Modello di Organizzazione, Gestione e Controllo ex-D.Lgs. 231/2001

PARTI SPECIALI

Codice Documento	MOG 231_PS
Versione	Versione 2 Release 0
Data emissione	12 dicembre 2014
Redatto	Responsabile Internal Audit
Verificato	Organismo di Vigilanza
Approvato	Consiglio d'Amministrazione (verbale n. 80 del 22 dicembre 2014)

InnovaPuglia S.p.A.
Società assoggettata alla direzione e controllo della Regione Puglia
Strada Provinciale per Casamassima Km. 3 70010 - Valenzano Bari
CCIAA di Bari n. 513395 - P.Iva 06837080727
Capitale Sociale Euro 1.434.576,00 i.v. a socio unico

tel. +39 080.46.70.418
fax +39 080.45.51.868
info@innova.puglia.it
www.innova.puglia.it

Storia delle Revisioni

Ver.	Data	Contenuto sintetico
	10 / 05 / 2011	Prima emissione Parte Speciale A
vers 1 rel 0	26 / 09 / 2014	Aggiornamento Parte Speciale A Prima emissione Parti speciali B, C, D, E, F, G
vers 2 rel 0	12 / 12 / 2014	

INDICE

INTRODUZIONE

A partire dagli elementi descrittivi della Società riportati nel documento "Parte Generale", il presente documento definisce, nel merito, le componenti del sistema di controllo utili a prevenire la commissione dei reati previsti dal D.Lgs, 231/2001.

Le "Parti Speciali" si focalizzano sulle specifiche fattispecie di reato per le quali si rilevi un possibile livello di rischio rispetto alle attività esercitate da InnovaPuglia spa; nello specifico, tali fattispecie sono ad oggi identificate in :

Parte Speciale A: "Reati contro la Pubblica Amministrazione e i reati commessi nei rapporti con la Pubblica Amministrazione";

Parte Speciale B: "Reati Societari";

Parte Speciale C: "Reati di omicidio colposo e lesioni colpose gravi o gravissime commessi in violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro";

Parte Speciale D: "Reati per delitti informatici e trattamento illecito dei dati – cyber crimes "

Parte Speciale E: "Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria"

Parte Speciale F: "Delitti in materia di violazione del diritto di autore "

Parte Speciale G: **"**Reati Ambientali".

Non sono stati invece ravvisati significativi profili di rischio rispetto alla commissione di altri reati presupposto, in particolare :

- Reati transnazionali
- Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (art. 25-octies, D.Lgs. 231/01)
- Delitti contro la personalità individuale (art. 25-quinquies, D.Lgs. 231/01)
- Pratiche di mutilazione degli organi genitali femminili (art. 25-quater.1, D.Lgs. 231/01)
- Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (art. 25-quater, D.Lgs. 231/01)
- Delitti contro l'industria e il commercio (art. 25-bis.1., D.Lgs. 231/01)
- Reati di falso nummario (art. 25-bis, D.Lgs. 231/01)
- Delitti di criminalità organizzata (art. 24-ter, D.Lgs. 231/01)
- Impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25-duodecies)
- Reati di abusi di mercato (artt. 25 sexies D.Lgs. 231/01).

fermo restando, la previsione del rimando al Codice Etico e ad una condotta rispettosa delle Leggi e Regolamenti in materia.

E', comunque, demandato al Consiglio di Amministrazione il compito di integrare il presente Modello con ulteriori Parti Speciali relative a ulteriori tipologie di reati o di Illeciti ogni qualvolta, sulla base delle periodiche verifiche effettuate, risulti opportuno procedere in tale direzione.

Ciascuna Parte Speciale è articolata secondo la

- descrizione schematica delle **fattispecie di reato** previste dalla normativa (cap. 2) ([1]);
- identificazione delle **attività sensibili**, ovvero di quelle attività aziendali che sono maggiormente esposte al rischio di commissione dei reati espressamente richiamati dal Decreto (cap 3) ([2]);
- descrizione delle regole comportamentali ("***principi di comportamento specifici"***) che, richiamandosi all'osservanza del Codice Etico, specificano le regole di condotta dei destinatari del Modello al fine di prevenire la commissione dei singoli gruppi di reati (§ 4.1) e, quindi, complementano il sistema di regole comportamentali generali già definito dal Codice etico;
- definizione dei ***protocolli procedurali specifici*** che devono regolare, nella Società, la formazione delle decisioni, la loro attuazione, insieme ai controlli relativi a tali azioni, in modo da garantire la prevenzione della commissione dei reati presupposto (§ 4.2). Tali protocolli si basano sui princìpi di

    - chiara definizione dei ruoli e delle responsabilità, ovvero
        a) assetto organizzativo che definisca in modo chiaro poteri, funzioni, responsabilità e riporti gerarchici di ogni organo e dei suoi componenti;
        b) sistema di deleghe e attribuzione di poteri e procure che definisca in modo chiaro quali soggetti hanno competenze decisionali e autorizzative;
        c) chiara separazione dei ruoli tra chi è responsabile, esecutore o controllore di una attività
    - tracciabilità di tutte le attività svolte e dei soggetti coinvolti, mediante sistemi adeguati di documentazione, anche informatica, delle operazioni e di conservazione delle informazioni prodotte
    - proceduralizzazione delle attività, in termini di procedure manuali e, soprattutto, informatiche (sistemi informativi) tali da regolamentare lo svolgimento delle attività, prevedendo anche opportuni punti di controllo in linea (i cosiddetti controlli di 1° livello)
    - controllo di gestione (controlli di 2° livello), in grado di fornire segnalazione dell'esistenza e dell'insorgere di situazioni di criticità.

  I protocolli specifici, finalizzati ad una efficace azione preventiva rispetto ai rischi previsti dal D.Lgs 231/01, possono includere tanto strumenti di gestione e controllo già vigenti in azienda (messi a punto, ad esempio, con finalità di efficacia ed efficienza operativa [es: Sistemi Qualità], ma che possono anche avere efficacia esimente a fini "231"), tanto ulteriori protocolli, da adottare da parte della Società.

---

1 Una trattazione più approfondita delle singole fattispecie è riportata in Allegato 1.

2 Tale identificazione è stata ottenuta attraverso una attività sistematica di valutazione del rischio per tutti i processi aziendali, così come articolati in All. A della Parte Generale del Modello, individuando cioè quelle condotte astrattamente ipotizzabili che determinerebbero la commissione dei reati previsti dal Decreto. Il dettaglio del processo di valutazione sui singoli processi è riportato in Allegato 2 del presente documento, mentre il cap. 3 di ciascuna Parte Speciale riporta l'esito di tale analisi, in termini di lista delle attività sensibili rispetto a cui sviluppare le componenti del Modello

- identificazione dei ***flussi informativi verso l'OdV*** , che come controllo di 3° livello, forniscono un efficace monitoring dei fattori di criticità e, quindi, permettono all'OdV stesso lo svolgimento del proprio ruolo di controllo sul funzionamento complessivo del Modello di Organizzazione e Gestione e la pronta attuazione di misure reattive (cap 5).

PARTE SPECIALE A : REATI NEI RAPPORTI CON LA P.A.

1 AMBITO APPLICATIVO ED OBIETTIVI

Non tutte le persone fisiche che agiscono nella sfera ed in relazione alle pubbliche amministrazioni sono soggetti nei confronti dei quali (o ad opera dei quali) si perfezionano le fattispecie di Reati nei rapporti con la Pubblica Amministrazione. Le figure che assumono rilevanza a tal fine sono soltanto quelle dei "Pubblici Ufficiali" e degli "Incaricati di Pubblico Servizio" (si vedano le relative definizioni a cap 7) , laddove la società InnovaPuglia, stando i propri compiti statutari, può quindi essere qualificata in quest'ultima categoria.

2 LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati *ex* art. 5 del d.lgs. n. 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.
Si riporta, pertanto, di seguito una breve descrizione dei reati richiamati dagli art 24 (*Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico)* e 25 (*Concussione e corruzione*) del d.lgs. n. 231/2001; una discussione più puntuale degli stesi reati è riportata in Allegato 1.A .

2.1 Reati di tipo corruttivo

Corruzione per l'esercizio della funzione e ambito applicativo (Artt. 318 e 320 c.p.)
L'ipotesi di reato di cui all'art. 318 c.p. si configura nel caso in cui un pubblico ufficiale, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa.

Corruzione per un atto contrario ai doveri di ufficio, circostanze aggravanti e ambito applicativo (artt. 319, 319 bis e 320 c.p.)
L'ipotesi di reato di cui all'art. 319 c.p. si configura nel caso in cui il pubblico ufficiale, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa.
Ai fini della configurabilità di tale reato in relazione al compimento di un atto contrario ai doveri di ufficio vanno considerati sia gli atti illegittimi o illeciti (vietati, cioè, da norme imperative o contrastanti con norme dettate per la loro validità ed efficacia) sia quegli atti che, pur formalmente regolari, siano stati posti in essere dal pubblico ufficiale violando il dovere d'imparzialità o asservendo la sua funzione a interessi privati o comunque estranei a quelli proprio della Pubblica Amministrazione.
Si sottolinea infine come le ipotesi di reato di cui agli artt. 318 e 319 c.p. si differenzino dalla concussione in quanto tra corrotto e corruttore esiste un accordo finalizzato a raggiungere un vantaggio reciproco, mentre nella concussione il privato subisce la condotta del pubblico ufficiale.

Corruzione in atti giudiziari (Art. 319 ter c.p.)
Tale ipotesi di reato si configura nel caso in cui, per favorire o danneggiare una parte in un procedimento giudiziario, si corrompa un pubblico ufficiale, e dunque un magistrato, un cancelliere o altro funzionario dell'autorità giudiziaria.
È importante sottolineare come il reato possa configurarsi a carico della Società indipendentemente dal fatto che la stessa sia parte del procedimento.

Istigazione alla corruzione (Art. 322 c.p.)
Tale ipotesi di reato si configura nel caso in cui venga offerto o promesso danaro o altra utilità ad un pubblico ufficiale o incaricato di pubblico servizio (per l'esercizio delle sue funzioni o dei suoi poteri, per omettere o a ritardare un atto del suo ufficio, ovvero per fare un atto contrario ai suoi doveri) e tale offerta o promessa non venga accettata.

Corruzione tra privati (art.2635 c.c.)
Il reato in esame si configura allorché gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori ovvero chi è sottoposto alla direzione alla vigilanza di uno dei soggetti indicati precedentemente, 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.
Inoltre, il reato si configura nelle ipotesi in cui taluno dà o promette denaro o altra utilità alle persone sopra indicate.
Tale caso è il solo rilevante ai fini della responsabilità amministrativa delle società in quanto è espressamente richiamato dall'art.25-*ter* del d.lgs.231/01.

2.2 Reato di concussione

Concussione (Art. 317 c.p.)
Il reato si configura nel caso in cui il pubblico ufficiale che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità.
Anche la concussione, al pari della corruzione, è un reato bilaterale, in quanto richiede la condotta di due distinti soggetti, il concussore e il concusso.
Tuttavia, a differenza della corruzione, solo il concussore è assoggettato a pena, in quanto il concusso è la vittima del reato.
Le ipotesi di responsabilità dell'Ente per concussione sono poco significative, in quanto il comportamento concussivo dovrebbe essere realizzato nell'interesse o a vantaggio dell'ente e non, come accade di solito, nell'esclusivo interesse del concussore.

Induzione indebita a dare o promettere utilità (art.319 quater c.p.)
Tale ipotesi di reato si configura nel caso in cui il pubblico ufficiale o l'incaricato di pubblico servizio, abusando della sua qualità o dei suoi poteri, indice taluno a dare o promettere indebitamente, a lui o un terzo, denaro o altra utilità.

2.3 Reati di truffa

Truffa in danno dello stato o di altro ente pubblico (art. 640, comma 2, n. 1 c.p.)
Tale ipotesi di reato si configura nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifizi e raggiri (intendendosi ricompresa in tale definizione anche l'eventuale omissione di informazioni che, se conosciute, avrebbero certamente determinato in senso negativo la volontà dello Stato, di altro ente pubblico o dell'Unione Europea) tali da indurre in errore e da arrecare un danno (di tipo patrimoniale) a tali enti.

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

Frode informatica (Art. 640 ter c.p.)
Si configura il reato di frode informatica quando, al fine di procurare a sé o ad altri un ingiusto profitto, venga alterato in qualsiasi modo il funzionamento di un sistema informatico, o si intervenga, senza diritto, su dati, informazioni o programmi contenuti in un sistema informatico.

2.4 Reati di malversazione e di indebita percezione di erogazioni

Malversazione a danno dello Stato (Art. 316 bis c.p.)

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

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

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

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

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

La linea di demarcazione tra l'ipotesi di Indebita percezione di erogazioni a danno dello Stato (ex art. 316 ter c.p.) e quella di Truffa aggravata per il conseguimento di erogazioni pubbliche (ex art. 640 bis c.p.) risiede nel tipo di condotta criminosa del reo che, nel primo caso, si limita a presentare documenti falsi o ad omettere informazioni dovute; mentre nella seconda ipotesi pone in essere artifizi o raggiri che provocano l'induzione in errore della Pubblica Amministrazione.

3 LE ATTIVITAôSENSIBILI AI FINI DEL D.LGS. 231/2001

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'individuazione delle attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dagli artt. 24 e 25 del d.lgs. n. 231/2001, è stata ottenuta attraverso l'analisi puntuale dei processi della Società (così come riportati in All. A della Parte Generale del Modello) , individuando quelle condotte astrattamente ipotizzabili che determinerebbero la commissione dei reati previsti dal Decreto. L'individuazione puntuale dei processi a rischio è riportata in Allegato 2.A al presente documento.

