa:

a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 1, d.lgs. 74/2000,la sanzione pecuniaria fino a cinquecento quote;
b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 2-*bis*,d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote;
c) per il delitto di dichiarazione fraudolenta mediante altri artifici previsto dall'art. 3, d.lgs. 74/2000, la sanzione pecuniaria fino a cinquecento quote;
d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8,d.lgs. 74/2000, comma 1, la sanzione pecuniaria fino a cinquecento quote;
e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, comma 2-*bis*, d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote;
f) per il delitto di occultamento o distruzione di documenti contabili previsto dall'art. 10,d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote;
g) per il delitto di sottrazione fraudolenta al pagamento di imposte previsto dall'art. 11,d.lgs. 74/2000, la sanzione pecuniaria fino a quattrocento quote.

In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:

a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;
b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;
c) per il delitto di indebita compensazione previsto dall'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote.

In caso di profitto di rilevante entità la sanzione pecuniaria subisce un aumento di un terzo.

Sono inoltre applicabili le sanzioni interdittive di cui all'art. 9, comma 2, d.lgs. 231/2001, lettere c) (divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio), lettera d) (esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi) e lettera e) (divieto di pubblicizzare beni o servizi).

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia in questa sede in esame è sicuramente presente; vi è, pertanto, la presenza di rischi per la commissione di reati tributari.

CONTRABBANDO (ai sensi dell'art. 25-sexiesdecies del D.Lgs. 231/2001)

In data 15 luglio 2020 è stato pubblicato in Gazzetta Ufficiale il Decreto Legislativo n. 75 del 14 luglio 2020 "Attuazione della Direttiva UE 2017/1371 relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale" (cd. Direttiva PIF) che, tra le varie novità, ha ampliato il catalogo dei reati presupposto di cui al D.Lgs. 231/2001.

In particolare, + stato introdotto nel D.Lgs. 231/2001 l'articolo 25-*sexiesdecies*- Contrabbando:

1. *In relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, si applica all'ente la sanzione pecuniaria fino a duecento quote.*
2. *Quando i diritti di confine dovuti superano centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote.*
3. *Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) e e)*.

- ✓ **RILEVANZA**

Nell'ambito dell'attività di ICTLAB PA la possibilità che si verifichino reati appartenenti alla tipologia quivi in esame appare remoto.

4.2 Attività sensibili e misure preventive generali

Tutte le attività compiute all'interno di ICTLAB PA devono essere svolte sempre conformemente alle leggi vigenti ed alle regole fissate dal presente Modello, dal Codice Etico e dai processi Aziendali.

Il rischio di commissione di reati è distribuito nei processi relativi alle diverse aree di ICTLAB PA.

Di seguito si riportano i principi generali di prevenzione adottati dalla Società.

In linea generale il Sistema di Organizzazione della Società deve rispettare i seguenti requisiti fondamentali:

1. Sono adottati strumenti organizzativi (organigramma,funzionigramma, disposizioni di servizio, procedure) orientati ad assicurare:
   - una chiara formalizzazione e delimitazione dei ruoli, delle funzioni, delle responsabilità e dei livelli di autonomia;

- una chiara descrizione delle linee di riporto gerarchico;
- per ciascuna area aziendale, un Sistema di Procure corrispondente agli effettivi poteri di rappresentanza e di delega conferiti mediante le disposizioni organizzative interne;
- un'ampia diffusione e costante disponibilità all'interno dell'Organizzazione dei corrispondenti documenti;

2. tutti i processi devono essere regolamentati da idonee procedure che assicurino:
   - standard comportamentali omogenei cui l'intera organizzazione deve conformarsi;
   - la separazione dei ruoli all'interno di ciascun processo (separatezza tra chi origina il processo, chi lo esegue, chi lo conclude e chi lo controlla);
   - la tracciabilità di ciascuna fase rilevante del processo e delle corrispondenti verifiche;
   - un adeguato livello di formalizzazione dei controlli eseguiti anche a livello di supervisione gerarchica;
3. si deve assicurare un chiaro, efficace e costante processo di comunicazione al personale relativamente al presente Modello, al Codice Etico, ai suoi eventuali aggiornamenti, nonché a modifiche organizzative, definizione dei poteri autorizzativi, delle deleghe, della enucleazione e disciplina dei processi e quant'altro contribuisca a dare trasparenza all'operatività aziendale; inoltre devono essere condotte specifiche sessioni formative per il personale delle Aree sensibili, finalizzate alla diffusione delle informazioni necessarie a migliorare il livello di conoscenza dei processi interessati al rischio di commissione di reati e delle misure di prevenzione previste dai protocolli aziendali;
4. tutti coloro che mantengono formali rapporti con la P.A. per conto di ICTLAB PA, devono essere formalmente abilitati mediante apposita delega (per Dipendenti, distaccati ed Organi sociali) oppure mediante specifico contratto (per collaboratori, consulenti o partner) che, in sostanza, dia conto preventivamente e in maniera trasparente della attribuzione dei poteri connessi alla gestione di tali rapporti e dei relativi limiti. Per i rapporti già in corso alla data di adozione del presente modello, l'Amministratore unico curerà l'adeguamento dei relativi titoli (specificazione delle deleghe rilasciate dal superiore gerarchico o comunque nel rispetto del relativo assetto, ovvero contratti di collaborazione, consulenza o altro) tempestivamente, anche in maniera progressiva e in base all'ordine di priorità imposto dalle effettive occorrenze;
5. i contratti con i collaboratori, i consulenti, partner ed i fornitori devono contenere clausole di impegno al rispetto dei principi del D.Lgs. 231/01 e del Codice Etico e del presente Modello, nonché le sanzioni applicate nei casi di loro inosservanza. Anche in questo caso, per i rapporti in essere alla data di adozione del presente Modello, si procede all'adeguamento con modalità analoghe a quelle sopra evidenziate al punto 4.;
6. i contratti con i clienti devono contenere clausole di presa d'atto dei principi del D.Lgs. 231/01 e del Codice Etico e del Modello 231 adottato da ICTLAB PA;
7. nei nuovi Contratti con i collaboratori, i consulenti, i partner ed i fornitori deve essere inserita un'apposita clausola con cui gli stessi dichiarino, antecedentemente alla stipula del contratto, se sono mai stati assoggettati a misura cautelare, rinviati a giudizio, imputati, condannati (anche con sentenza *ex* art. 444 c.p.p.) per reati di cui al D.Lgs. 231/2001. In caso di provvedimento, anche non passato in giudicato, di condanna ovvero di applicazione della pena su richiesta per reati presupposto per la responsabilità di cui al d.lgs. n. 231/2001, la Società si astiene dall'instaurazione del rapporto con il collaboratore, consulente, partner o fornitore; nelle altre su richiamate ipotesi, ICTLAB PA, acquisite tutte le informazioni consentite del caso, si riserva di adottare ogni più opportuna ed efficace iniziativa a tutela dal rischio della commissione di eventi rilevanti ai sensi del D.Lgs. n. 231/2001;
8. le informazioni, dichiarazioni o comunicazioni rese alla PA devono contenere solo dati e notizie veritiere ed essere sottoposte alla verifica e supervisione di altra funzione indipendente da quelle dell'unità organizzativa che le ha effettuate;
9. i contatti con funzionari pubblici od incaricati di pubblico servizio, da parte di dipendenti, distaccati, consulenti, collaboratori e partner di ICTLAB PA, devono essere tracciati mediante la redazione di specifici verbali riportanti,in maniera sintetica ma completa, lo scopo ed il contenuto degli stessi, protocollati e destinati a restare allegati agli atti del procedimento nonché, in caso di criticità, occorre, anche a cura del responsabile della funzione interessata, informare tempestivamente per iscritto l'O.d.V.;
10. in occasione di ispezioni da parte delle Autorità, i contatti con il personale incaricato delle verifiche devono essere tenuti dall'Amministratore Unico di ICTLAB PA; è fatto obbligo inoltre di redigere specifici resoconti, in forma sintetica ma completa, riportanti l'andamento e gli esiti dell'ispezione, da conservare

protocollati agli atti del procedimento e di informare tempestivamente per iscritto l'O.d.V. di eventuali criticità;

11. I soggetti che hanno rapporti di collaborazione, consulenza o altro con ICTLAB PA, devono informare con nota scritta l'O.d.V. di qualunque criticità o conflitto di interesse nel rapporto con la P.A. di cui vengano a conoscenza, secondo quanto previsto contrattualmente, e con le modalità ivi previste;
12. in tutte le attività di reporting, interlocuzione o coinvolgimento con le Autorità di vigilanza non va frapposto alcun ostacolo all'esercizio delle attività di sorveglianza e vanno fornite, nel pieno rispetto delle normative di legge e delle procedure aziendali, tempestivamente ed in piena correttezza e buona fede, tutte le informazioni richieste;
13. all'insorgere di situazioni di potenziale conflitto di interessi il dipendente o il soggetto operante presso ICTLAB PA in regime di distacco di personale deve comunicare tale situazione al proprio superiore o al soggetto che comunque abbia la responsabilità funzionale di supervisione e coordinamento, astenendosida qualsiasi attività che appaia in conflitto di interesse;
14. nel caso di attività svolte per conto di ICTLAB PA da soggetti terzi, sia soci che non soci, sotto il coordinamento o supervisione di un Dirigente o di un Coordinatore di ICTLAB PA o di un soggetto operante presso ICTLAB PA in regime di distacco di personale, il presente Modello e quindi i protocolli in esso previsti devono essere adottati anche con riferimento a dette attività; a tal fine il Dirigente o il Coordinatore di ICTLAB PA dovrà effettuare un'adeguata e documentata attività di supervisione dei suddetti soggetti terzi in ordine al rispetto dei protocolli previsti dal Modello di ICTLAB PA.

Al fine di fornire una visione delle specifiche criticità, di seguito vengono focalizzate, per ogni categoria di reati potenzialmente realizzabili all'interno della ICTLAB PA, le aree sensibili, i destinatari, i principi generali di comportamento ed i corrispondenti processi per la loro prevenzione.

4.3 Reati contro la Pubblica Amministrazione

Potenziali reati:

- Corruzione;
- Corruzione per un atto d'ufficio o contrario ai doveri d'ufficio;
- Corruzione in atti giudiziari;
- Istigazione alla corruzione;
- Malversazione a danno dello Stato o dell'UE;
- Indebita percezione di erogazioni in danno dello Stato o dell'UE;
- Truffa in danno dello Stato, di altro ente pubblico o dell'UE;
- Truffa aggravata per il conseguimento di erogazioni pubbliche;
- Frode informatica in danno dello Stato o di altro ente pubblico;
- Induzione indebita a dare o promettere utilità;
- Traffico di influenze illecite;
- Frode nelle pubbliche forniture;
- Peculato mediante profitto dell'errore altrui.

4.3.1 *Le aree sensibili*

L'art. 6, comma 2, lett. a) del D. Lgs. 231/2001 indica, tra gli elementi essenziali del modello di organizzazione, gestione e controllo, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal D. Lgs. 231/2001.

Tali reati possono essere commessi nella gestione dei rapporti con la Pubblica Amministrazione (intesa in senso lato e incluse, ove compatibili, le società a partecipazione pubblica) e nello svolgimento di attività che interagiscano con una pubblica funzione.

ICTLAB PA, allo stato, intrattiene diversi rapporti contrattuali con la Pubblica Amministrazione, sia offrendo servizi di consulenza, formazione e ricerca per le pp.aa., sia partecipando a gare pubbliche o procedure per la sottoscrizione di contratti pubblici.

Al fine dell'individuazione delle Attività Sensibili, si è posta l'attenzione sugli ambiti in cui ICTLAB PA nell'esercizio della propria attività, potrebbe, in astratto, incorrere nella commissione dei reati sopra elencati.

Così, in concreto, sono emerse le seguenti Attività Sensibili:

- contrattazione, negoziazione e partecipazione a gare con enti pubblici;
- acquisizione di incarichi diretti;
- rapporti istituzionali;
- verifiche e ispezioni da parte di autorità esterne;
- stipula di convenzioni;
- gestione dei flussi di cassa e solleciti di pagamento;
- richiesta e impiego di erogazione di fondi pubblici per la formazione;
- pagamento dei contributi;
- rapporti con altri enti pubblici, funzionari pubblici e soggetti, anche privati, esercenti funzioni di pubblico servizio in relazione alle attività di fornitura dei servizi;
- gestione dei contenziosi giudiziari e stragiudiziali;
- comunicazioni alla Pubblica Amministrazione di informazioni o dati aziendali;
- gestione acquisti e consulenze;
- assunzione e gestione del personale dipendente, anche con riferimento ai trattamenti previdenziali e assistenziali;
- gestione omaggi, liberalità e sponsorizzazioni;
- gestione note spese.

4.3.2 I destinatari

La presente sezione della Parte Speciale si riferisce a comportamenti posti in essere dall'Amministratore e dai Dirigenti della Società (cosiddetti soggetti apicali), nonché dai dipendenti della Società (cosiddetti soggetti interni sottoposti ad altrui direzione) coinvolti, a qualsiasi titolo, nelle attività sensibili rilevanti ai fini della presente Parte Speciale (qui di seguito tutti definiti i "Destinatari").

In forza di accordi e/o apposite clausole contrattuali e limitatamente allo svolgimento delle attività sensibili a cui essi eventualmente partecipano, possono essere destinatari della presente Parte Speciale, i seguenti soggetti esterni:

- collaboratori, consulenti ed, in genere, tutti i soggetti che svolgono attività di lavoro autonomo nella misura in cui operino nell'ambito delle aree di attività Sensibili per conto o nell'interesse della Società;
- lavoratori distaccati che operano nell'ambito delle aree di attività Sensibili per conto o nell'interesse della Società;
- fornitori e partner commerciali che operano in maniera rilevante e che operano nell'ambito delle aree di attività Sensibili per conto o nell'interesse della Società.

4.3.3 Principi generali di comportamento: processi e procedure aziendali

Processi aziendali in essere:

- **Processo "Commerciale" – Partecipazione a gare e acquisizione incarichi diretti. Il processo si articola nelle seguenti fasi:**
  - decisione sulla partecipazione alle gare;
  - configurazione RTI e negoziazione con i partner di quote e parti del servizio (eventuale);
  - individuazione del Responsabile dell'Offerta tecnica e Team stesura offerta tecnica;
  - supervisione del Responsabile dell'Offerta tecnica;
  - validazione Offerta tecnica;
  - validazione Offerta economica e budget;
- **Processo "Approvvigionamento di beni e servizi" – Stipula di Convenzioni;**
- **Processo "Erogazione del servizio e controllo" – Rapporto diretto con la Committenza Pubblica**, a sua volta articolato nelle fasi di seguito indicate:
  - predisposizione budget di progetto;
  - definizione gruppo di lavoro;
  - supervisione e controllo del gruppo di lavoro;
  - conduzione tecnica del team di progetto;
  - formazione delle risorse umane del team di progetto;
  - programmazione e controllo operativo delle attività di commessa e dei carichi di lavoro;
  - controllo di gestione di commessa e costi diretti;
  - monitoraggio avanzamenti produzione e rispetto dei tempi di delivery.
- **Processo "Gestione degli adempimenti, delle comunicazioni e dei rapporti (istituzionali e nel corso di visite ispettive) con la Pubblica Amministrazione e le Autorità di Vigilanza";**
- **Processo "Selezione, assunzione, gestione e sviluppo del personale dipendente e professionale";**
- **Processo "Gestione dei contenziosi giudiziari e stragiudiziali";**
- **Processo "Gestione dei flussi monetari e finanziari e solleciti di pagamento";**
- **Processo "Gestione dei finanziamenti pubblici";**
- **Processo "Gestione trasferte e rimborsi spese a dipendenti e professionisti";**
- **Processo "Gestione omaggi e spese di rappresentanza".**