Le attività sensibili individuate attraverso tale processo e che trovano come presupposto l'instaurazione di rapporti, diretti o indiretti, con le pubbliche amministrazioni, sono, pertanto:

1. Gestione dei rapporti con la Regione Puglia

Processi di interesse : - negoziazione di nuovi affidamenti
- definizione delle tariffe applicabili

2. Progettazione e sviluppo del sistema informativo regionale

Processi di interesse :
- progettazione di dettaglio
- project management
- esecuzione contratti

3. Gestione rapporti con Autorità ed Enti pubblici

Processi di interesse :
- richieste concessioni, autorizzazioni, licenze
- gestione rapporti con VVF, ASL, INAIL,… e relative certificazioni
- gestione rapporti con enti fiscali, previdenziali,..

4. Gestione del contenzioso giudiziario

Processi di interesse :
- gestione rapporti con legali esterni
- gestione del contenzioso giudiziario

Sono altresì stati individuati i seguenti processi da considerarsi sia come "**strumentali**" alle attività sopra esaminate in quanto, pur non essendo caratterizzati dall'esistenza di rapporti diretti con la Pubblica Amministrazione, possono costituire supporto e presupposto (finanziario ed operativo) per la commissione dei reati nei rapporti con la P.A.; sia come attività "sensibili" con riferimento al reato di corruzione tra privati in quanto caratterizzati dall'esistenza di rapporti diretti con soggetti privati:

a. Gestione del processo di gara

Processi di interesse :
- procedure ordinarie di gara
- acquisti in economia

b. Attività di Organismo Intermedio

Processi di interesse :
- Bandi per incentivi alla innovazione delle imprese / Istruttoria valutativa
- Monitoraggio interventi ammessi ad agevolazione

c. Reclutamento del personale

Processi di interesse :
- Bandi pubblici di selezione

d. Conferimento incarichi di consulenza / collaborazione

Processi di interesse :
- Selezione con procedura comparativa
- affidamento diretto (es: incarichi "intuitu personae")
- attribuzione incarichi legali

e. Gestione degli acquisti

Processi di interesse :
- Acquisti con ordine commerciale

f. Gestione tesoreria e movimenti finanziari

Processi di interesse:
- gestione conti correnti
- pagamenti
- incassi

4 PROTOCOLLI PER LA FORMAZIONE E LôATTUAZIONE DELLE DECISIONI E SISTEMA DI CONTROLLO

4.1 Principi specifici di comportamento

I seguenti principi di comportamento si applicano ai Destinatari che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto ai reati con la Pubblica Amministrazione di cui all'art.24 e 25 del D.Lgs. 231/2001.

Le condotte di ordine generale descritte integrano e non sostituiscono i principi previsti dal Codice Etico, nonché le eventuali procedure di maggiore tutela previste all'interno di InnovaPuglia e relative alle attività sensibili.

La presente Parte Speciale prevede l'espresso **obbligo** 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 ed alle attività relative allo svolgimento 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;
- ✓ segnalare tempestivamente l'insorgenza di ogni situazione che possa creare situazioni di conflitto di interessi

La presente Parte Speciale prevede, conseguentemente, l'espresso **divieto** – a carico degli esponenti aziendali, in via diretta e a carico dei Collaboratori esterni e Fornitori, tramite apposite clausole contrattuali – di:

- ✓ porre in essere comportamenti tali da integrare le fattispecie di reato sopra considerate (artt. 24 e 25 del Decreto);
- ✓ porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- ✓ effettuare o promettere, direttamente o tramite terzi, pagamenti e compensi per indurre, facilitare o remunerare una decisione, il compimento di un atto d'ufficio o contrario ai doveri d'ufficio da parte di soggetti della Pubblica Amministrazione;
- ✓ accogliere richieste (indebite) di un pubblico funzionario volte a dare o promettere utilità
- ✓ distribuire omaggi e regali a funzionari pubblici, o a loro familiari, chiamati a decidere su fatti rilevanti per la Società, ovvero che concorrano in dette decisioni e che possano influenzarne la discrezionalità o l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda; si applicano in ogni caso le disposizioni previste dal Codice Etico;
- ✓ favorire, attraverso i processi di acquisto di beni e servizi e i processi di selezione e gestione consulenze e incarichi professionali, specifici soggetti dietro segnalazione dei Rappresentanti della Pubblica Amministrazione, in cambio di favori, compensi o altri vantaggi per sé e/o per la Società;
- ✓ presentare dichiarazioni incomplete o comunque non veritiere ad organismi pubblici nazionali o comunitari, al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati;
- ✓ destinare somme ricevute da organismi pubblici nazionali, regionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati
- ✓ intrattenere rapporti con la Pubblica Amministrazione in rappresentanza o per conto della Società, per ragioni estranee a quelle professionali e non riconducibili alle competenze ed alle funzioni assegnate;

- ✓ tenere una condotta ingannevole che possa indurre i Rappresentanti della Pubblica Amministrazione in errori di valutazione tecnico-economica sulla documentazione presentata dalla Società, nell'ambito dei molteplici rapporti che essa intrattiene con la pubblica autorità;
- ✓ omettere informazioni dovute alla Pubblica Amministrazione al fine di orientarne a proprio favore le decisioni;
- ✓ presentare ai Rappresentanti della Pubblica Amministrazione dichiarazioni, dati o documenti non veritieri in occasione delle definizione e sottoscrizione di atti e convenzioni;
- ✓ frazionare artificiosamente gli importi allo scopo di eludere le normative applicabili.

In nessun caso le assunzioni e, in generale, la gestione del personale può costituire occasione di possibili "scambi di favori" con soggetti appartenenti alla Pubblica Amministrazione. Tutti i contatti relativi devono avvenire in condizioni di correttezza e trasparenza.

Gli acquisti di beni e servizi avvengono nel rispetto dei principi di efficacia, efficienza, economicità, libera concorrenza, non discriminazione, trasparenza delle informazioni ed in coerenza con le disposizioni contenute nel D.Lgs 163/2006 e s.m.i.

In caso di rapporti con la PA gestiti da soggetti esterni (es: professionisti, consulenti,…) gli stessi devono impegnarsi a rispettare i principi contenuti nel Codice Etico e nelle disposizioni di legge.
In particolare, per gli incarichi legali, lo svolgimento della prestazione deve avvenire nel rispetto dei principi di trasparenza e del divieto di attuare qualsiasi forma di corruzione in atti giudiziari.

4.2 Protocolli Specifici

4.2.1 Gestione dei rapporti con la Regione Puglia

Processi di interesse	- negoziazione di nuovi affidamenti - definizione delle tariffe applicabili
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ tutti i rapporti di valenza decisionale con soggetti regionali possono essere gestiti solo da soggetti formalmente delegati ✓ tutti i rapporti con aziende che propongano o gestiscano contatti extra-contrattuali con la Regione devono essere comunicati e autorizzati ✓ viene definita e concordata con la Regione una procedura standard per il calcolo delle tariffe riconosciute per l'attività della Società e le relative modalità di aggiornamento ✓ Verbalizzazione degli incontri, rilevanti a fini di nuovi affidamenti, con responsabili regionali, con conservazione della relativa documentazione in archivio centralizzato, ✓ Verbalizzazione di incontri con aziende che intendano proporsi alla

	Regione ovvero che siano segnalate da esponenti regionali ✓ Verbalizzazione di incontri conoscitivi/ strategici con associazioni di imprese ✓ la documentazione (tecnica, economica, preventivi, indagini di mercato, comunicazioni, altre evidenze informali,..) funzionale alla formulazione di nuove schede progetto deve essere conservata a cura del dirigente responsabile ✓ relazione relativa ad ogni aggiornamento delle tariffe, garantendo la tracciabilità dei parametri di base su cui sono calcolate le tariffe stesse

4.2.2 Progettazione e sviluppo del sistema informativo regionale

Processi di interesse	- progettazione di dettaglio - project management - esecuzione contratti
Procedure/ regolamenti applicabili	✓ *Procedura di erogazione di servizi IT : Analisi del servizio IT - PRQSIanaser* ✓ *Procedura di erogazione di servizi IT : Progettazione del servizio IT - PRQSIprogser* ✓ *Procedura di erogazione di servizi IT : Gestione del servizio IT - PRQSIgesprog* ✓ *Procedura per l'esecuzione del contratto*
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ verificare l'esistenza di conflitti di interesse per attività di progettazione e/o gestione di progetti ✓ evidenziare eventuali contributi alla redazione della documentazione di progetto (in particolare, capitolati di gara) da parte di soggetti esterni alla Società ✓ tutte le risorse di progetto devono ricevere lettera di servizio con definizione quali-quantitativa dell'impegno previsto ✓ adozione del *time report* , da parte delle risorse di progetto, per la registrazione settimanale delle attività svolte ✓ definire procedura interna per la gestione delle varianti (proroghe, modifiche tecniche, allocazione budget) ✓ i processi di autorizzazione e controllo delle trasferte devono essere sempre ispirati a criteri di economicità e di massima trasparenza, sia nei confronti della regolamentazione aziendale interna che nei confronti delle leggi e delle normative fiscali vigenti; ✓ le dotazioni tecnologiche individuali acquisite su progetto devono essere adeguatamente giustificate rispetto all'utilizzo previsto e assegnate a personale operativo sul progetto stesso ✓ il sostenimento di spese di rappresentanza deve soddisfare il concetto di "opportunità" della spesa, in linea pertanto con gli obiettivi aziendali e progettuali ✓ le spese di trasferta e i rimborsi spese su progetto sostenute da

	rappresentanti della Pubblica Amministrazione devono essere adeguatamente motivate, nel rispetto dei limiti di spesa e con collegamento alle relative fatture / note spese ✓ Implementare una procedura standard di rilevazione della *customer satisfaction* del referente regionale del progetto relativamente alle modalità di attuazione e ai risultati conseguiti ✓ per attività appaltate a terzi, verificare l'esistenza di possibili conflitti d'interesse per il Responsabile dell'Esecuzione del Contratto (REC) ✓ il monitoraggio della regolare esecuzione delle prestazioni da parte dei fornitori e le decisioni su aspetti economici ad esse collegate, devono risultare per iscritto, fondarsi su criteri oggettivi e imparziali, nonché sulle clausole contrattuali; in tali attività il REC viene sempre affiancato da personale aziendale esterno alle attività svolte; ✓ tutta la documentazione tecnica di commessa, insieme al fascicolo di commessa, viene gestita e conservata in modo centralizzato e accessibile con predefiniti livelli di autorizzazione ✓ tutte le riunioni di progetto di significativa rilevanza devono essere verbalizzate

4.2.3 Gestione rapporti con Autorità ed Enti pubblici

Processi di interesse	- richieste concessioni, autorizzazioni, licenze - gestione rapporti con VVF, ASL, INAIL,… e relative certificazioni - gestione rapporti con enti fiscali, previdenziali,..
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	✓ procura al DG per pratiche presso la PA per concessioni, autorizzazioni e licenze
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ dovrà essere assicurata, in caso di accertamenti ispettivi svolti dalle Autorità (es. relative al D.Lgs. 81/08, verifiche tributarie, INPS, etc.) , una adeguata collaborazione da parte delle unità aziendali competenti. In particolare, di volta in volta per ciascuna ispezione disposta dalle Autorità, dovrà essere individuato in ambito aziendale un responsabile incaricato di assicurare il coordinamento tra gli addetti delle diverse unità aziendali ai fini del corretto espletamento da parte di questi ultimi delle attività di propria competenza; ✓ solo i soggetti muniti di apposita procura sono autorizzati a fornire la documentazione richiesta durante lo svolgimento delle attività di verifica e di controllo e a firmare i verbali ✓ le funzioni interessate dovranno dotarsi di un calendario/scadenzario per quanto riguarda gli adempimenti ricorrenti ✓ ove fosse necessario coinvolgere consulenti, partner o collaboratori esterni per assistere la Società durante il processo di verifica/ispezione, questi devono essere scelti con metodi trasparenti e secondo specifica procedura aziendale

	✓ nel caso il verbale conclusivo evidenzi criticità, l'OdV ne deve essere informato con nota scritta da parte del responsabile della Direzione coinvolta ✓ di tutto il procedimento relativo all'ispezione devono essere redatti e conservati appositi verbali. La documentazione deve essere conservata dal responsabile di direzione competente in un apposito archivio, con modalità tali da impedire la modifica successiva se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi

4.2.4 Gestione del contenzioso giudiziario

Processi di interesse	- gestione rapporti con professionisti esterni - gestione del contenzioso giudiziario
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	✓ il DG può agire in rappresentanza della Società innanzi a qualsiasi Autorità amministrativa e giudiziaria
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ l'eventuale transazione e/o conciliazione deve essere condotta da soggetto titolare di un'apposita procura ad litem, che contempli il potere di conciliare o transigere la controversia ✓ i responsabili di Servizio trasmettono tempestivamente al Direttore Generale e Direttore Affari Generali ogni eventuale diffida e/o comunicazione, di natura giudiziale, indirizzata loro o alla Società, da cui possa desumersi l'esistenza o il probabile insorgere di un contenzioso; ✓ il Direttore Generale, con la collaborazione del responsabile di Divisione / Servizio coinvolto e del Direttore Affari Generali, esamina la documentazione e definisce le azioni da intraprendere, anche avvalendosi del supporto di legali esterni; ✓ definire i limiti delle deleghe di spesa dei soggetti coinvolti nella gestione del contenzioso; ✓ prevedere specifiche linee di reporting periodico sullo stato delle vertenze, sulle possibilità e sui termini di definizione stragiudiziale o di conciliazione giudiziale della stessa; ✓ assicurarsi che tutta la documentazione depositata dal proprio avvocato e dalla controparte sia disponibile in sede e non rimanga presso lo studio dell'avvocato stesso ✓ mantenere traccia dei soggetti interni (amministratori, dirigenti, dipendenti) chiamati a rendere dichiarazioni innanzi all'Autorità Giudiziaria in merito ad attività connessa alla gestione e amministrazione societaria. ✓ mantenere un sistema di registrazione degli atti giudiziali ricevuti ✓ deve essere garantita la tracciabilità delle singole fasi del processo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte effettuate e delle fonti informative utilizzate