Procedure aziendali in essere:

(*in relazione ai processi aziendali)*

- **PR01 Ufficio Gare:** (*Commerciale*) Monitoraggio Gare - Gestione SharePoint- Preparazione Documentazione Amministrativa Gare - Gestione Database CV - Gestione Documentazione - Gestione Amministrativa commesse – Chiusura e certificazione commesse
- **PR 03 Tendering e Gestione Progetti**: (*Commerciale - Approvvigionamento servizi):* monitoraggio sistematico opportunità, verifica requisiti minimi di partecipazione, decisione partecipazione a gara, predisposizione espressioni di interesse, offerta tecnica, predisposizione offerta economica, Individuazione del Responsabile Offerta e team di preparazione offerta e tipo di partecipazione (singola, RTI, subappalto, avvalimento, ecc.), Individuazione partner per RTI e accordi economici e organizzativi, etc; gestione tecnico ed amministrativa del progetto/commessa in tutti vari aspetti quali predisposizione del budget e gruppo di lavoro, conduzione tecnica del team di progetto, programmazione e controllo operativo delle attività di commessa e dei carichi di lavoro, controllo dei costi di commessa, monitoraggio avanzamenti produzione e rispetto dei tempi di delivery, interazione strategica con la Committenza, etc.;
- **PR 05 Soddisfazione clienti:***(Erogazione del servizio e controllo)* per la rilevazione e verifica della soddisfazione dei clienti per i servizi professionali forniti.

Qui di seguito sono elencati i principi generali di comportamento, applicabili ai processi aziendali in essere, nonché relativi alle attività sensibili di ICTLAB PA nei rapporti con la Pubblica Amministrazione.

L'obiettivo è quello di indirizzare le attività sensibili poste in essere dai Destinatari al fine di prevenire il verificarsi dei reati contro la Pubblica Amministrazione di cui agli articoli 24 e 25 del Decreto.

Preliminarmente, è il caso di ribadire espressamente i doveri generali di condotta nei rapporti con la P.A per tutti gli esponenti aziendali, e precisamente, gli obblighi di:

- stretta osservanza di tutte le leggi e regolamenti che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano contatti e rapporti con la Pubblica Amministrazione o incaricati di una pubblica funzione o di un pubblico servizio;
- instaurazione e mantenimento di qualsiasi rapporto con la Pubblica Amministrazione sulla base di criteri di massima correttezza e trasparenza, con osservanza dei principi del Codice Etico della Società, nonché delle disposizioni contenute nella Parte Generale e nella Parte Speciale del presente Modello.

Nell'espletamento delle attività considerate a rischio, i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- astenersi dal tenere comportamenti tali da integrare le fattispecie di reato previste in questa parte speciale del Modello;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Inoltre, è necessario che venga osservato quanto segue:

- ICTLAB PA non inizierà o proseguirà nessun rapporto con esponenti aziendali, collaboratori esterni o partner che non intendano allinearsi al principio della stretta osservanza delle leggi;
- i rapporti nei confronti della Pubblica Amministrazione per le aree di attività a rischio ed i rapporti instaurati con i terzidevono essere gestiti in modo unitario, procedendo alla nomina di responsabili per le aree a rischio in ciascuna Area (ove non si sia già provveduto);
- i rapporti con Enti Pubblici, Pubbliche Amministrazioni, Pubblici Ufficiali o Incaricati di Pubblici Servizi devono essere improntati alla massima trasparenza, correttezza ed imparzialità;
- le dichiarazioni rese alle Istituzioni pubbliche e alla Pubblica Amministrazione devono contenere solo elementi assolutamente veritieri, devono essere complete e basate su validi documenti al fine di garantirne la corretta valutazione da parte dell'Istituzione o della Pubblica Amministrazione interessata;
- deve essere conservato un adeguato supporto documentale di ciascuna operazione, che consenta il controllo delle caratteristiche dell'operazione medesima, del relativo processo decisionale, delle autorizzazioni rilasciate per la stessa e delle verifiche su di essa effettuate;
- nell'ambito dei rapporti con la Pubblica Amministrazione, eventuali accordi di associazione temporanee di imprese, joint venture, finanza di progetto, compartecipazione societaria o coinvestimento con partner contrattuali sia italiani che stranieri devono essere definiti per iscritto, evidenziando tutte le condizioni dell'accordo stesso, con particolare riferimento alle condizioni

economiche concordate per la partecipazione congiunta alla procedura, progetto, associazione o società di scopo e devono essere verificabili in ogni momento dall'OdV;

- la selezione dei collaboratori esterni, fornitori, partner commerciali e consulenti deve essere ispirata a principi di obiettività, trasparenza, competenza, economicità e correttezza; a tal fine, l'attività di selezione del personale deve essere effettuata sulla base di criteri oggettivi quali la qualità, il prezzo e la capacità di fornire e garantire beni o servizi di livello adeguato. Non è ammesso alcun tipo di pressione indebita da parte di pubblici funzionari o esercenti un pubblico servizio, finalizzata a favorire un soggetto a discapito di un altro;
- gli incarichi conferiti ai collaboratori esterni devono essere redatti per iscritto, con l'indicazione del compenso pattuito, e comunicati all'HBU qualora prevedano condizioni diverse da quelle normalmente applicate agli altri collaboratori ai quali siano affidati analoghi incarichi;
- ogni dichiarazione di impegno o manifestazione della volontà sociale deve essere effettuata dai soggetti agenti per conto di ICTLAB PA nei limiti delle attribuzioni e dei poteri conferiti.

Nei rapporti con Pubblici Ufficiali o Incaricati di pubblico servizio o con dipendenti, in genere, della P.A. o di altre Istituzioni pubbliche, italiane o straniere, è fatto divieto agli esponenti aziendali di:

- effettuare elargizioni in denaro di qualsiasi entità nonché promettere o offrire loro (o ai loro parenti ed affini entro il quarto grado) denaro, doni o omaggi o altre utilità suscettibili di valutazione economica;
- accettare omaggi e regali o altre utilità suscettibili di valutazione economica, ad eccezione di regali d'uso di modico valore, che possano essere interpretati come azioni arrecanti un vantaggio lecito e trasparente fuori da quanto concesso e descritto nel Decreto, e comunque tali da non compromettere l'integrità e la reputazione di ICTLAB PA;
- chiedere a terzi di proporre la corresponsione o la dazione di denaro o altra utilità a un Pubblico funzionario o incaricato di pubblico servizio, che possano essere interpretati come azioni arrecanti un vantaggio lecito e trasparente fuori da quanto concesso e descritto nel Decreto;
- accordare o promettere altri vantaggi di qualsiasi natura, anche non immediatamente suscettibile di valutazione economica (promesse di assunzione, opportunità commerciali, etc.) in favore di rappresentanti della Pubblica Amministrazione, pubblici funzionari o incaricati di pubblico servizio (o ai loro parenti ed affini entro il quarto grado), che possano essere interpretati come azioni arrecanti un vantaggio lecito e trasparente fuori da quanto concesso e descritto nel Decreto, e comunque tali da non compromettere l'integrità e la reputazione di ICTLAB PA;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;
- effettuare prestazioni in favore dei Partner aziendali che abbiano relazioni con soggetti della Pubblica Amministrazione, pubblici funzionari o incaricati di pubblico servizio, in nome e per conto di ICTLAB PA, che non trovino adeguata giustificazione nel contesto del rapporto di business costituito con i Partner stessi;
- riconoscere compensi in favore dei Partner e dei collaboratori esterni che non trovino adeguata giustificazione in relazione sia al tipo e al contenuto di incarico da svolgere, sia in merito all'ammontare del compenso in relazione alle prassi di mercato accettate;
- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o esteri, al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o esteri, al fine di creare un vantaggio economico o competitivo per sé o per altri per l'aggiudicazione di contratti;
- destinare o utilizzare somme ricevute da organismi pubblici nazionali o esteri a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati o con modalità diverse da quelle previste;
- porre in essere artifici o raggiri, tali da indurre in errore o da arrecare un danno allo Stato (oppure ad altro Ente Pubblico o all'Unione Europea o ad organismi di diritto pubblico nazionale o internazionale) per realizzare un ingiusto profitto;
- accedere in maniera non autorizzata ai sistemi informativi utilizzati dalla Pubblica Amministrazione o altre Istituzioni Pubbliche, alterarne in qualsiasi modo il funzionamento o intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi per ottenere o modificare indebitamente informazioni a vantaggio della Società o di terzi;