4.2.5 Gestione del processo di gara

Processi di interesse	- procedure ordinarie di gara - acquisti in economia
Procedure/ regolamenti applicabili	✓ *Regolamento per l'acquisto in economia di forniture di beni e servizi* (Approvazione CdA del 15/10/2012 verb. 049) ✓ *Procedura di gara (aperta / ristretta)* ✓ le gare vengono attuate di norma in modalità telematica avvalendosi della piattaforma EmPULIA ✓ per gli acquisti in economia, i fornitori da invitare vengono individuati nell'ambito dell'Albo online dei fornitori della Regione Puglia
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ va definito un regolamento per la nomina e il funzionamento della Commissione di Gara ✓ in particolare, la composizione della commissione deve rispettare, per quanto possibile, criteri di competenza, di turnazione e di segregazione dei ruoli (chi ha richiesto una specifica fornitura è diverso da chi valuta le offerte) ✓ i soggetti che partecipano alle commissioni di gara in qualità di presidente/commissario e/o in qualità di RUP si astengono, in caso di conflitto di interessi, dall'assumere decisioni o dallo svolgere attività inerenti alla propria mansione, dandone comunicazione scritta al Direttore Generale; ✓ i componenti delle commissioni di gara si astengono dall'intrattenere rapporti con i soggetti interessati ad ottenere informazioni circa le caratteristiche e lo svolgimento della gara ✓ le commissioni di gara devono dare evidenza, nei verbali predisposti dalla commissione stessa, della presenza di eventuali soggetti estranei (es: personale tecnico o altri ausiliari) alle relative sedute ✓ ogni comunicazione con il concorrente avviene per iscritto nelle forme di legge

4.2.6 Attività di Organismo Intermedio

Processi di interesse	- Bandi per incentivi alla innovazione delle imprese / Istruttoria valutativa - Monitoraggio interventi ammessi ad agevolazione
Procedure/ regolamenti applicabili	✓ *Sistema di Gestione e controllo di InnovaPuglia in qualità di Organismo Intermedio*

	✓ *Procedure dell'Unità di Controllo (UdC)* ✓ Chiara separazione dei ruoli funzionali tra RUP, Nucleo di Valutazione, Unità di Gestione [UdG], Unità di Monitoraggio [UdM] e Unità di Controllo [UdC]
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ regolamento per la nomina e il funzionamento del Nucleo di Valutazione ✓ regolamento per la turnazione del personale dell'Organismo Intermedio nei ruoli di UdG, UdM e UdC

4.2.7 Reclutamento del personale

Processi di interesse	- Bandi pubblici di selezione
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	✓ Il DG propone al CdA l'assunzione del personale dipendente e dei dirigenti
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ definire un regolamento per la costituzione della Commissione di selezione, rispetto a cui occorre: - garantire che i componenti siano scelti esclusivamente tra esperti di provata competenza nelle tematiche cui il bando si riferisce, scelti anche tra funzionari delle amministrazioni, docenti ed estranei alle medesime, che non siano componenti dell'organo di direzione politica dell'amministrazione, che non ricoprano cariche politiche e che non siano rappresentanti sindacali o designati dalle confederazioni ed organizzazioni sindacali o dalle associazioni professionali; - verificare l'esistenza di conflitti di interesse da parte di tutti i membri della Commissione ✓ definire a priori, a cura della Commissione, un sistema strutturato, oggettivo e trasparente, di valutazione dei candidati, al fine di garantire la tracciabilità delle motivazioni che hanno indotto alla scelta/esclusione dei candidati ✓ rispetto delle pari opportunità tra lavoratrici e lavoratori; ✓ segnalare ogni tentativo, da parte di esponenti della PA o di altri soggetti, interni o esterni, di orientare le scelte della Commissione ✓ nelle operazioni di selezione prevedere una dichiarazione, sottoscritta dal candidato, che attesti l'eventuale esistenza di rapporti, diretti o indiretti, tra il candidato stesso e dipendenti della Società, ovvero con gli Organi sociali ovvero, più in generale, con soggetti della Pubblica Amministrazione, regionale e non e, in caso positivo, sia valutata l'eventuale sussistenza di ipotesi di conflitto di interessi;

	✓ devono essere definiti criteri di controllo nel caso in cui l'ente stesso faccia ricorso al lavoro interinale mediante le agenzie specializzate; ✓ all'atto dell'assunzione il dipendente firma specifica dichiarazione di accettazione del Codice Etico e del Modello di Organizzazione, Gestione e Controllo ex-D.Lgs 231/01; ✓ segregazione delle responsabilità tra le Unità Organizzative competenti che svolgono le attività di richiesta di assunzione di personale, di valutazione/selezione del personale, della definizione della proposta di assunzione, della firma della lettera di assunzione;

4.2.8 Conferimento incarichi di consulenza / collaborazione

Processi di interesse	- Selezione con procedura comparativa - affidamento diretto (es: incarichi "intuitu personae") - attribuzione incarichi legali
Procedure/ regolamenti applicabili	✓ *Regolamento per il conferimento di incarichi esterni* (approvato dal CdA del 21 marzo 2014 verbale n. 068) ✓ *Regolamento dell'Albo dei Consulenti di InnovaPuglia*
Poteri autorizzativi e di firma rilevanti per l'attività	✓ La designazione della Commissione di selezione è rimessa al Direttore Generale ✓ Delega al DG per affidamento di incarichi non superiori a 25.000 euro
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ il processo di selezione viene avviato a fronte di una richiesta con requisiti oggettivi e verificabili ✓ valutare l'esistenza di situazioni di conflitto di interessi da parte dei componenti della Commissione di selezione ✓ utilizzabilità, ai fini dei processi di selezione da Albo, solamente di nominativi di professionisti iscritti all'Albo stesso almeno 30 gg prima della pubblicazione del bando di selezione ✓ la definizione del profilo professionale richiesto per la posizione deve risultare abbastanza ampia, caratterizzando un'area culturale e/o di saper fare, piuttosto che riferirsi a specializzazioni estremamente caratterizzate. Ove sia richiesta una specifica competenza (es: su un prodotto) che restringa notevolmente la potenziale rosa dei candidati, questo deve essere esplicitamente giustificato ✓ prevedere una dichiarazione, sottoscritta dal candidato, che attesti l'eventuale esistenza di rapporti, diretti o indiretti, tra il candidato stesso e dipendenti della Società, ovvero con gli Organi sociali ovvero, più in generale, con soggetti della Pubblica Amministrazione, regionale e non ✓ in caso di selezione di soggetti che abbiano attestato l'esistenza di tali rapporti, il caso deve essere segnalato all'OdV ✓ il compenso riconosciuto deve trovare adeguata giustificazione in relazione al tipo di incarico da svolgere e deve risultare coerente con altri contratti di consulenza assegnati dalla Società e assimilabili ✓ definire meccanismi di valutazione complessiva del servizio reso; ✓ nell'impiego di consulenti esterni devono essere previsti dei meccanismi

	di verifica preventiva dell'assenza di contemporanea collaborazione sulla medesima materia con le stesse amministrazioni pubbliche (per esempio mediante auto-certificazione del consulente esterno); ✓ evitare il ricorso allo strumento del rinnovo dell'incarico, salvo adeguata giustificazione che deve essere preventivamente approvata dagli Organi ✓ per incarichi di consulenza assegnati secondo l'istituto dell' *intuitu personae*, va predisposta, da parte del richiedente, specifica motivazione del ricorso all'istituto, oltre che della scelta dello specifico professionista ✓ il pagamento al consulente/ professionista è effettuato solo al corretto completamento della prestazione contrattualizzata ovvero, se espressamente previsto, a stato di avanzamento attività ✓ prevedere, nel contratto di consulenza/collaborazione, l'accettazione esplicita del Codice Etico aziendale, regolando, altresì, le conseguenze della violazione, da parte degli stessi, delle norme e dei principi di cui al D.Lgs 231/01 ✓ nei contratti con consulenti deve essere contenuta apposita dichiarazione dei medesimi di non aver mai subito condanne con sentenza passata in giudicato o provvedimenti equiparati in procedimenti giudiziari relativi ai reati contemplati dal presente Modello <u>Per incarichi di consulenza legale:</u> ✓ i legali e consulenti esterni, incaricati di assistere InnovaPuglia nei contenziosi devono essere scelti e valutati con metodi trasparenti e secondo specifica procedura aziendale (ad esempio, capacità tecnica, esperienza, requisiti soggettivi di professionalità e onorabilità, referenze qualificanti, politica di prezzo) e delle modalità di gestione; ✓ verificare la mancanza di cause di incompatibilità o l'esistenza di eventuali conflitti d'interesse del professionista esterno per la difesa della Società; ✓ l'importo del compenso, le provvigioni o le commissioni, devono essere pattuiti in sede contrattuale, determinati in misura congrua rispetto alle prestazioni rese e conformi all'incarico conferito, secondo le condizioni o le prassi esistenti sul mercato o le tariffe professionali vigenti per la categoria interessata (in particolare, con riferimento alle tabelle approvate dalla Regione Puglia) ✓ implementare strumenti di monitoraggio e controllo dell'operato, allo scopo di verificare la resa prestazione ✓ predisposizione, registrazione e archiviazione della documentazione al fine di consentire la ricostruzione delle diverse fasi del processo. ✓ Procedura di verifica della natura e pertinenza degli oneri legali sostenuti;

4.2.9 Gestione degli acquisti

Processi di interesse	- Acquisti con ordine commerciale
Procedure/ regolamenti applicabili	✓ *Regolamento per l'acquisto in economia di forniture di beni e servizi* (approvato dal CdA del 21 marzo 2014, verb. n. 68)
Poteri autorizzativi e di firma rilevanti per l'attività	✓ delega al DG per espletare gare e affidamenti entro 40.000 euro

Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ gli acquisti di beni e servizi (per importi inferiori a 20.000 euro) avvengono esclusivamente sulla base di richieste formulate per iscritto, approvate ed evase dai Servizi/Unità Organizzative competenti (mod. M24) ; ✓ i rapporti con i fornitori di beni e servizi sono gestiti esclusivamente dal personale individuato nei regolamenti aziendali; ✓ la corretta e fisiologica rotazione dei fornitori viene assicurata anche attraverso un adeguato sistema di monitoraggio; ✓ prevedere una chiara segregazione dei ruoli tra chi predispone la richiesta d'acquisto, chi seleziona, chi sottoscrive i relativi contratti e chi ne garantisce la corretta esecuzione; ✓ nei contratti con i fornitori deve essere contenuta apposita dichiarazione dei medesimi di non aver mai subito condanne con sentenza passata in giudicato o provvedimenti equiparati in procedimenti giudiziari relativi ai reati contemplati dal presente Modello;

4.2.10 Gestione tesoreria e movimenti finanziari

Processi di interesse	- gestione conti correnti - pagamenti - incassi
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	✓ il DAG ha procura per effettuare versamenti, dare disposizioni di pagamento sui conti correnti intestati alla Società a fronte di impegni della Società (da obblighi di legge o per prestazioni o forniture di terzi) ✓ il DAG ha procura per recupero crediti ✓ il DAG ha procura per sottoscrizione e invio documentazione fiscale e tributaria ✓ il DAG ha procura per gli adempimenti previdenziali e assicurativi per il personale e i lavoratori autonomi
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ il Consiglio di Amministrazione, o il soggetto da esso delegato, deve stabilire e modificare, se necessario, la procedura di firma congiunta per determinate tipologie di operazioni o per operazioni che superino una determinata soglia quantitativa. Di tale modifica è data informazione all'Organismo di Vigilanza; ✓ definire con chiarezza ruoli, compiti e responsabilità delle Funzioni/Unità organizzative coinvolte durante le diverse fasi del processo (gestione dei pagamenti; gestione degli incassi, gestione delle fatture); ✓ devono essere vietati i flussi sia in entrata che in uscita in denaro contante, salvo che per tipologie minime di spesa espressamente

	autorizzate dalla funzione amministrazione, ed in particolare per le operazioni di piccola cassa che sono comunque codificate in modo tale da permettere di risalire al disponente e al beneficiario; ✓ le operazioni di apertura, gestione e chiusura dei conti correnti bancari e postali (i.e. invio di documentazione, comunicazioni etc.) è effettuata nel rispetto delle deleghe aziendali; ✓ i poteri di firma depositati presso le banche devono essere aggiornati rispetto alle procure esistenti ✓ verificare, nei pagamenti a favore di terzi, il rispetto di tutti i passaggi autorizzativi relativi alla predisposizione, validazione ed emissione del mandato di pagamento, nonché della registrazione a sistema della relativa distinta; ✓ i movimenti che transitano in addebito sul conto corrente (i.e. pagamenti di fatture, etc.) devono essere in linea con gli impegni di spesa ed autorizzati dal responsabile del procedimento di spesa; ✓ gli ordinativi di pagamento sono vidimati dal Responsabile del Servizio; ✓ gli incassi sono supportati da documentazione comprovante la sussistenza del titolo giuridico, il nominativo del debitore, la somma da incassare e la relativa scadenza; ✓ le operazioni che comportano l'utilizzo o l'impiego di risorse economiche (acquisizione, gestione, trasferimento di denaro e valori) o finanziarie sono sempre contrassegnate da una causale espressa, documentate e registrate in conformità ai principi di correttezza gestionale e contabile; il processo operativo e decisionale deve essere tracciabile e verificabile nelle singole operazioni; ✓ viene effettuata la verifica periodica sulla corrispondenza di ciascun pagamento e incasso con la documentazione contabile e contrattuale giustificativa; ✓ il soggetto delegato possiede le credenziali per accedere al servizio di home banking ✓ deve essere verificata la regolarità dei pagamenti con riferimento alla piena coincidenza dei destinatari/ ordinanti i pagamenti e le controparti effettivamente coinvolte nella transazione ✓ non deve esservi identità soggettiva tra chi impegna la società nei confronti di terzi e chi autorizza o dispone il pagamento di somme dovute in base agli impegni assunti; laddove ciò non sia possibile in merito a singole operazioni, ne deve essere data comunicazione all'Organismo di Vigilanza; ✓ il sistema (anche informatico) deve consentire la tracciabilità dei singoli passaggi e l'identificazione dei soggetti che inseriscono i dati nel sistema nonché la conservazione della documentazione giustificativa a supporto i) delle registrazioni contabili relative alle singole operazioni di incasso, pagamento e apertura/ chiusura/movimentazione dei conti correnti; ii) dei controlli effettuati sulla completezza e correttezza delle relative registrazioni contabili ✓ deve essere possibile attuare l'analisi dei tempi di pagamento sulla base della singola commessa / centro di costo (analisi dei ritardi di pagamento rispetto ai tempi di fatturazione del fornitore / ai tempi di incasso dalla PA / ….)