- intraprendere (direttamente o indirettamente) azioni illecite al fine di favorire o danneggiare ingiustamente una delle parti in causa nel corso di processi civili, penali, amministrativi o tributari o di procedimenti arbitrali di qualsiasi natura.

4.4 Reati societari e di *market abuse*

Potenziali reati:

- False comunicazioni sociali;
- False comunicazioni sociali in danno della società, dei soci o dei creditori;
- Falsità nelle relazioni o nelle comunicazioni delle società di revisione;
- Impedito controllo;
- Indebita restituzione dei conferimenti;
- Illegale ripartizione degli utili o delle riserve;
- Illecite operazioni sulle azioni o quote sociali o della società controllante;
- Operazioni in pregiudizio dei creditori;
- Omessa comunicazione del conflitto di interesse;
- Formazione fittizia del capitale;
- Indebita ripartizione dei beni sociali da parte dei liquidatori;
- Corruzione tra privati;
- Illecita influenza sull'Assemblea;
- Aggiotaggio;
- Ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza.

4.4.1 *Le aree sensibili*

Sono state individuate, per ciascuno dei reati sopra indicati, le attività considerate sensibili, ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati all'esame.

Come già chiarito in precedenza, la punibilità della Società è, viceversa, esclusa, qualora il soggetto attivo del reato abbia agito per il proprio ed esclusivo interesse.

Infine, per quanto attiene l'individuazione delle funzioni aziendali coinvolte, occorre tener conto che alcuni reati societari rientrano nell'ambito dei reati c.d. "propri", rispetto ai quali la commissione è ipotizzabile unicamente ad opera di coloro che sono titolari della qualifica soggettiva indicata dal legislatore (i.e. gli amministratori, i sindaci, ecc.).

Tale circostanza non esclude, tuttavia, la possibilità che anche altre funzioni aziendali siano coinvolte, a titolo di concorso ex art. 110 c.p., nella commissione del reato.

Con riferimento ai reati societari richiamati dall'art. 25-ter del D. Lgs. 231/2001, le attività sensibili individuate sono le seguenti:

- Tenuta della contabilità, redazione del bilancio, delle comunicazioni sociali in genere, nonché relativi adempimenti di oneri informativi obbligatori per legge;
- Conservazione e comunicazione di dati e informazioni soggette a controllo da parte di soci, sindaci e società di revisione;
- Rapporti con i soci e predisposizione di comunicazioni dirette ai soci in generale riguardo alla situazione economica, patrimoniale e finanziaria della Società (bilancio d'esercizio, bilancio consolidato, relazione trimestrale e semestrale, etc);
- Predisposizione e divulgazione verso l'esterno di dati o notizie relativi alla Società stessa;
- Acquisizioni incarichi diretti con clientela privata
- Gestione rapporti con Enti certificatori
- Gestione rapporti infragruppo.

Inoltre, con riferimento alla fattispecie di reato della corruzione tra privati, le attività sensibili individuate sono le seguenti:

- gestione dei flussi di cassa e solleciti di pagamento;

- pagamento dei contributi;
- gestione acquisti e consulenze;
- assunzione e gestione del personale dipendente, anche con riferimento ai trattamenti previdenziali e assistenziali;
- gestione omaggi, liberalità e sponsorizzazioni;
- gestione note spese.

4.4.2 I destinatari

La presente sezione della Parte Speciale si riferisce a comportamenti posti in essere dall'Amministratore e dai Dirigenti della Società (cosiddetti soggetti apicali), nonché ai dipendenti della Società (cosiddetti soggetti interni sottoposti ad altrui direzione) coinvolti, a qualsiasi titolo, nelle attività sensibili rilevanti ai fini della presente Parte Speciale (qui di seguito tutti definiti i "Destinatari").

In forza di accordi o di apposite clausole contrattuali e limitatamente allo svolgimento delle attività sensibili a cui essi eventualmente partecipano, possono essere destinatari della presente Parte Speciale, i seguenti soggetti esterni:

- collaboratori, consulenti, revisori ed, in genere, tutti i soggetti che svolgono attività di lavoro autonomo nella misura in cui operino nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società;
- lavoratori distaccati che operano nell'ambito delle aree di attività Sensibili per conto o nell'interesse della Società;
- fornitori e partner commerciali che operano in maniera rilevante e che operano nell'ambito delle aree di attività Sensibili per conto o nell'interesse della Società.

4.4.3 Principi generali di comportamento e processi/procedure aziendali

Processi aziendali in essere:

- **Processo "Gestione Amministrativa e Finanziaria" – Predisposizione del bilancio**:
  - Comunicazioni periodiche dirette ai soci in relazione alla situazione economica patrimoniale e finanziaria della società;
  - Redazione progetto di bilancio da parte dell'Organo Amministrativo (Amministratore Unico);
  - Presentazione del progetto bilancio agli organi preposti al controllo, se esistenti;
  - Deposito progetto di bilancio presso sede sociale;
  - Approvazione del bilancio da parte dell'Assemblea dei Soci;
  - Deposito del bilancio presso Registro delle Imprese.

Qui di seguito sono elencati i principi generali di comportamento, applicabili ai processi aziendali in essere, nonché relativi alle aree a rischio, al fine di prevenire ed impedire il verificarsi dei Reati Societari.

In particolare, nell'espletamento delle attività considerate a rischio, i Destinatari dovranno attenersi ai seguenti principi generali di condotta:

- astenersi dal tenere comportamenti tali da integrare le fattispecie di reato previste in questa parte speciale del Modello;
- astenersi dal tenere comportamenti che, sebbene risultino tali da non costituire, di per sé, fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- tenere un comportamento corretto e trasparente, assicurando un pieno rispetto delle norme di legge e regolamentari, nonché delle procedure aziendali interne, nello svolgimento di tutte le attività finalizzate alla formazione del bilancio, delle situazioni contabili periodiche e delle altre comunicazioni sociali, al fine di fornire ai soci ed al pubblico in generale una informazione veritiera e appropriata sulla situazione economica, patrimoniale e finanziaria della Società;
- astenersi dal porre in essere operazioni simulate o altrimenti fraudolente, nonché dal diffondere notizie false o non corrette, idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari;

- astenersi dal compimento di atti che possano rilevare al fine di una configurazione di reati di abuso di mercato (in quest'ultimo caso, ovviamente, nei limiti in cui tale evento potrebbe risultare ipotizzabile in concorso con altri soggetti, considerato che la Società ICTLAB PA allo stato non rientra tra i soggetti destinatari delle previsioni di cui agli artt. 181 e ss. TUF);
- 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 e delle altre comunicazioni sociali, al fine di fornire al pubblico un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria di ICTLAB PA;
- osservare le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere.

Al fine di evitare la commissione dei reati descritti nella presente Parte Speciale del Modello, è fatto divieto agli esponenti aziendali e agli altri Destinatari di:

- tenere comportamenti tali da integrare le fattispecie di reato previste in questa parte speciale del Modello;
- tenere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- predisporre o comunicare dati falsi, lacunosi o comunque suscettibili di fornire una descrizione non veritiera, non corretta della realtà, riguardo alla situazione economica, patrimoniale e finanziaria della Società, o comunque contrastante con i criteri generali di redazione dei documenti interessati;
- omettere di comunicare dati ed informazioni richiesti dalla normativa e dalle procedure in vigore riguardo alla situazione economica, patrimoniale e finanziaria della Società;
- alterare o, comunque, riportare in modo non veritiero o non corretto i dati e le informazioni destinati alla stesura di prospetti informativi, ove effettivamente richiesti;
- ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possono per legge essere distribuite;
- effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
- procedere in ogni modo a formazione o aumento fittizi del capitale sociale;
- ripartire i beni sociali tra i soci – in fase di liquidazione – prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie per soddisfarli;
- tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di alteri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte degli amministratori o della società di revisione;
- porre in essere, in occasione di assemblee, atti simulati o fraudolenti finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- concedere denaro, altre utilità quali omaggi o promesse d'assunzione, in favore di parenti e affini e/o soggetti segnalati da amministratori, direttori generali, dirigente preposto alla redazione dei documenti contabili societari e sottoposti alla vigilanza di questi ultimi responsabili di curare i rapporti commerciali presso i clienti i fornitori e i partner commerciali, al sol fine di influenzarne l'indipendenza di giudizio;
- promettere o concedere denaro o altre utilità ad amministratori, dirigente preposto alla redazione dei documenti contabili societari e direttori di società terze, al fine di indurli a praticare sconti o ad eseguire altre prestazioni a beneficio della Società.

Nei rapporti con partner contrattuali o terzi privati, è fatto divieto agli esponenti aziendali di:

- effettuare elargizioni in denaro di qualsiasi entità nonché promettere o offrire loro (o ai loro parenti ed affini entro il quarto grado) denaro, doni o omaggi o altre utilità suscettibili di valutazione economica, ove tali promesse od offerte di denaro, omaggi, doni siano volte a perseguire finalità corruttive o comunque illecite;
- accettare omaggi e regali o altre utilità suscettibili di valutazione economica, ove questi siano volti a perseguire finalità corruttive o comunque illecite;
- chiedere a terzi di proporre la corresponsione o la dazione di denaro o altra utilità ove questi siano volti a perseguire finalità corruttive o comunque illecite;

- accordare o promettere altri vantaggi di qualsiasi natura (promesse di assunzione, o opportunità commerciali, etc.) che possano essere interpretati come azioni arrecanti un vantaggio lecito e trasparente fuori da quanto concesso e descritto nel Decreto, e comunque tali da non compromettere l'integrità e la reputazione di ICTLAB PA;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;
- effettuare prestazioni in favore dei Partner aziendali che non trovino adeguata giustificazione nel contesto del rapporto di business costituito con i Partner stessi;
- riconoscere compensi in favore dei Partner esterni che non trovino adeguata giustificazione in relazione sia al tipo di incarico da svolgere, sia in merito all'ammontare del compenso in relazione alle prassi di mercato accettate;
- intraprendere (direttamente o indirettamente) azioni illecite che possano, nel corso di processi civili, penali o amministrativi, favorire o danneggiare una delle parti in causa e che possano essere interpretate come azioni arrecanti un vantaggio lecito e trasparente fuori da quanto concesso e descritto nel Decreto.

4.5 Reati di omicidio colposo o lesioni gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro

Potenziali reati:

- Lesioni colpose gravi;
- Lesioni colpose gravissime;
- Omicidio colposo.

4.5.1 *Le aree sensibili*

Con riferimento ai rischi connessi all'art. 25.*septies*, le aree ritenute più specificatamente a rischio risultano essere le seguenti:

- rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- attività di sorveglianza sanitaria;
- attività di informazione e formazione dei lavoratori;
- attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- acquisizione di documentazioni e certificazioni obbligatorie di legge;
- periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate;
- adozione ed implementazione delle misure previste dalle norme antinfortunistiche in materia di salute e sicurezza nei luoghi di lavoro;
- nomina del Responsabile Sicurezza Prevenzione e Protezione e del Medico competente;
- effettuazione della valutazione dei rischi;
- elaborazione del documento di valutazione dei rischi e del suo periodico aggiornamento;
- designazione del Responsabile Servizio Prevenzione e Protezione (RSPP);
- predisposizione degli impianti, apparecchi e / o strumenti di segnalazione destinati alla prevenzione di disastri e / o infortuni sul lavoro;
- collocazione degli apparecchi o degli altri strumenti destinati alla estinzione di un incendio ovvero al salvataggio o soccorso in caso di disastro o infortunio sul lavoro presso le sedi ed eventuali unità locali di ICTLAB PA.

4.5.2 I destinatari

I soggetti tradizionalmente destinatari degli obblighi di sicurezza, di igiene e di salute del lavoro sono il datore di lavoro (da individuarsi, nel caso di ICTLAB PA, nell'Amministratore Unico, salvo delega delle funzioni antinfortunistiche ad un soggetto esterno munito dei requisiti richiesti dalla legge e dalla giurisprudenza), i dirigenti e i preposti. A tali soggetti si aggiungono quelli istituzionalmente tenuti all'osservanza delle norme di sicurezza, di igiene e di salute del lavoro da disposizioni normative che regolino il caso concreto.

4.5.3 Principi generali di comportamento e processi/procedure aziendali

Processi aziendali in essere:

- **Processo "Gestione Risorse" – Ambiente di lavoro**:
  - Sicurezza luoghi di lavoro;
  - Apertura e chiusura sedi o unità locali;
  - Gestione contratti di affitto e locazione;
  - Rapporti con proprietà o amministrazione.

Procedure aziendali in essere:

- **PR 04 – Sicurezza sedi:**

ICTLAB PA si è dotata di una struttura organizzativa per la garanzia della sicurezza in tutte le sedi, che risponde pienamente a quanto previsto dalla normativa di riferimento (D.lgs 81/2008 e s.m.i.).

Tutte le figure previste sono state formalmente nominate, incaricate e formate come previsto dalla legge e operano presso le sedi di competenza per garantire la tutela della salute di tutti i lavoratori e le persone che accedono nelle sedi di ICTLAB PA.

Tra gli obblighi di sicurezza, di igiene e di salute del lavoro cui l'ente deve adempiere si ricordano – per la loro ampiezza e grande significatività – quelli che seguono:

- effettuare un'analisi diretta a valutare il grado di generale conoscenza ed ottemperanza dei maggiori adempimenti alle normative antinfortunistiche ed a tutela dell'igiene e della salute nel lavoro da parte delle Società;
- assicurare un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi:
  - al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici, biologici e cancerogeni;
  - alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
  - alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
  - alle attività di sorveglianza sanitaria;
  - alle attività di informazione e formazione dei lavoratori;
  - alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
  - alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
  - alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.
- adeguare il proprio Modello di organizzazione, gestione e controllo, stabilendo i seguenti **principi di comportamento specifici** ed introducendo i seguenti elementi organizzativi:

a) principi in materia di struttura organizzativa della Società:

- le deleghe in materia di sicurezza del lavoro e sulla tutela dell'igiene e salute sul lavoro devono essere redatte per iscritto determinando in modo chiaro, specifico ed univoco le funzioni assegnate, assicurando la coerenza del sistema delle deleghe, dei poteri di firma e di spesa con le responsabilità assegnate;