5 FLUSSI INFORMATIVI SPECIFICI VERSO LôODV

I controlli svolti dall'Organismo di Vigilanza sono diretti a verificare la conformità delle attività aziendali ai principi espressi nella presente Parte Speciale e, in particolare, alle procedure interne in essere ed a quelle che saranno adottate in futuro, in attuazione della presente Parte Speciale.

A tal fine l'Organismo di Vigilanza

- effettua periodicamente controlli a campione sulle attività connesse ai «processi sensibili», diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. In questa prospettiva, pur garantendo all'Organismo libero accesso a tutta la documentazione aziendale rilevante così come previsto nella Parte Generale, vengono, comunque garantiti, in maniera continuativa, i flussi informativi elencati di seguito in tabella

- può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello 231.

PROCESSO DA VERIFICARE	FLUSSO INFORMATIVO VERSO OdV	FREQUENZA
Assetto organizzativo	- Modifiche organizzative che impattano su attività a rischio reato	Annuale
Processi decisionali degli organi sociali / Definizione delle aliquote	- Modello di calcolo delle tariffe - Documentazione relativa ad ogni aggiornamento delle tariffe	Annuale
Ispezioni, accessi, verifiche da parte di Autorità Pubbliche (Agenzia delle Entrate, Guardia di Finanza, Arpa, Vigili del Fuoco, Ispettorato del lavoro, etc.)	- Copia dei verbali rilasciati dalle autorità pubbliche; - elenco delle verifiche/visite effettuate e delle richieste formulate dalla Amministrazione competente	Annuale
Procedimento di negoziazione	- Lista dei progetti in fase di negoziazione - Copia delle convenzioni sottoscritte	Annuale
Project management	- Lista delle richieste di varianti su convenzioni / contratti in corso	Annuale
Richieste di autorizzazioni/licenze	- Elenco delle richieste di autorizzazioni/licenze; - Copia della documentazione inviata alla PA	Semestrale
Assunzione del personale	- Lista delle assunzioni; - Descrizione del procedimento - Composizione delle commissioni di	Annuale

	selezione	
Contenziosi giudiziari	- elenco dei contenziosi attivi e passivi con indicazione del relativo oggetto, dello stato del contenzioso, dei relativi avvocati incaricati e delle parcelle pattuite/ corrisposte	Annuale
Gestione dell'omaggistica/ donazioni/ sponsorizzazioni	- Elenco omaggi; donazioni; sponsorizzazioni	Annuale
Acquisto di beni e servizi	Per ogni acquisto: lista dei preventivi esaminati Lista dei fornitori (ultimi 2 anni, a scorrimento) con indicazione di - data contratti - tipologia merceologica - importo - modalità selezione del fornitore	Semestrale
Gestione tesoreria e movimenti finanziari	- Copia dell'estratto conto semestrale dei c/c attivi; - Copia delle fatture relative a pagamenti importanti (> 250.000 euro)	Semestrale
Incarichi di consulenza e collaborazione	Lista, su base nominativa, di tutti i destinatari di nuovi contratti di consulenza e collaborazione assegnati nel periodo di osservazione (a partire dal 1/1/2014) evidenziando - Oggetto - Importo - Periodo contrattuale - Centro di costo - Composizione commissione di selezione - Eventuali rinnovi Copia dei contratti di consulenza assegnati per l'area amministrativa	semestrale
Procedimenti di gara	Prospetto di sintesi relativo ai bandi espletati nel periodo di osservazione: - richiedente, - oggetto del bando - composizione della commissione di gara, - aziende aggiudicatarie - importo di aggiudicazione	semestrale
Gestione del personale	Provvedimenti disciplinari comminati (a partire dal 1/ 1 / 2009)	annuale

6 DEFINIZIONI

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

Pubblica amministrazione : l'insieme degli organi e delle attività preordinati al perseguimento di compiti o scopi di pubblico interesse in una determinata collettività statale. Tali soggetti giuridici svolgono attività legislativa, giurisdizionale o amministrativa in forza di norme di diritto pubblico e di atti autoritativi.
Nel sistema amministrativo italiano, accanto allo Stato esistono svariati soggetti giuridici (i cosiddetti enti pubblici) che esplicano funzioni e compiti amministrativi ([3]).

Autorità Pubbliche di Vigilanza: enti nominativamente individuati per legge, dotati di particolare autonomia e imparzialità, preposti alla tutela di alcuni interessi di rilievo costituzionale, tra i quali la vigilanza sui Contratti Pubblici, la tutela della sfera di Riservatezza professionale e personale, la libertà di Concorrenza, la tutela dei Mercati Finanziari, ecc..

Pubblico servizio : un'attività disciplinata da norme diritto pubblico, ma caratterizzata dalla mancanza da poteri di natura deliberativa, autorizzativi e certificativi (tipici della Pubblica funzione amministrativa). In questo senso lo svolgimento di semplici mansioni di ordine né la prestazione di opera meramente materiale non può mai costituire Pubblico servizio.

Pubblici ufficiali : Agli effetti della legge penale (art. 357 c.p.), sono pubblici ufficiali coloro i quali esercitano 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 e dal suo svolgersi per mezzo di poteri autoritativi e certificativi.
La L. 181/1992 ha ulteriormente ampliato il concetto di funzione pubblica: È pubblico ufficiale anche chi concorre in modo sussidiario o accessorio all'attuazione dei fini della pubblica amministrazione, con azioni che non possano essere isolate dal contesto delle funzioni pubbliche (Cass. Pen., Sez. VI, 85/172191).
Sono pubblici ufficiali coloro che:
• concorrono a formare la volontà di una pubblica amministrazione;
• sono muniti di poteri:
- ✓ decisionali;
- ✓ di certificazione;
- ✓ di attestazione;
- ✓ di coazione (Cass. Pen. Sez. VI 81/148796);
- ✓ di collaborazione, anche saltuaria (Cass. Pen. Sez. VI n. 84/166013).

[3] A titolo puramente esemplificativo si citano :
- istituti e scuole di ogni ordine e grado e le istituzioni educative;
- enti ed amministrazioni dello Stato ad ordinamento autonomo (quali, ad esempio, Ministeri, Camera e Senato, Dipartimento Politiche Comunitarie, Autorità Garante della Concorrenza e del Mercato, Autorità per l'Energia Elettrica ed il Gas, Autorità per le Garanzie nelle Comunicazioni, Banca d'Italia, Consob, Autorità Garante per la protezione dei dati personali, Agenzia delle Entrate, ISVAP, COVIP, sezioni fallimentari);
- Regioni;
- Province;
- Partiti politici ed associazioni loro collegate;
- Comuni e società municipalizzate;
- Comunità montane, loro consorzi e associazioni;
- Camere di Commercio, Industria, Artigianato e Agricoltura, e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali (quali, ad esempio, INPS, CNR, INAIL, INPDAI, INPDAP, ISTAT, ENASARCO);
- ASL;
- Enti e Monopoli di Stato;
- Soggetti di diritto privato che esercitano pubblico servizio (ad esempio, la RAI);
- Fondi pensione o casse di assistenza loro collegati;
- Fondazioni di previdenza ed assistenza.

Ai sensi dell'articolo n. 357, comma 1, c.p., è considerato pubblico ufficiale "agli effetti della legge penale" colui il quale esercita "una pubblica funzione legislativa, giudiziaria o amministrativa".
Il secondo comma dell'articolo in esame precisa che, agli effetti della legge penale "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".
Può essere utile ricordare che assumono la qualifica di pubblici ufficiali non solo i soggetti al vertice politico amministrativo dello Stato o di enti territoriali, ma anche tutti coloro che, in base allo statuto, nonché alle deleghe che esso consente, ne formino legittimamente la volontà e/o la portino all'esterno in forza di un potere di rappresentanza.

Pur anticipando la discussione sulle tipologie di reato nei rapporti con la PA riportata nel capitolo 3, si fa presente che i reati che possono essere commessi solo da o verso i " pubblici ufficiali " sono :

- ✓ concussione (art 317 c.p.)
- ✓ corruzione per l'esercizio della funzione (art 318 c.p.)
- ✓ corruzione per atto contrario ai doveri d'ufficio (art 319 c.p.)
- ✓ corruzione in atti giudiziari (art 319-ter c.p.)
- ✓ induzione indebita a dare o promettere utilità (art 319-quater c.p.)
- ✓ istigazione alla corruzione (art 322 c.p.)
- ✓ peculato, concussione, corruzione e istigazione alla corruzione dei membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (art 322-bis c.p.)

Incaricato di pubblico servizio : chi, pur non essendo propriamente un pubblico ufficiale con le funzioni proprie di tale status (certificative, autorizzative o deliberative), svolge un servizio di pubblica utilità presso organismi pubblici in genere. In particolare, « agli effetti della legge penale (Art. 358 c.p,) sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio, secondo la definizione riportata in precedenza.
Esempi di incaricati di pubblico servizio sono: i dipendenti delle autorità di vigilanza che non concorrono a formare la volontà dell'autorità e che non hanno poteri autoritativi, i dipendenti degli enti che svolgono servizi pubblici anche se aventi natura di enti privati, gli impiegati degli uffici pubblici, …
Il legislatore ha precisato che non può mai costituire "servizio pubblico" lo svolgimento di "prestazioni di opera meramente materiale"
Con riferimento alle attività che vengono svolte da soggetti privati in base ad un rapporto concessorio con un soggetto pubblico, si ritiene che, ai fini della definizione come servizio pubblico dell'intera attività svolta nell'ambito di tale rapporto concessorio, è necessario accertare se le singole attività che vengono in questione siano a loro volta soggette ad una disciplina di tipo pubblicistico.
In sostanza la giurisprudenza ha individuato la categoria degli incaricati di pubblico servizio nei soggetti che danno un contributo concreto alla realizzazione delle finalità del pubblico servizio, con connotazione di sussidiarietà e di complementarietà rispetto all'attività pubblica in senso stretto, esercitando di fatto una funzione pubblica.
Elemento discriminante per indicare se un soggetto riveste o meno la qualifica di incaricato di pubblico servizio è rappresentato non dalla natura giuridica assunta o detenuta dall'ente, ma dalle funzioni affidate al soggetto, le quali devono consistere nella cura di interessi pubblici o nel soddisfacimento di bisogni di interesse generale.

Di nuovo, anticipando la discussione sulle tipologie di reato nei rapporti con la PA riportata in Allegato 1.A, si fa presente che possono essere ascritti agli "incaricati di pubblico servizio" i seguenti reati :

- ✓ corruzione per l'esercizio della funzione (art 318 c.p.)
- ✓ corruzione per atto contrario ai doveri d'ufficio (art 319 c.p.)
- ✓ corruzione in atti giudiziari (art 319-ter c.p.)
- ✓ induzione indebita a dare o promettere utilità (art 319-quater c.p.)
- ✓ istigazione alla corruzione (art 322 c.p.)
- ✓ peculato, concussione, corruzione e istigazione alla corruzione dei membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati esteri (art 322-bis c.p.)

PARTE SPECIALE B : REATI SOCIETARI

1 AMBITO APPLICATIVO ED OBIETTIVI

La presente Parte Speciale riguarda i reati societari, contemplati all'art. 25 ter del D. Lgs. n. 231/2001.

In particolare, per i reati di seguito descritti, "*se commessi nell'interesse della società, da amministratori, direttori generali o liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si fosse realizzato se essi avessero vigilato in conformità agli obblighi inerenti alla loro carica*", trova applicazione il sistema sanzionatorio di carattere pecuniario previsto nell'art. 25 ter del D. Lgs n. 231/2001, qualora sia rilevata l'inesistenza del Modello di organizzazione, gestione e controllo ed il mancato rispetto degli obblighi di vigilanza.

2 LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati *ex* art. 5 del d.lgs. n. 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.
Si riporta, pertanto, di seguito una descrizione schematica dei reati richiamati dall'art. 25-ter (*Reati societari*) del d.lgs. n. 231/2001.

Una discussione più puntuale degli stessi reati è riportata in Allegato 1.B .

2.1 False comunicazioni e prospetti

False comunicazioni sociali (artt. 2621 e 2622 c.c.)
Questo reato si realizza tramite l'esposizione nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, di fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene con l'intenzione di ingannare i soci o il pubblico; ovvero tramite l'omissione, con la stessa intenzione, di informazioni sulla situazione medesima la cui comunicazione è imposta dalla legge.

2.2 Frodi

Aggiotaggio (art. 2637 c.c.)
La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari, quotati o non quotati, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.

2.3 Operazioni sul capitale sociale e sul patrimonio della società,

Formazione fittizia del capitale (art. 2632 c.c.)
Tale reato può consumarsi quando: viene formato o aumentato fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali in misura complessivamente superiore all'ammontare del capitale sociale; vengono sottoscritte reciprocamente azioni o quote; vengono sopravvalutati in modo rilevante i conferimenti dei beni in natura, i crediti ovvero il patrimonio della società, nel caso di trasformazione.

Indebita restituzione dei conferimenti (art. 2626 c.c.)
La "condotta tipica" prevede, fuori dei casi di legittima riduzione del capitale sociale, la restituzione, anche simulata, dei conferimenti ai soci o la liberazione degli stessi dall'obbligo di eseguirli.

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.

Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.)
Questo reato si perfeziona con l'acquisto o la sottoscrizione, fuori dei casi consentiti dalla legge, di azioni o quote sociali o della società controllante che cagioni una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.

Operazioni in pregiudizio dei creditori (art. 2629 c.c.)
La fattispecie si realizza con l'effettuazione, in violazione delle disposizioni di legge a tutela dei creditori, di riduzioni del capitale sociale o fusioni con altra società o scissioni, che cagionino danno ai creditori.

Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)
Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessario a soddisfarli, che cagioni un danno ai creditori.

2.4 Illeciti nel funzionamento della società e degli organi sociali

Illecita influenza sull'assemblea (art. 2636 c.c.)
La "condotta tipica" prevede che si determini, con atti simulati o con frode, la maggioranza in assemblea allo scopo di conseguire, per sé o per altri, un ingiusto profitto.

Impedito controllo (art. 2625 c.c.)
Il primo comma dell'art. 2625 c.c. prevede un illecito amministrativo proprio degli amministratori, consistente nell'impedimento delle funzioni di controllo attribuite ai soci o agli organi sociali. L'illecito amministrativo non genera la responsabilità diretta dell'Ente, che invece è prevista per l'ipotesi delittuosa, contemplata dal secondo comma dello stesso art. 2625 c.c., che è integrato quando dalla condotta di impedimento derivi un danno ai soci.
La condotta punibile consiste nell'occultamento di documentazione, ovvero nella realizzazione di altri artifici idonei alla produzione dei due eventi costitutivi del reato (impedito controllo o impedita revisione). Si noti ancora che la norma comprende tra le forme di manifestazione della condotta vietata anche il semplice ostacolo, il che estende l'area del divieto sino al mero ostruzionismo .

2.5 Ostacoli alle funzioni di vigilanza

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 valutazioni, sulla situazione economica, patrimoniale o finanziaria dei soggetti sottoposti alla vigilanza; ovvero attraverso l'occultamento con altri mezzi fraudolenti, in tutto o in parte, di fatti che avrebbero dovuto essere comunicati, concernenti la situazione medesima.

La condotta criminosa si realizza, altresì, quando siano, in qualsiasi forma, anche mediante omissione delle comunicazioni dovute, intenzionalmente ostacolate le funzioni delle autorità di vigilanza.

Nel caso di reati fiscali, laddove l'unico soggetto cui si intende recare danno con il falso in bilancio sia il Fisco (ad esempio, occultamento di ricavi), per pacifica interpretazione - sorretta anche dalla Relazione ministeriale al d.lgs. 11 aprile 2002, n. 61 (modificativo dei reati societari) - le false comunicazioni sociali (che darebbero luogo alla responsabilità della persona giuridica) non si verificano e sussiste soltanto il reato fiscale (che, invece, non costituisce base per tale tipo di responsabilità).

3 LE ATTIVITAôSENSIBILI AI FINI DEL D.LGS. 231/2001

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'individuazione delle attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-*ter* del d.lgs. n. 231/2001, è stata ottenuta attraverso l'analisi puntuale dei processi della Società (così come riportati in All. A della Parte Generale del Modello) , individuando quelle condotte astrattamente ipotizzabili che determinerebbero la commissione dei reati previsti dal Decreto. L'individuazione puntuale dei processi a rischio è riportata in Allegato 2.B al presente documento.

Le attività sensibili individuate attraverso tale processo sono, pertanto:

1. ***Gestione rapporti con le autorità di controllo della Regione Puglia***
2. ***Gestione rapporti con Società di revisione***
3. ***Attuazione obblighi di trasparenza***
4. ***Rapporti con organi di informazione***
5. ***Gestione archivi aziendali cartacei***
6. ***Formazione del bilancio***

4 PROTOCOLLI PER LA FORMAZIONE E LôATTUAZIONE DELLE DECISIONI E SISTEMA DI CONTROLLO

4.1 Principi specifici di comportamento

I seguenti principi di comportamento si applicano ai Destinatari che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto ai reati societari di cui all'art. 25 ter del D.Lgs. 231/2001.

Le condotte di ordine generale descritte integrano e non sostituiscono i principi previsti dal Codice Etico, nonché le eventuali procedure di maggiore tutela previste all'interno di InnovaPuglia e relative alle attività sensibili.

In via generale, ai Destinatari è fatto **obbligo** di:

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire al Socio e al pubblico un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria;
- 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;
- assicurare il regolare funzionamento della Società e dei suoi organi sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge;
- effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità Pubbliche di Vigilanza, non ostacolando l'esercizio delle funzioni di vigilanza da queste intraprese;
- tenere un comportamento corretto e veritiero con gli organi di stampa e di informazione;
- garantire il rispetto delle regole comportamentali previste nel Codice Etico, con particolare riguardo all'esigenza di assicurare che ogni operazione e transazione sia correttamente registrata, autorizzata, verificabile, legittima, coerente e congrua;
- astenersi dal compiere qualsivoglia operazione o iniziativa qualora vi sia una situazione di conflitto di interessi, ovvero qualora sussista, anche per conto di terzi, un interesse in conflitto con quello della Società;

È fatto espresso **divieto** ai Destinatari di:

- rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilancio, nelle relazioni o nelle altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti al vero, ovvero predisporre comunicazioni sociali che non rappresentino in modo veritiero la situazione economica, patrimoniale e finanziaria della Società;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della Società;
- restituire conferimenti o liberare dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale;
- ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva;
- effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno;
- porre in essere comportamenti che impediscano, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, ovvero ostacolino lo svolgimento dell'attività di controllo da parte del socio ovvero del Collegio Sindacale e della Società di revisione

4.2 Protocolli Specifici

4.2.1 Gestione rapporti con le autorità di controllo della Regione Puglia

Processi di interesse	
Procedure/ regolamenti applicabili	*PRQ GEN 07 "Adempimenti funzionali al monitoraggio conformemente alla DGR n. 812/2014",* in fase di approvazione
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ Formalizzazione del soggetto incaricato di gestire il rapporto con i servizi regionali di controllo ✓ nella predisposizione della documentazione prevista dalla DGR 812/2014, occorre operare con la massima diligenza e professionalità in modo da fornire informazioni chiare, accurate, complete, fedeli e veritiere ✓ i soggetti incaricati di gestire il rapporto con i servizi regionali di controllo, in attuazione della DGR 812/2014, verificano la documentazione predisposta dal personale operativo e provvedono all'inoltro telematico secondo la procedura PRQ GEN07 ✓ Separazione tra il personale responsabile di gestire il rapporto con le strutture regionali di controllo (es: inviando la documentazione prevista) e gli uffici che producono i relativi atti

4.2.2 Gestione rapporti con Società di revisione

Processi di interesse	
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ identificazione del soggetto preposto alla trasmissione della documentazione alla società di revisione legale ✓ verifica del rispetto dei requisiti di indipendenza dei revisori dai vertici sociali, così come richiamato dal D.Lgs 27 gennaio 2010 n. 39 (Decreto sulla Revisione legale) ✓ possibilità per il responsabile della società di revisione legale di prendere contatto con l'OdV per verificare congiuntamente situazioni che possano presentare aspetti di criticità in relazione alle ipotesi di reato considerate; ✓ divieto di attribuire, alla società di revisione o ad altre società appartenenti alla medesima rete nonché ai soci, gli amministratori, i

	componenti degli organi di controllo e i dipendenti della società di revisione stessa e delle società da essa controllate, ad essa collegate o che la controllano o sono sottoposte a comune controllo, alcuno dei seguenti servizi alla Società: - tenuta dei libri contabili e altri servizi relativi alle registrazioni contabili o alle relazioni di bilancio; - progettazione e realizzazione dei sistemi informativi contabili; - servizi di valutazione e stima ed emissione di pareri *pro veritate*; - servizi attuariali; - gestione esterna dei servizi di controllo interno; - consulenza e servizi in materia di organizzazione aziendale diretti alla selezione, formazione e gestione del personale; - prestazione di difesa giudiziale; ✓ divieto di stipulare, con il responsabile della revisione legale, per conto della società di revisione incaricata, contratti di lavoro autonomo o subordinato aventi ad oggetto funzioni dirigenziali di rilievo se non sia decorso almeno un biennio dalla conclusione dell'incarico ovvero dal momento in cui abbia cessato di essere socio, amministratore o dipendente della società di revisione

4.2.3 Attuazione obblighi di trasparenza

Processi di interesse	
Procedure/ regolamenti applicabili	✓ *Programma Triennale per la Trasparenza e l'Integrità*
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ segregazione tra i responsabili della immissione dei dati nel portale Amministrazione Trasparente (secondo quanto previsto dal Programma Triennale) e il Responsabile della Trasparenza

4.2.4 Rapporti con organi di informazione

Processi di interesse	
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	

Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ lista di tutti i contatti con organi di stampa (testata giornalistica, oggetto, interlocutore,.,…)

4.2.5 Gestione archivi aziendali cartacei

Processi di interesse	
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ Adeguamento del livello di sicurezza fisica degli archivi cartacei, in modo omogeneo con la sicurezza delle infrastrutture IT

4.2.6 Formazione del bilancio

Processi di interesse	
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ predisposizione di procedure amministrative e contabili formalizzate relative al processo di formazione del bilancio di esercizio ✓ il responsabile di Divisione / Servizio deve rilasciare una dichiarazione di veridicità e completezza delle informazioni contabili e, in generale, delle altre informazioni rilevanti da lui trasmesse all'ufficio preposto alla materiale redazione del bilancio; ✓ il sistema informatico utilizzato per la trasmissione di dati e informazioni deve garantire la tracciabilità dei singoli passaggi e l'identificazione delle postazioni che inseriscono i dati nel sistema. Il responsabile di ciascuna Direzione/Servizio coinvolto nel processo deve garantire la tracciabilità di tutti i dati e le informazioni finanziarie

	✓ ogni modifica ai dati contabili deve essere effettuata dalla sola Direzione/Servizio che li ha generati, garantendo la tracciabilità dell'operazione di modifica e previa formale autorizzazione del Direttore/Responsabile di servizio; non deve essere ammessa l'alterazione, da parte della funzione preposta alla formazione del bilancio, dei dati trasmessi dai Servizi ✓ qualora siano formulate ingiustificate richieste di variazione dei criteri di rilevazione, registrazione e rappresentazione contabile o di variazione quantitativa dei dati rispetto a quelli già contabilizzati in base alle procedure correnti, deve essere previsto che la funzione preposta informi tempestivamente l'Organismo di Vigilanza; ✓ predisposizione di una procedura periodica di ricognizione del patrimonio ✓ predisposizione di una modalità di raccolta e valorizzazione di informazioni su contenziosi già insorti o di possibile insorgenza ✓ prima della stesura finale del bilancio, deve essere tenuta almeno una riunione di scambio di informazioni e di valutazioni tra tutti i soggetti coinvolti nella funzione di controllo: collegio sindacale, società di revisione, organismo di vigilanza; ✓ tutti i documenti contabili relativi agli argomenti indicati nell'ordine del giorno delle riunioni del Consiglio di Amministrazione (e in particolare la bozza di bilancio) devono essere completi e messi a disposizione degli Amministratori con ragionevole anticipo rispetto alla data della riunione; ✓ devono essere previste regole formalizzate che identifichino ruoli e responsabilità, relativamente alla tenuta, conservazione e aggiornamento del fascicolo di bilancio dall'approvazione del Consiglio di Amministrazione al deposito e pubblicazione (anche informatica) dello stesso e alla relativa archiviazione

5 FLUSSI INFORMATIVI SPECIFICI VERSO LÕOdV

I controlli svolti dall'Organismo di Vigilanza sono diretti a verificare la conformità delle attività aziendali ai principi espressi nella presente Parte Speciale e, in particolare, alle procedure interne in essere ed a quelle che saranno adottate in futuro, in attuazione della presente Parte Speciale.

A tal fine l'Organismo di Vigilanza

- effettua periodicamente controlli a campione sulle attività connesse ai «processi sensibili», diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. In questa prospettiva, pur garantendo all'Organismo libero accesso a tutta la documentazione aziendale rilevante così come previsto nella Parte Generale, vengono, comunque garantiti, in maniera continuativa, i flussi informativi elencati di seguito in tabella

- può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello 231.