- devono essere correttamente formalizzate le responsabilità, i compiti organizzativi e operativi di dirigenti e preposti, e devono essere chiaramente descritte le mansioni di ciascun dipendente della Società in materia di sicurezza e dell'igiene e salute sul lavoro;
- devono essere correttamente nominati i soggetti previsti dalla normativa in materia di igiene, salute e sicurezza dei luoghi di lavoro e devono essere conferite adeguate direttive e poteri necessari allo svolgimento dei ruoli assegnati;
- devono essere resi noti a tutti i livelli dell'organizzazione, le funzioni ed i compiti del Responsabile del Servizio di Prevenzione e Protezione (RSPP), degli eventuali Addetti al Servizio di Prevenzione e Protezione (ASPP), del Rappresentante dei Lavoratori per la Sicurezza (RLS), e degli addetti alla gestione delle emergenze, nonché i compiti e le responsabilità del medico competente;
- i responsabili interni e gli eventuali consulenti esterni e i soggetti previsti in materia di igiene e sicurezza dei luoghi di lavoro (tra cui, l'RSPP, il medico competente, eventuale personale tecnico, etc.) devono essere scelti sulla base di requisiti di professionalità e competenza degli stessi, motivando adeguatamente le scelte effettuate;
- devono essere predisposti con prontezza e accuratezza i protocolli relativi alle situazioni di emergenza e devono essere adeguati i relativi regolamenti sullo Smart work, tenendo in considerazione le informative redatte dall'INAIL.

b) principi in materia di attività di formazione ed addestramento

- deve essere garantita adeguata conoscenza della normativa applicabile in materia infortunistica ai soggetti responsabili della sicurezza, all'RSPP ed agli addetti al sistema prevenzione e protezione, ed agli addetti alle squadre di pronto soccorso ed emergenza;
- deve essere adeguatamente programmata ed effettuata la formazione e informazione dei dipendenti e dei collaboratori della Società con riferimento alle materie antinfortunistiche in generale ed ai rischi cui sono sottoposti con riferimento alla specifica mansione da svolgere e nei limiti degli effettivi rischi connessi a tale mansione, ad eventuali rischi specifici (quali il rischio VDT etc.), ed alle misure di prevenzione e comportamenti da adottare;
- il personale deve essere costantemente formato ed informato in merito alle misure di prevenzione e protezione (ivi compresi i dispositivi di prevenzione individuale) adottati e deve essere pienamente consapevole degli obblighi ai quali è tenuto per la protezione dell'incolumità e della salute propria, dei colleghi e di terzi, in coerenza con le effettive mansioni alle quali i dipendenti sono rispettivamente addetti;
- il datore di lavoro provvede a nominare e formare gli addetti alla lotta antincendio e gestione delle emergenze, nonché al primo soccorso aziendale;

c) principi in materia di attività di gestione operativa in materia di sicurezza

- deve essere adeguatamente effettuata, ed aggiornata su base continuativa, la valutazione di tutti i rischi per la sicurezza e la salute dei lavoratori nei luoghi di lavoro, in applicazione di quanto previsto dal Testo Unico, tenendo adeguatamente conto di ogni mutamento intervenuto nei processi produttivi nell'organizzazione del lavoro e dei luoghi di lavoro;
- deve essere data adeguata attuazione ed aggiornamento delle misure di prevenzione e protezione dai rischi come identificati nell'attività di valutazione rischi;
- deve essere predisposta adeguata segnaletica nei luoghi di lavoro e devono essere garantiti adeguati mezzi di protezione individuale ai dipendenti;
- devono essere individuati eventuali rischi specifici (es. VDT, etc.) e devono essere attuate le misure di protezione relative;
- devono essere adeguatamente organizzate le squadre di soccorso ed emergenza ed adeguatamente predisposte e formalizzate le procedure e i manuali di gestione delle emergenze ed effettuate le prove periodiche ivi previste;
- l'attività di manutenzione dei luoghi di lavoro, di controllo periodico, manutenzione e verifica degli impianti e delle attrezzature di lavoro (ivi comprese le autovetture aziendali) deve essere organizzata in maniera adeguata e, comunque, idonea a garantire la prevenzione di danni, infortuni derivanti da inadeguatezze, scorretto uso od altre problematiche tecniche e la sicurezza, in linea con le prescrizioni di legge;

- deve essere garantita la consultazione dei lavoratori nelle materie attinenti alla sicurezza così come prevista dalla normativa vigente;
- deve essere garantito idoneo coordinamento delle diverse imprese appaltatrici o dei lavoratori autonomi che operano presso la Società, anche attraverso riunioni periodiche dell'RSPP con i responsabili delle imprese e i lavoratori autonomi;

d) principi in materia di attività di monitoraggio, ispezione e controllo

- deve essere predisposta e mantenuta adeguata documentazione delle attività effettuate in ambito della gestione della sicurezza quali quelle sopra elencate;
- deve essere effettuata adeguata registrazione, monitoraggio ed analisi degli infortuni sul lavoro e delle malattie professionali e delle relative cause anche al fine di ridurne l'incidenza;
- devono essere programmate, effettuate, documentate e registrate le attività di verifica ed ispezione tecnica dei luoghi e delle attività di lavoro su base continuativa da parte dell'RSPP, del Medico competente, e di eventuali esperti terzi, e devono essere tempestivamente sanate le eventuali difformità riscontrate;
- devono essere programmate, effettuate, documentate e registrate attività di verifica dell'effettiva attuazione delle procedure previste in materia di sicurezza e del rispetto delle norme di legge e regolamentari in materia;

e) principi di comportamento per tutti i dipendenti e lavoratori presso la Società

- devono essere osservate le disposizioni di legge, la normativa interna e le istruzioni impartite in materia di sicurezza anche con specifico riferimento alla mansione ricoperta;
- devono essere utilizzati correttamente e secondo le istruzioni impartite e le procedure esistenti, apparecchiature, utensili, mezzi di trasporto e le altre attrezzature di lavoro;
- deve essere segnalato tempestivamente ai responsabili o agli addetti alle emergenze l'insorgere di eventuali situazioni di pericolo potenziale o reale adoperandosi, nell'ambito delle proprie competenze e responsabilità, al fine di attenuare dette situazioni di pericolo.

4.6 Delitti informatici e trattamento illecito di dati

Potenziali reati:

- Falsità in documenti informatici;
- Accesso abusivo ad un sistema informatico o telematico;
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici;
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche;
- Danneggiamento di informazioni, dati e programmi informatici;
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità;
- Danneggiamento di sistemi informatici o telematici;
- Danneggiamento di sistemi informatici o telematici di pubblica utilità.

4.6.1 Le aree sensibili

Le attività che possono condurre alla commissione dei reati sopra descritti sono proprie di ogni ambito e funzione aziendale che utilizza le tecnologie dell'informazione.

In particolare, la Società valuta come "sensibili" le seguenti attività che essa pone in essere per mezzo dei Destinatari ed anche, eventualmente, in collaborazione con soggetti esterni:

- gestione dei servizi IT;
- trattamento di banche dati e/o dati informatici;
- gestione comunicazioni interne tramite email;
- gestione sito internet aziendale;
- gestione delle caselle di posta elettronica certificata;
- gestione del sistema informativo per la gestione delle attività e dei documenti: SharePoint, che rappresenta l'area di lavoro in cui è presente tutta la documentazione afferente i progetti della Società.

4.6.2 I destinatari

Il presente Modello si applica a tutte le funzioni coinvolte nella gestione e nell'utilizzo dei sistemi e dei dati informatici, ed in particolare si riferisce ai comportamenti posti in essere dall'Amministratore, dai Dirigenti, dai Responsabili e Dipendenti di ICTLAB PA, nonché da partner e collaboratori esterni con essa operanti sulla base di un rapporto contrattuale.