PROCESSO DA VERIFICARE	FLUSSO INFORMATIVO VERSO OdV	FREQUENZA
Operazioni societarie	- Informativa su operazioni societarie aventi carattere straordinario	annuale
Attuazione del sistema dei controlli / Supporto ai controlli da parte del socio Regione Puglia	- copia delle informative inviate alla Regione ai sensi della DGR 812/2014	semestrale
Attuazione del sistema dei controlli / Controlli di Revisione legale da Società di Revisione	- informativa di ogni incarico conferito o che si intende conferire (diverso dalla revisione del bilancio) alla società di revisione o a società collegata a questa;	Annuale e quando si verifica
Attuazione del sistema dei controlli / Certificazione dei sistemi di gestione	- Documentazione dell'iter di aggiudicazione dell'incarico a società di certificazione	Annuale e quando si verifica
Predisposizione del bilancio	- Osservazioni effettuate dal Collegio Sindacale in merito al Bilancio di esercizio; - Osservazioni della Società di Revisione	Annuale
Verifica del sistema delle deleghe	- Copia del verbale di conferimento dei poteri; - copia delle procure	Annuale

6 DEFINIZIONI

Reati propri : a differenza dei **reati comuni,** caratterizzati dal fatto che chiunque ne può essere l'autore, i **reati propri** necessitano, in capo all'autore, il possesso di specifiche qualità personali.

PARTE SPECIALE C : REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME COMMESSI CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO

1 AMBITO APPLICATIVO ED OBIETTIVI

L'entrata in vigore della Legge 3 agosto 2007 n° 123 ha modificato il D. Lgs 231/2001 con l'inserimento dell'art. 25-*septies* che introduce la responsabilità amministrativa della Società nel caso di reati di omicidio colposo e lesioni gravi e gravissime di cui agli artt. 589 c.p. (omicidio colposo) e 590, terzo comma c.p. (lesioni personali colpose gravi o gravissime), commessi con **violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro** (**TU Sicurezza**, approvato con il Decreto Legislativo 81/2008, attuativo della delega di cui all'articolo 1 della legge 3 agosto 2007 n. 123 in materia di tutela della salute e sicurezza nei luoghi di lavoro, modificato dal Decreto Legislativo 3 agosto 2009, n. 106 "Disposizioni integrative e correttive del decreto legislativo 9 aprile 2008, n. 81, in materia di tutela della salute e della sicurezza nei luoghi di lavoro")

Le condotte penalmente rilevanti consistono nel fatto, da chiunque commesso, di cagionare la morte o lesioni gravi/gravissime al lavoratore, per effetto dell'inosservanza di norme antinfortunistiche. In linea teorica, soggetto attivo dei reati può essere chiunque sia tenuto ad osservare o far osservare la norme di prevenzione e protezione. Tale soggetto può quindi individuarsi, ai sensi del decreto 81/2008, nei datori di lavoro, nei dirigenti, nei preposti, nei soggetti destinatari di deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro, nonché nei medesimi lavoratori.

Con l'art. 25-*septies* si introduce per la prima volta una responsabilità amministrativa dell'ente per reati colposi (i.e. omicidio colposo e lesioni personali colpose) in contrapposizione a quella derivante dalle altre fattispecie delittuose richiamate dal D.Lgs. 231/2001 fondate, invece, sull'elemento soggettivo del dolo (tipicamente riconducibile ad una decisione). In questo senso, il vantaggio e/o interesse dell'ente si configura per il solo fatto che i presìdi e le misure previsti dalla normativa sulla tutela della salute e sicurezza sul lavoro non sono stati (adeguatamente) implementati, determinando, in tal modo, un vantaggio economico indiretto per l'ente (es: spese per i consulenti e/o messa a norma in sicurezza degli impianti e/o delle strutture). Il legislatore ha ritenuto quindi di poter individuare la fonte di tale colpevolezza della persona giuridica in una sorta di "colpa di organizzazione", ritenendo cioè che l'ente debba essere chiamato a rispondere dell'illecito commesso da determinate persone fisiche quando alcune lacune e manchevolezze nell'organizzazione della sua attività abbiano consentito ad altri soggetti di tenere condotte delittuose.

Di fatto l'inserimento dell'art 25-*septies* fa sì che in caso di incidente, oltre che nelle responsabilità di matrice civile e penale tipiche della materia, la Società incorre anche nelle ulteriori sanzioni del decreto 231 del 2001 ove non abbia predisposto ed efficacemente attuato un idoneo Modello di Organizzazione, Gestione e Controllo.
Di contro, nel caso di un incidente, la responsabilità del datore di lavoro e dell'ente non sussiste nei casi in cui il lavoratore rimanga vittima di uno dei reati richiamati dall'art. 25-*septies* qualora la condotta di quest'ultimo non abbia rispettato gli standard generali di prudenza e possa essere definita come abnorme (non conforme), in relazione alle mansioni assegnate e alle modalità di esecuzione delle stesse.

Stando la complessità della materia e l'ampia rete di disposizioni normative che già regola il settore della sicurezza sul lavoro, è opportuno chiarire il nesso tra il D.Lgs 81/2008 (Testo Unico per la normativa antinfortunistica) e il D.Lgs 231/01.

Il D.Lgs 81/2008 mira direttamente a prevenire gli infortuni e le malattie sviluppate nei luoghi di lavoro e a contrastare quelle pratiche (comportamenti e omissioni) che ne incrementano le probabilità di accadimento e l'impatto derivante. Il Decreto, in quanto normativa cogente, contiene misure vincolanti per i destinatari, obbligati a conformarsi alle sue disposizioni ai fini della tutela della salute e sicurezza negli ambienti di lavoro.

Il programma di prevenzione dei rischi-reato ex D.Lgs. 231/01 è senza dubbio prevalentemente ed essenzialmente un *compliance program* teso, appunto, a gestire i rischi di non conformità: la conformità ai requisiti di cui al D.Lgs. 231/01, in sé non obbligatoria, pone l'azienda nella condizione di poter ricevere il beneficio dell'esimente (non essere chiamati a rispondere dei reati commessi) o la riduzione dell'afflittività delle sanzioni previste dal Decreto 231 stesso. In questo senso la presente Parte Speciale si integra, non si sovrappone e non si sostituisce al sistema di gestione della salute e sicurezza nei luoghi di lavoro adottato dall'azienda a cui è demandata la predisposizione puntuale delle misure di prevenzione degli infortuni e delle malattie (controllo di

primo livello) conformemente alla normativa corrente. Le misure previste in questa Parte Speciale mettono piuttosto l'Organismo di Vigilanza nelle condizioni di svolgere un controllo di secondo livello sul rispetto della normativa.

2 LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

Le fattispecie di reato "presupposto" della responsabilità amministrativa della Società ai sensi dell' art. 25-*septies* sono*:*

Omicidio colposo (art. 589 c.p.)

Lesioni personali colpose (art. 590 c.p.)

La natura del reato è **colposa** ovverosia manca nel soggetto attivo l'intenzionalità dell'evento lesivo che tuttavia si realizza a seguito della sua negligenza, imperizia, imprudenza (colpa generica) o per l'inosservanza di leggi e regolamenti (colpa specifica). Un esempio potrebbe essere dato dal caso in cui un dipendente omette di comunicare l'avvenuto danneggiamento di un dispositivo di produzione: laddove tale danneggiamento produca un incidente, l'omessa comunicazione si trasforma in reato (colposo).

La condotta negligente dell'ente che, omettendo di implementare le norme poste a tutela della sicurezza del lavoratore (attraverso per esempio la mancata valutazione dei rischi aziendali e/o della nomina del responsabile interno per la sicurezza), abbia arrecato una lesione al soggetto passivo può costituire il presupposto per l'insorgere di responsabilità *ex* D.Lgs. 231/2001.

Un maggior approfondimento delle suddette fattispecie di reato è riportato in Allegato 1.C

3 LE ATTIVITAôSENSIBILI AI FINI DEL D.LGS. 231/2001

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.
Ai fini della individuazione delle attività sensibili, nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25 - *septies* del d.lgs. 231/2001, occorre fare riferimento a quanto stabilito dall'art 30 del D.Lgs 81/2008 che definisce la caratteristiche di un modello di organizzazione e gestione per avere valore esimente rispetto alle tematiche della salute e sicurezza sul lavoro. In particolare l'art 30 recita :

1. Il modello di organizzazione e di gestione idoneo ad avere efficacia esimente della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica di cui al decreto legislativo 8 giugno 2001, n. 231, deve essere adottato ed efficacemente attuato, assicurando un sistema aziendale per l'adempimento di tutti gli obblighi giuridici relativi a :

(i) rispetto degli standard tecnico-strutturali relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;

(ii) attività di valutazione dei rischi e predisposizione delle misure di prevenzione e protezione conseguenti;

(iii) attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
(iv) attività di sorveglianza sanitaria;
(v) attività di informazione e formazione dei lavoratori;
(vi) attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
(vii) acquisizione di documentazioni e certificazioni obbligatorie per legge;
(viii) periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

2. Il modello organizzativo e gestionale di cui al comma 1 deve prevedere idonei sistemi di registrazione dell'avvenuta effettuazione delle attività di cui al comma 1.

3. Il modello organizzativo deve in ogni caso prevedere, per quanto richiesto dalla natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

4. Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

5. In sede di prima applicazione, i modelli di organizzazione aziendale definiti conformemente alle Linee guida UNI-INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) del 28 settembre 2001 o al British Standard OHSAS 18001:2007 si presumono conformi ai requisiti di cui al presente articolo per le parti corrispondenti. Agli stessi fini ulteriori modelli di organizzazione e gestione aziendale possono essere indicati dalla Commissione di cui all'articolo 6.

5-bis. La commissione consultiva permanente per la salute e sicurezza sul lavoro elabora procedure semplificate per la adozione e la efficace attuazione dei modelli di organizzazione e gestione della sicurezza nelle piccole e medie imprese. Tali procedure sono recepite con decreto del Ministero del lavoro, della salute e delle politiche sociali.

A fronte di tale impostazione metodologica è stata svolta l'analisi puntuale dei processi della Società (così come riportati in All. A della Parte Generale del Modello), individuando quelle condotte astrattamente ipotizzabili che determinerebbero la commissione dei reati previsti dal Decreto. L'individuazione puntuale dei processi a rischio è riportata in Allegato 2.C al presente documento. Le attività sensibili individuate sono, pertanto:

1. Gestione attrezzature, impianti e luoghi di lavoro

Processi di interesse :
- Gestione degli asset (attrezzature, ambienti di lavoro, impiantistica) : verifiche periodiche, manutenzione, adeguamenti
- gestione fisica delle infrastrutture : inventariazione
- ottenimento certificazioni in materia di sicurezza e igiene sul lavoro

2.Valutazione dei rischi e predisposizione delle misure di prevenzione e protezione conseguenti

Processi di interesse :
- redazione del DVR
- redazione dei piani di emergenza & definizione delle procedure interne in tema di salute, sicurezza e igiene sul lavoro
- gestione DPI
- sorveglianza sanitaria
- rapporti con i fornitori: adeguamento clausole contrattuali (DUVRI) & verifica adempimenti di competenza dell'affidatario (DURC, POS,..)

3. Organizzazione per la salute e sicurezza

Processi di interesse : - definizione dell'organigramma per la sicurezza / assegnazione delle deleghe
- consultazione dei rappresentanti dei lavoratori per la sicurezza

4. Informazione e formazione

Processi di interesse : - formazione dei lavoratori in tema di salute, sicurezza e igiene sul lavoro

5. Vigilanza su rispetto delle procedure e delle istruzioni operative

6. Verifica della applicazione e della efficacia del modello adottato e sul mantenimento nel tempo delle condizioni di idoneità

Processi di interesse : - monitoraggio infortuni/ tenuta registro infortuni e malattie professionali
- gestione rapporti con VVF, ASL, INAIL,..

4 PROTOCOLLI PER LA FORMAZIONE E LôATTUAZIONE DELLE DECISIONI E SISTEMA DI CONTROLLO

Il presente Protocollo ha lo scopo di definire i principi comportamentali e i principi di controllo specifico a cui tutto il personale di InnovaPuglia si attiene nel processo di gestione degli adempimenti in materia di salute e sicurezza del personale e di tutti coloro che abbiano accesso ai relativi ambienti di lavoro.
Il "Modello" non intende sostituirsi ai compiti ed alle responsabilità disciplinate dal D. Lgs. n. 81/2008, ma si integra con esso, intende costituire un ulteriore presidio di controllo e verifica della esistenza, efficacia ed adeguatezza della struttura e dell'organizzazione posta in essere da InnovaPuglia in ossequio alla normativa in materia di scurezza e salute dei lavoratori.

4.1 Principi specifici di comportamento

Tutti i Destinatari del Modello adottano regole di condotta conformi ai principi contenuti nel Codice Etico della Società, nel D.Lgs. 81/2008 e nella normativa vigente in materia di antinfortunistica, tutela della sicurezza e della salute nei luoghi di lavoro, al fine di prevenire il verificarsi di reati quali l'omicidio e le lesioni colposi.

Tutti i destinatari del Modello devono quindi
- considerare sempre prevalente la necessità di tutelare la salute e la sicurezza dei dipendenti e dei terzi eventualmente presenti rispetto a qualsiasi considerazione economica;
- contribuire, per quanto di propria competenza, all'adempimento degli obblighi previsti a tutela della salute e della sicurezza sui luoghi di lavoro;
- valutare sempre gli effetti delle proprie condotte in relazione al rischio di infortuni sul lavoro;

Per un'effettiva prevenzione dai rischi ed in conformità anche agli adempimenti prescritti dalla normativa in materia di sicurezza sul lavoro, è fatta espressa richiesta:

- al **Datore di lavoro** di compiere le funzioni rimessegli dalla normativa antinfortunistica vigente (D.Lgs. n. 81/2008 e s.m.i.) secondo il sistema di deleghe e procure definito formalmente da InnovaPuglia in detta materia, vigilando affinché il proprio delegato eserciti i compiti e le attribuzioni affidategli. Va tenuto presente che, ai sensi dell'art 17 dello stesso decreto, il datore di lavoro non può delegare le seguenti attività:
  a) valutazione di tutti i rischi con la conseguente elaborazione del documento previsto dall'art. 28;
  b) designazione del responsabile del servizio di prevenzione e protezione dai rischi.

- al **Responsabile del Servizio di Prevenzione e Protezione** di rappresentare tempestivamente al Datore di lavoro le esigenze di aggiornamento del DVR in funzione delle modifiche normative sopravvenute, dello status organizzativo dell'Ente ovvero delle nuove tecnologie in detto specifico settore, nonché ogni altro compiti rientrante nel relativo incarico. Tale documento, infatti, deve essere soggetto a verifica periodica del permanere nel tempo della sua validità ed efficacia, con obbligo di adeguamento ogni qualvolta vi siano mutate o nuove situazioni di rischio derivanti da significative modifiche del processo produttivo o della organizzazione del lavoro, ovvero derivanti dall'evoluzione delle tecnologie, della prevenzione o della protezione o, ancora, a seguito di infortuni significativi o quando i risultati della sorveglianza sanitaria ne evidenzino la necessità;
- ai **preposti** di vigilare sulla corretta osservanza, da parte di tutti i lavoratori, delle misure e delle procedure di sicurezza aziendali, segnalando eventuali carenze o disallineamenti rispetto alle norme di buona tecnica e di sicurezza, eventuali situazioni di pericolo che si verificassero durante il lavoro, ovvero comportamenti non conformi agli obblighi di legge per gli opportuni conseguenti provvedimenti;
- alle altre **figure chiave designate dalla Società** ai sensi del D.Lgs. n. 81/2008 e s.m.i. (es. gli Incaricati dell'attuazione delle misure di prevenzione incendi, lotta antincendio, evacuazione dei lavoratori in caso di pericolo; gli addetti al primo soccorso; il rappresentante per la Sicurezza dei Lavoratori) di svolgere, ciascuno nell'ambito delle proprie competenze e attribuzioni, i compiti specificamente previsti dal citato decreto, in ogni caso attenendosi scrupolosamente alle disposizioni dell'Ente in materia di salute e sicurezza sul lavoro;
- a **tutti i dipendenti** di aver cura della propria sicurezza e salute e di quella dei propri colleghi ed anche di ogni altra persona presente negli ambienti di lavoro di InnovaPuglia, con obbligo – pena anche l'irrogazione di provvedimenti disciplinari, di:
  - ✓ prendere parte alla formazione erogata da InnovaPuglia ed alle visite mediche periodiche previste in funzione della mansione svolta dal protocollo sanitario;
  - ✓ evitare comportamenti imprudenti, incauti, negligenti rispetto alle disposizioni della Società in materia di salute e sicurezza sul lavoro e della formazione ricevuta;
  - ✓ collaborare attivamente con il Datore di lavoro, l'RSPP, i preposti e ogni altra figura chiave del sistema, mediante comportamenti prudenti e responsabili, ad un corretto ed efficace sistema di gestione della sicurezza sul lavoro.

Nello specifico, per i soggetti precedentemente specificati vengono indicate le relative responsabilità:

Divieti

La presente Parte Speciale prevede l'espresso divieto – a carico degli Esponenti Aziendali, in via diretta, ed a carico dei Collaboratori esterni e Partner, tramite apposite clausole contrattuali – di:

- ✓ mettere in atto comportamenti tali da esporre InnovaPuglia ad una delle fattispecie di reato previste dall'art. 25-septies del d.Lgs 231/2001;
- ✓ mettere in atto comportamenti tali da favorire l'attuarsi di fattispecie di reato previste dall'art. 25-septies del d.Lgs 231/2001;
- ✓ omettere l'aggiornamento delle misure di prevenzione, in relazione a mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e della sicurezza sul lavoro ovvero in relazione al grado di evoluzione della tecnica, della prevenzione e della protezione;

- ✓ omettere l'adozione di misure appropriate affinché soltanto i lavoratori che abbiano ricevuto adeguate istruzioni possano accedere nelle zone che li espongono ad un rischio grave e specifico;
- ✓ emanare ordini di ripresa del lavoro, nonostante la persistenza di una situazione di pericolo grave ed immediato;
- ✓ omettere l'adozione di provvedimenti idonei ad evitare che le misure tecniche impiegate possano causare rischi per la salute della popolazione e danni all'ambiente esterno;
- ✓ omettere l'adozione di provvedimenti idonei ad evitare che le misure tecniche impiegate possano causare rischi per la salute della popolazione e danno all'ambiente esterno;
- ✓ omettere l'adozione di misure antincendio e di pronta evacuazione in caso di pericolo grave ed immediato.

Obblighi

La presente Parte Speciale prevede l'espresso obbligo a carico dei soggetti sopra indicati di:

- ✓ osservare le disposizioni e le istruzioni impartite da InnovaPuglia, ai fini della protezione collettiva ed individuale;
- ✓ utilizzare correttamente le apparecchiature, i mezzi di trasporto e le altre attrezzature di lavoro, nonché i dispositivi di sicurezza;
- ✓ utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;
- ✓ segnalare immediatamente al Responsabile del Servizio di Prevenzione e Protezione, le deficienze dei mezzi dispositivi di cui ai due punti che precedono, nonché le altre eventuali condizioni di pericolo di cui vengono a conoscenza, adoperandosi direttamente in caso di urgenza;
- ✓ non rimuovere o modificare senza autorizzazione o comunque compromettere i dispositivi di sicurezza o di segnalazione o di controllo;
- ✓ non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;
- ✓ rispettare le prescrizioni contenute nel Piano di Emergenza ed Evacuazione;
- ✓ rispettare le prescrizioni impartite dalla segnaletica di sicurezza nonché i contenuti delle procedure di sicurezza emergenza trasmesse dal Responsabile del Servizio di Prevenzione e Protezione anche attraverso la formazione di aula.

Le condotte di ordine generale sopra descritte integrano e non sostituiscono i principi previsti dal Codice Etico, nonché le eventuali procedure di maggiore tutela previste all'interno di InnovaPuglia e relative alle attività sensibili.

4.2 Protocolli Specifici

I protocolli per la formazione e l'attuazione delle decisioni e il relativo sistema di controllo fanno riferimento al citato art 30 del D.Lgs 81/2008 oltre che, ovviamente, alle linee guida per i modelli ex-D.Lgs 231/01. In tal senso i principi base a cui devono riferirsi i protocolli sono quelli della

- ✓ suddivisione e univoca attribuzione di ruoli e compiti;
- ✓ documentazione (protocolli, procedure) per l'individuazione di criteri, modalità operative e responsabilità;
- ✓ tracciabilità delle transazioni/operazioni a comprova dell'effettività del modello.

4.2.1 Gestione attrezzature, impianti e luoghi di lavoro

Processi di interesse	- Gestione degli asset (ambienti di lavoro, impiantistica) : verifiche periodiche, manutenzione, adeguamenti - gestione fisica delle infrastrutture : inventariazione - ottenimento certificazioni in materia di sicurezza e igiene sul lavoro

Procedure/ regolamenti applicabili	- Capitolato tecnico allegato al contratto di "global service"
Poteri autorizzativi e di firma rilevanti per l'attività	Referente del contratto (interfaccia Emmegiesse / InnovaPuglia) (solo ruolo di controllo)
Tracciabilità nel sistema informativo aziendale	- rapporti mensili di intervento (non informatizzati)
Ulteriori protocolli da adottare	✓ prevedere la formalizzazione e la gestione di uno scadenziario delle verifiche periodiche di adeguatezza e di integrità degli asset e di conformità ai requisiti normativi applicabili oltre che degli interventi di manutenzione ✓ creazione e aggiornamento della lista delle attrezzature

4.2.2 Valutazione dei rischi e predisposizione delle misure di prevenzione e protezione conseguenti

Processi di interesse	- redazione del DVR - redazione dei piani di emergenza & definizione delle procedure interne in tema di salute, sicurezza e igiene sul lavoro - gestione DPI - sorveglianza sanitaria - rapporti con i fornitori: adeguamento clausole contrattuali (DUVRI) & verifica adempimenti di competenza dell'affidatario (DURC, POS,..)
Procedure/ regolamenti applicabili	➢ Documento di Valutazione dei Rischi (DVR) ex-art 17 e 28 del D.Lgs 81/2008, sia per quei pericoli che possono causare eventi infortunistici a danno del lavoratore, quindi effetti di tipo "acuto", sia per la valutazione di quei pericoli che hanno come conseguenza le malattie professionali, quindi aspetti di igiene industriale, con effetti di tipo "cronico" ➢ Piano di Emergenza, predisposto in ottemperanza delle disposizioni di cui all'art. 5 del D. M. 10.03.1998 per i luoghi di lavoro
Poteri autorizzativi e di firma rilevanti per l'attività	IL DG è delegato a svolgere le funzioni di Datore di Lavoro ai sensi dell'art 16 del D.Lgs 81/08
Tracciabilità nel sistema informativo aziendale	- Piano di miglioramento del livello di sicurezza - Registro antincendio (a cura del "global service")
Ulteriori protocolli da adottare	✓ garantire la tracciabilità dell'avvenuto coinvolgimento del Medico Competente nel processo di identificazione dei pericoli e valutazione dei rischi; ✓ regolamentazione delle modalità operative per l'affidamento di compiti e mansioni ai lavoratori da parte del DDL. In particolare è necessario prevedere: i) i criteri di affidamento delle mansioni ai lavoratori in base alle capacità e alle condizioni degli stessi in rapporto alla loro salute e alla sicurezza e a quanto emerso dai risultati degli accertamenti

	sanitari eseguiti; ii) le modalità di pianificazione delle visite periodiche; iii) le misure organizzative per la partecipazione del Medico Competente e del RSPP nella valutazione dell'idoneità dei lavoratori alle specifiche mansioni; iv) la tracciabilità delle attività di assessment svolte a tale scopo; ✓ prevedere clausole contrattuali standard riguardanti i costi della sicurezza nei contratti di appalto. ✓ prevedere la formalizzazione delle attività di gestione, distribuzione e mantenimento in efficienza dei Dispositivi di Protezione Individuale (DPI). In particolare è necessario: i) definire le modalità per la verifica dei necessari requisiti quali resistenza, idoneità e mantenimento in buon stato di conservazione ed efficienza dei DPI; ii) prevedere la tracciabilità delle attività di consegna e verifica della funzionalità dei DPI;

4.2.3 Organizzazione per la salute e sicurezza

Processi di interesse	- definizione dell'organigramma per la sicurezza / assegnazione delle deleghe - consultazione dei rappresentanti dei lavoratori per la sicurezza
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	- DG delegato a svolgere le funzioni di Datore di lavoro -
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ Con riferimento all'organizzazione ed alle responsabilità in materia (Responsabile del Servizio Prevenzione e Protezione [RSPP] / Addetti del Servizio di Prevenzione e Protezione [ASPP] / Medico Competente / Incaricati Emergenze) prevedere i) definizione esplicita dei requisiti specifici coerenti alle disposizioni di legge in materia e necessari ad assicurare le competenze tecniche per la verifica, gestione e controllo del rischio ; ii) adeguato livello di tracciabilità delle verifiche svolte in ordine al possesso dei requisiti specifici; iii) tracciabilità della formale accettazione dell'incarico; ✓ Verifica che il sistema di deleghe di funzioni da parte del datore di lavoro risulti coerente con quanto previsto dalle disposizioni normative in materia, fatto particolare riferimento all'art. 16 del d.lgs. n. 81/2008. In particolare: (i) i delegati devono possedere tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;

	(ii) la delega deve attribuire tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate, nonché l'autonomia di spesa necessaria allo svolgimento delle predette funzioni ✓ prevedere una modalità di tracciabilità delle riunioni periodiche dei *rappresentanti dei lavoratori per la sicurezza* e adeguata diffusione delle risultanze delle riunioni all'interno dell'organizzazione.