In particolare, si applica a:

- tutte le funzioni coinvolte nella gestione e nell'utilizzo dei sistemi informativi che utilizzano software della Pubblica Amministrazione (ad es. fatturazione elettronica nei confronti della P.A., invio telematico di domande di partecipazione alle gare, etc.);
- tutte le funzioni deputate alla progettazione, alla realizzazione o gestione di strumenti informatici, tecnologici o di telecomunicazioni;
- tutte le funzioni che hanno la responsabilità di realizzare interventi di tipo organizzativo, normativo e tecnologico per garantire la protezione del patrimonio informativo nelle attività connesse con il proprio mandato e nelle relazioni con i terzi che accedono al patrimonio informatico;
- tutte le figure professionali coinvolte nei processi aziendali e ivi operanti a qualsiasi titolo, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale, che utilizzano i sistemi informativi e trattano i dati del patrimonio informativo.

4.6.3 Principi generali di comportamento e processi/procedure aziendali

Processi aziendali in essere:

- **Processo "Gestione Risorse" – Infrastruttura:**
  - Sviluppo sistemi informativi;
  - Protezione dei dati;
  - Infrastrutture: banda larga, linee telefoniche, etc.
- **Processo "Gestione Comunicazione Interna ed Esterna" – Editoria di Gruppo**:
  - Gestione sito internet;
  - Eventi.

Le funzioni a qualsiasi titolo coinvolte nelle attività di gestione e utilizzo di sistemi informatici e del patrimonio informativo della Società sono tenute ad osservare le disposizioni di legge esistenti in materia, la normativa interna nonché le previsioni del presente Modello al fine di impedire il verificarsi di reati informatici.

Inoltre, i Destinatari devono:

- osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali in materia di utilizzo e gestione degli strumenti informatici accedere esclusivamente ai siti informatici;
- consentire l'accesso e l'utilizzo degli strumenti informatici ad essi affidati ai soli soggetti autorizzati;
- evitare di introdurre o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso, nonché applicazioni o software che non siano stati preventivamente approvati dal Responsabile di

Area o la cui provenienza sia dubbia o il cui utilizzo non sia consentito sulla base di idoneo titolo di acquisto, locazione finanziaria, licenza o altro da parte della Società;

- evitare di trasferire all'esterno della Società o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà della Società, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, in caso di dubbio, previa autorizzazione del proprio Responsabile;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla stessa o comunque dei quali la società sia in possesso di regolare licenza per l'utilizzo lecito;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società.

Al fine di evitare la commissione dei reati descritti nella presente Parte Speciale del Modello, è fatto divieto agli esponenti aziendali e agli altri Destinatari di:

- introdursi in sistemi informativi e banche dati altrui senza averne autorizzazione o licenza;
- intercettare ovvero interrompere comunicazioni telematiche;
- effettuare il download di programmi finalizzati ad attività di hackeraggio;
- modificare le impostazioni degli strumenti informatici a disposizione in assenza di autorizzazione da parte dei soggetti preposti;
- utilizzare gli strumenti informatici a disposizione della Società al di fuori delle prescritte autorizzazioni;
- installare software (es: spyware) o apparecchiature non autorizzate e potenzialmente in grado di consentire la commissione di "reati presupposto";
- diffondere all'esterno della Società codici di accesso ai sistemi informatici interni o di controparti;
- effettuare copie non specificamente autorizzate di dati e di software;
- utilizzare firme elettroniche di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione;
- utilizzare password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione;
- prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del Responsabile di Divisione;
- lasciare incustodito o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso e della connessa apparecchiatura informatica ad altre persone.

4.7 Reati ambientali

Potenziali reati:

- norme poste a tutela delle specie animali e vegetali protette e di habitat all'interno dei siti protetti;
- norme in materia di scarichi di acque reflue e gestione dei rifiuti;
- attività di gestione di rifiuti non autorizzata;
- omessa bonifica dei siti in conformità al progetto approvato dall'autorità competente;
- violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari;
- traffico illecito di rifiuti;
- attività organizzate per il traffico illecito di rifiuti;
- falsità ideologica del certificato di analisi dei rifiuti, anche utilizzato nell'ambito del SISTRI – Area Movimentazione, e falsità ideologica e materiale della scheda SISTRI – Area Movimentazione;
- superamento dei valori limite di emissione che determinano il superamento dei valori limite di qualità dell'aria;
- norme a tutela dell'ozono stratosferico;
- norme sul commercio internazionale delle specie animali e vegetali in via di estinzione;

- falsificazione o alterazione di certificati, licenze, notifiche di importazione, dichiarazioni, comunicazioni di informazioni;
- detenzione di esemplari vivi di mammiferi e rettili di specie selvatica ed esemplari vivi di mammiferi e rettili provenienti da riproduzioni in cattività che costituiscano pericolo per la salute e per l'incolumità pubblica;
- norme finalizzate alla prevenzione dell'inquinamento provocato dalle navi.

4.7.1 Le aree sensibili

Ai fini della individuazione di eventuali Attività Sensibili, si è posta l'attenzione sui settori in cui la Società, estrinsecando la propria attività, potrebbe, attraverso l'Amministratore, dipendenti, dirigenti, collaboratori, sindaci o partner contrattuali, incorrere nella commissione dei reati sopra elencati.

A seguito dell'analisi, si è distinto tra reati ambientali la cui commissione nell'interesse o a vantaggio della Società è in concreto esclusa dalla effettiva individuazione del raggio di azione della operatività aziendale, dati contenuto e caratteristiche delle attività aziendali, ed altri reati ambientali che, al contrario, potrebbero, in via di ipotesi, essere commessi ad opera dei Destinatari del Modello. In relazione a questi ultimi, si è valutato il livello di rischio, avuto riguardo alle attività rientranti nell'oggetto sociale della Società e alla concreta prassi operativa della stessa.

Ai fini della presente Parte Speciale, le aree di attività nelle quali possono essere commessi i reati sopra descritti di cui all'art. 25-undecies del Decreto, ai fini della presente Parte Speciale, risultano essere le seguenti:

- Prevenzione dell'inquinamento;
- Uso razionale delle risorse;
- Utilizzazione di risorse idriche e scarico acque reflue;
- Gestione ottimale dei rifiuti;
- Emissione gas in atmosfera;
- Acquisti "verdi";
- Gestione degli impatti diretti.

4.7.2 I destinatari

La presente sezione della Parte Speciale si riferisce a comportamenti posti in essere dall'Amministratore e dai Dirigenti della Società (cosiddetti soggetti apicali), nonché ai dipendenti della Società (cosiddetti soggetti interni sottoposti ad altrui direzione) coinvolti, a qualsiasi titolo, nelle attività sensibili rilevanti ai fini della presente Parte Speciale (qui di seguito tutti definiti i "Destinatari").

In forza di accordi e/o apposite clausole contrattuali e limitatamente allo svolgimento delle attività sensibili a cui essi eventualmente partecipano, possono essere destinatari della presente Parte Speciale, i seguenti soggetti esterni:

- collaboratori, consulenti ed, in genere, tutti i soggetti che svolgono attività di lavoro autonomo nella misura in cui operino nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società;
- lavoratori distaccati che operano nell'ambito delle aree di attività Sensibili per conto o nell'interesse della Società;
- fornitori e partner commerciali che operano in maniera rilevante e che operano nell'ambito delle aree di attività Sensibili per conto o nell'interesse della Società.

4.8 Delitti di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, come previsto *ex* art. 377-*bis* codice penale

La fattispecie di induzione a non rendere dichiarazioni mendaci all'autorità giudiziaria di cui all'art. 377-*bis* concerne i delitti contro l'attività giudiziaria. La norma tutela il corretto svolgimento dell'attività processuale contro le interferenze indebite e, specificamente, la spontaneità del comportamento processuale. Il reato si realizza mediante l'induzione con violenza (fisica e psichica) o minaccia o con offerta o promessa di denaro o di altra utilità, a non rendere dichiarazioni o a renderle mendaci.

4.8.1. Le aree sensibili

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsti dal decreto, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della Società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

L'analisi dei processi della Società ha consentito di individuare le seguenti attività "sensibili", nel cui ambito potrebbe astrattamente realizzarsi la fattispecie di reato in oggetto:

1) Gestione dei rapporti con l'Autorità Giudiziaria;
2) Gestione acquisti e consulenze;
3) Gestione di eventuali contenziosi giudiziali e stragiudiziali.

4.8.2. I destinatari

Il destinatario della condotta del reo è il soggetto chiamato, in un procedimento penale, a rendere dichiarazioni utilizzabili davanti all'autorità giudiziaria, con facoltà di non rispondere.

Quanto alle modalità tipiche della realizzazione della condotta, l'induzione rilevante ai fine della consumazione del reato, si realizza mediante l'azione con la quale un soggetto esplica un'influenza sulla psiche di un altro soggetto, determinandolo a tenere un certo comportamento, esplicata attraverso i mezzi tassativamente indicati dalla norma, ovvero minaccia, violenza o promessa di denaro o altra utilità.

È richiesto, inoltre, per la realizzazione degli elementi costitutivi della fattispecie, che:

- la persona indotta non abbia reso dichiarazioni o le abbia rese mendaci;
- l'agente si rappresenti che la persona da lui indotta - con le modalità indicate dalla norma - a non rendere dichiarazioni o a renderle non veritiere, aveva la facoltà di non rispondere.

Il reato potrebbe, dunque, dirsi integrato qualora un soggetto riferibile all'ente ponga in essere, con violenza, minaccia o promessa di denaro o altra utilità, misure atte ad indurre le persone che sono tenute a rendere dichiarazioni (es. testimonianze) all'autorità giudiziaria utilizzabili in un procedimento penale a rendere dichiarazioni non veritiere con riferimento, ad esempio, ad attività illecite degli amministratori/o altri dipendenti della società.

4.9 Reati tributari

Potenziali reati:

- delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 1, d.lgs. 74/2000;
- delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'art. 2, comma 2-*bis*,d.lgs. 74/2000;
- delitto di dichiarazione fraudolenta mediante altri artifici previsto dall'art. 3, d.lgs. 74/2000;
- delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, d.lgs. 74/2000, comma 1;
- delitto di emissione di fatture o altri documenti per operazioni inesistenti previsto dall'art. 8, comma 2-*bis*, d.lgs. 74/2000;
- delitto di occultamento o distruzione di documenti contabili previsto dall'art. 10, d.lgs. 74/2000;
- delitto di sottrazione fraudolenta al pagamento di imposte previsto dall'art. 11, d.lgs. 74/2000.

4.9.1. Le aree sensibili

L'analisi dei processi aziendali ha consentito di individuare le attività sensibili nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-quinquiesdecies del d.lgs. 231/01, come di seguito dettagliate:

- Gestione degli adempimenti fiscali;
- Acquisti e consulenze e processo commerciale;
- Vendite e ciclo attivo.

4.9.2. I destinatari

La presente sezione della Parte Speciale si riferisce a comportamenti posti in essere dall'Amministratore e dai Dirigenti della Società (cosiddetti soggetti apicali), nonché ai dipendenti della Società (cosiddetti soggetti interni sottoposti ad altrui direzione) coinvolti, a qualsiasi titolo, nelle attività sensibili rilevanti ai fini della presente Parte Speciale (qui di seguito tutti definiti i "Destinatari").

In forza di accordi e/o apposite clausole contrattuali e limitatamente allo svolgimento delle attività sensibili a cui essi eventualmente partecipano, possono essere destinatari della presente Parte Speciale, i seguenti soggetti esterni:

- collaboratori, consulenti ed, in genere, tutti i soggetti che svolgono attività di lavoro autonomo nella misura in cui operino nell'ambito delle aree di attività sensibili per conto o nell'interesse della Società;
- lavoratori distaccati che operano nell'ambito delle aree di attività Sensibili per conto o nell'interesse della Società;
- fornitori e partner commerciali che operano in maniera rilevante e che operano nell'ambito delle aree di attività Sensibili per conto o nell'interesse della Società.

4.9.3. Principi generali di comportamento e processi aziendali

Tutti i Destinatari del presente Modello sono tenuti a rispettare le seguenti regole di comportamento:

- rispettare scrupolosamente le disposizioni della Società e tutte le procedure formalizzate occorrenti per assolvere correttamente agli obblighi tributari e contributivi della Società;
- verificare che i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative e gestionali assegnate;
- verificare che ogni operazione relativa all'attività sensibile debba essere adeguatamente registrata ed il processo di decisione, autorizzazione e svolgimento dell'attività deve essere verificabile ex post, anche tramite appositi supporti documentali dovendo essere tracciabili le eventuali cancellazioni o distruzioni di registrazioni effettuate;
- fermi restando i protocolli specifici nella gestione di acquisizione di beni e servizi, verificare che per i nuovi fornitori e soggetti con cui la Società si relaziona per la prima volta, siano stati effettuati opportuni controlli presso la Camera di Commercio e comunque di avere informative idonee a valutare l'affidabilità del soggetto che emette la fattura;
- osservare rigorosamente tutte le leggi e i regolamenti che disciplinano l'attività della Società, con particolare riferimento alle attività che comportano l'emissione di documenti contabili sia attivi, sia passivi;
- instaurare e mantenere qualsiasi rapporto con l'Agenzia delle Entrate sulla base di criteri di massima correttezza e trasparenza;
- assicurare da parte della funzione competente un calendario delle scadenze fiscali e contributive e dei relativi adempimenti, ovvero verificare che consulenti e collaboratori in outsourcing per provvedere alle incombenze della presente area condividano con le funzioni societarie competenti tale calendario delle scadenze;
- garantire forme di controllo costante e mirato degli adempimenti contabili e tributari, sotto la responsabilità del soggetto preposto al controllo contabile;
- acquisire e conservare per un periodo di tempo non inferiore a 5 anni specifica dichiarazione di collaboratori e consulenti esterni a titolo di sgravio di responsabilità per eventuali violazioni di disposizioni tributarie e contributive agli stessi imputabili a titolo di dolo o colpa grave; in tale contesto, la società assicura che il collaboratore o il consulente esterno dia dimostrazione di apposita responsabilità civile per i possibili danni arrecabili a terzi, di importo coerente con i potenziali danni che possano gravare su ICTLAB PA;
- garantire apposita check list di controllo da parte della funzione preposta.

Più in generale coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi all'espletamento delle suddette attività (pagamento di fatture, erogazione di contributi, finanziamenti ottenuti dallo Stato o da organismi comunitari, ecc.) devono porre particolare attenzione sull'attuazione degli adempimenti stessi.

È fatto espresso divieto ai Destinatari di:

- presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire vantaggi contabili o di bilancio;
- esibire documenti e dati incompleti o comunicare dati falsi e alterati alla Pubblica Amministrazione o al concessionario della riscossione oppure sottrarre o omettere l'esibizione di documenti veri;
- alterare il funzionamento di sistemi informativi e telematici o manipolare i dati in essi contenuti;
- porre in essere qualunque comportamento tale da integrare le fattispecie dei reati tributari previsti dall'art. 25 quinquesdecies del D.lgs. n. 231/01 (dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, dichiarazione fraudolente mediante uso di altri artifici, emissione di fatture o altri documenti per operazioni inesistenti, occultamento o distruzione di documenti contabili, sottrazione fraudolenta al pagamento di imposte) e comunque porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle previste, possano potenzialmente diventarle.