4.2.4 Informazione e formazione

Processi di interesse	- formazione dei lavoratori in tema di salute, sicurezza e igiene sul lavoro
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	- attestati di partecipazione ai corsi di formazione e aggiornamento
Ulteriori protocolli da adottare	✓ prevedere uno standard efficace di comunicazione/informativa in tema di salute e sicurezza, tale da garantire a tutti i livelli aziendali conoscenze utili all'identificazione, riduzione e gestione dei rischi in ambiente di lavoro ✓ prevedere un piano di formazione annuale, in collaborazione con l'Ufficio Valorizzazione Risorse Umane, che definisca, attraverso l'utilizzo del fondo interprofessionale: i) le modalità ed erogazione della formazione; ii) i criteri di erogazione della formazione; iii) con riferimento ai soggetti coinvolti nella gestione delle tematiche della salute e della sicurezza, l'identificazione dell'ambito, i contenuti e le modalità della formazione in dipendenza del ruolo assunto all'interno della struttura organizzativa (Dirigenti, Preposti, RLS, ASPP); iv) i tempi di erogazione della formazione ai lavoratori sulla base delle modalità e dei criteri definiti;

4.2.5 Vigilanza su rispetto delle procedure e delle istruzioni operative

Processi di interesse	
Procedure/ regolamenti applicabili	✓ Manuale delle istruzioni operative per la gestione delle procedure di sicurezza, ediz. 1, rev. 1, 11/2/2013

Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ garantire la tracciabilità di documentazione aziendale da cui risultino ruoli, responsabilità e modalità di registrazione e monitoraggio per: i) i dati riguardanti la sorveglianza sanitaria; ii) i dati riguardanti la sicurezza degli impianti (ascensori, impianti elettrici, macchine;…) ✓ prevedere un programma di monitoraggio del rispetto, all'interno dell'azienda, delle procedure per la sicurezza sul lavoro. ✓ garantire la tracciabilità di documentazione aziendale da cui risultino: i) ruoli, responsabilità e modalità di rilevazione, registrazione, investigazione interna degli infortuni e delle malattie professionali; ii) ruoli, responsabilità e modalità di tracciabilità ed investigazione degli incidenti occorsi e dei "mancati incidenti"; ii) modalità di comunicazione, da parte dei responsabili operativi verso il datore di lavoro e al responsabile del servizio di prevenzione e protezione, relativamente a infortuni/incidenti occorsi

4.2.6 Verifica della applicazione e della efficacia del modello adottato e sul mantenimento nel tempo delle condizioni di idoneità

Processi di interesse	- monitoraggio infortuni/ tenuta registro infortuni e malattie professionali - gestione rapporti con VVF, ASL, INAIL,..
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ prevedere una modalità strutturata di verifica, da parte di terzi, della efficacia, nel tempo, delle procedure adottate per la gestione della sicurezza (ad esempio, con riferimento alle linee guida per Sistemi di Gestione della Sicurezza sul Lavoro redatte da INAIL . In prospettiva, adozione di un sistema di gestione compatibile OH SAS 18001) ✓ predisporre una modalità standard di monitoraggio delle performance delle modalità di gestione della sicurezza (infortuni, altri dati,…)

5 FLUSSI INFORMATIVI SPECIFICI VERSO LâOdV

L'Organismo di Vigilanza può ricevere dal personale, dai rappresentanti sindacali aziendali, dal rappresentante dei lavoratori per la sicurezza, dal medico competente, dai Responsabili del servizio di prevenzione e protezione e dal datore di lavoro, informazioni e notizie sulle eventuali carenze nella tutela della salute e sicurezza nei luoghi di lavoro;

I controlli svolti dall'Organismo di Vigilanza sono diretti a verificare la conformità delle attività aziendali ai principi espressi nella presente Parte Speciale e, in particolare, alle procedure interne in essere ed a quelle che saranno adottate in futuro, in attuazione della presente Parte Speciale.

E' facoltà dell'Organismo di Vigilanza, richiedere, con un ragionevole preavviso, l'assistenza del RSPP per l'esecuzione di verifiche a campione all'interno degli ambienti di lavoro.
E' facoltà dell'Organismo di Vigilanza, svolgere in via autonoma sopralluoghi all'interno degli ambienti di lavoro, anche senza l'ausilio del RSPP qualora non tempestivamente disponibile, a seguito di segnalazioni pervenute dai lavoratori.

A tal fine l'Organismo di Vigilanza

- effettua periodicamente controlli a campione sulle attività connesse ai «processi sensibili», diretti a verificare la corretta esplicazione delle stesse in relazione alle regole di cui al presente Modello. In questa prospettiva, pur garantendo all'Organismo libero accesso a tutta la documentazione aziendale rilevante così come previsto nella Parte Generale, vengono, comunque garantiti, in maniera continuativa, i flussi informativi elencati di seguito in tabella

- può attivarsi con specifici controlli a seguito delle segnalazioni ricevute, secondo quanto riportato nella Parte Generale del Modello 231.

PROCESSO DA VERIFICARE	FLUSSO INFORMATIVO VERSO OdV	FREQUENZA
Attuazione della gestione per la sicurezza sul lavoro	- Copia delle lettere di nomina del RSPP, RLS, medico competente	Annuale
	- cambiamenti della struttura organizzativa in materia di sicurezza e salute dei lavoratori e del sistema delle deleghe	Annuale / al momento della sostituzione
	- DVR ed ogni eventuale aggiornamento	
	- programma di formazione in materia di salute e sicurezza sul lavoro	annuale
	- Elenco degli eventi formativi svolti in materia di sicurezza	
Controllo sulla gestione per la sicurezza sul lavoro	- informativa su eventuali ispezioni effettuate presso la Società da autorità di controllo competenti in materia di sicurezza e salute sul lavoro e relative eventuali segnalazioni ricevute e/o prescrizioni	Semestrale e al loro verificarsi
	- infortuni occorsi con prognosi superiore a 40 giorni e attività di controllo effettuata dai delegati del datore di lavoro	annuale
	- Verbale riunioni periodiche	annuale

6 DEFINIZIONI

***Datore di lavoro**:* il soggetto titolare del rapporto di lavoro con il lavoratore o, comunque, il soggetto che, secondo il tipo e l'assetto dell'organizzazione nel cui ambito il lavoratore presta la propria attività, ha la responsabilità dell'organizzazione stessa o dell'unita produttiva in quanto esercita i poteri decisionali e di spesa. Per InnovaPuglia spa il datore di lavoro è il Presidente del Consiglio di Amministrazione

Responsabile del Servizio di Prevenzione e Protezione : persona in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 del D.Lgs. 81/08 designata dal datore di lavoro, a cui risponde, per coordinare il servizio di prevenzione e protezione dai rischi;

Preposto**:** persona che, in ragione delle competenze professionali e nei limiti di poteri gerarchici e funzionali adeguati alla natura dell'incarico conferitogli, sovrintende alla attività lavorativa e garantisce l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa;

Servizio di prevenzione e protezione dei rischi insieme delle persone, sistemi e mezzi esterni o interni all'azienda finalizzati all'attività di prevenzione e protezione dai rischi professionali per i lavoratori;

Addetto al servizio di prevenzione e protezione : persona in possesso delle capacità e dei requisiti professionali di cui all'articolo 32 del D.Lgs. 81/08, facente parte del servizio di prevenzione e protezione dei rischi

Medico competente: medico in possesso di uno dei titoli e dei requisiti formativi e professionali di cui all'articolo 38 del D.Lgs. 81/08, che collabora, secondo quanto previsto all'articolo 29, comma 1, dello stesso D.Lgs., con il datore di lavoro ai fini della valutazione dei rischi ed è nominato dallo stesso per effettuare la sorveglianza sanitaria e per tutti gli altri compiti di cui al presente decreto; i requisiti formativi e professionali del medico competente sono quelli indicati all' art. 38 del D.Lgs. 81/08.

Rappresentante dei lavoratori per la sicurezza: persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro;

Sorveglianza sanitaria: insieme degli atti medici, finalizzati alla tutela dello stato di salute e sicurezza dei lavoratori, in relazione all'ambiente di lavoro, ai fattori di rischio professionali e alle modalità di svolgimento dell'attività lavorativa;

Lesioni Gravi : Ai sensi dell'art. 583 c.p., la lesione personale è grave:

- 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;
- se il fatto produce l'indebolimento permanente di un senso o di un organo;

Lesioni Gravissime**:** Ai sensi dell'art. 583 c.p., la lesione personale é gravissima se dal fatto deriva:

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

Colpa incosciente : l'atteggiamento soggettivo in cui versa il singolo che ignora di violare, nel momento in cui agisce, una serie di prescrizioni cautelari atte ad evitare che dalla sua condotta pericolosa possano derivare pregiudizi per terzi soggetti.

Colpa cosciente: colui che agisce è sì consapevole della pericolosità del suo comportamento ed è conscio di agire in violazione di una norma prudenziale, ma comunque non vuole il prodursi dell'evento dannoso a carico di terzi ed è anzi certo che tale evento - nonostante la pericolosità della sua condotta - comunque non si verificherà . In tal caso, per quanto la violazione della normativa cautelare sia avvenuta intenzionalmente da parte del soggetto agente, tuttavia, la condotta criminale non può qualificarsi come dolosa.

PARTE SPECIALE D : REATI PER DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI ï CYBER CRIMES

1 AMBITO APPLICATIVO ED OBIETTIVI

L'art. 7 della legge 18 marzo 2008 n. 48, mediante l'inserimento nell'ambito del D. Lgs. 231/01 dell'art 24 *bis* sui delitti informatici e trattamento illecito dei dati, ha introdotto nuove fattispecie di reato che possono generare una responsabilità in capo alla Società.

La legge n.48/2008, infatti, relativa alla ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica fatta a Budapest il 23 Novembre 2001, ha previsto sia la modifica del Codice Penale, mediante l'introduzione di nuove norme incriminatrici e l'inasprimento di alcune fattispecie già esistenti, sia la modifica del D.lgs 231/2001 attraverso l'estensione della responsabilità delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, ai reati informatici per la mancata predisposizione preventiva di misure idonee ad evitare che figure apicali, dipendenti o collaboratori interni delle stesse commettano tale tipologia di illeciti. Ai fini della punibilità, va sempre ricordato che la Società deve trarre vantaggio dal reato ovvero deve comunque essere un portatore di interesse nel compimento del reato stesso.

L'adozione da parte di InnovaPuglia spa di un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs 231/01 in grado di

- ✓ prevenire adeguatamente le differenti ipotesi di illecito introdotte con tale normativa
- ✓ identificare eventuali comportamenti illeciti e l'autore degli stessi

trova il presupposto nella volontà di gestire il proprio sistema info-telematico attraverso l'adozione di regole e procedure alla cui osservanza tutti i dipendenti sono chiamati.

E' evidente che la redazione di questa Parte Speciale è basata in maniera determinante sulla esistenza, nella realtà aziendale di InnovaPuglia, di una pluralità di strumenti di gestione specifici per i temi connessi alla protezione delle infrastrutture IT, dei sistemi informatici/ telematici e delle applicazioni, dei dati e delle informazioni ivi contenute. In considerazione, infatti, del proprio ruolo istituzionale nei confronti della Regione Puglia, InnovaPuglia ha da tempo investito nella adozione di strumenti di gestione che garantissero il corretto e sicuro svolgimento della propria attività ruolo istituzionale; in particolare la Società ha

- adottato un **Sistema di Gestione della Sicurezza delle Informazioni** (SGSI) coerente con lo standard internazionale **ISO 27001:2006**, certificato da TÜV Italia e relativo alla **Gestione sistemistica dell'infrastruttura tecnologica di erogazione dei servizi ICT della Regione Puglia**.

- adottato un **Sistema di Gestione della Qualità** , coerente con lo standard internazionale **ISO 9001:2008**, certificato da TÜV Italia e avente come campo di applicazione la **Realizzazione, manutenzione, gestione e conduzione operativa delle componenti del Sistema Informativo della Regione Puglia e delle infrastrutture pubbliche di servizio alle PPAA ed ai cittadini**

- adottato un **Piano della Sicurezza** per il **Servizio di Posta Elettronica Certificata (PEC) ,** anch'esso fornito nell'ambito del Sistema Qualità certificato ISO 9001

- adeguato il proprio sistema organizzativo ai principi e obblighi di cui alla normativa vigente in materia e, in particolare, del **Decreto legislativo 30 giugno 2003, n. 196** (Codice in materia di protezione dei dati personali). Attraverso il **Documento Programmatico sulla Sicurezza** (DPS) (in fase di approvazione), i sistemi informatici/ telematici, i programmi informatici, nonché policies e procedure IT della Società garantiscono che il trattamento dei dati personali avvenga nel rispetto dei principi e norme di cui sopra, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Va ribadito, a tale proposito, che il Modello di Organizzazione e Gestione previsto ai fini del D.Lgs 231/01 non è sostitutivo di tali strumenti bensì li integra laddove sono funzionali alla riduzione del rischio di commissione dei reati previsti dal decreto stesso.

2 LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d.lgs. n. 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.
Si riporta, pertanto, di seguito una breve descrizione dei reati richiamati dall'art. 24-bis (*Delitti informatici e trattamento illecito dei dati*) del d.lgs. n. 231/2001; una discussione più puntuale è riportata in Allegato 1.D.

2.1 Reati di falsità in documenti informatici

L'articolo 491-bis del c.p. estende al caso dei documenti informatici, pubblici o privati, aventi efficacia probatoria, le disposizioni del c.p. relative ai seguenti reati di falso

- art 476 , relativo alla Formazione di un atto falso o alterazione di un atto vero.
- art 477, relativo a Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative
- art 478, relativo alla simulazione e rilascio in forma legale di una copia di un atto pubblico o privato la cui esistenza è solo supposta
- art 479, relativo a falsità ideologica commessa dal pubblico ufficiale in atti pubblici (falsa attestazione di fatti dei quali l'atto è destinato a provare la verità)
- art 480, relativo a Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative
- art 481, relativo a Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità.
- art 482 relativo a Falsità materiale commessa dal privato
- art 483 relativo a Falsità ideologica commessa dal privato in atto pubblico
- art 484 relativo a Falsità in registri e notificazioni ovvero registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o notificazioni all'Autorità stessa circa le proprie operazioni industriali, commerciali o professionali,
- art 485 relativo a Falsità in scrittura privata (scrittura privata falsa o alterazione di una scrittura privata vera)
- art 486 relativo a Falsità in foglio firmato in bianco/ Atto privato, ovvero il caso di chi, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato
- art 487 relativo a Falsità in foglio firmato in bianco / Atto pubblico
- art 490 relativo a Distruzione, soppressione e occultamento di un atto pubblico o di una scrittura privata.

2.2 Reati di accesso abusivo a sistemi informatici o telematici

Accesso abusivo a un sistema informatico o telematico (art. 615- ter c.p.)
Commette il delitto chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 - quater c.p.)
Il delitto è commesso da chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procuri, riproduca, diffonda, comunichi o consegni codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisca indicazioni o istruzioni idonee al predetto scopo.

2.3 Reati di danneggiamento, interruzione, intercettazione di sistemi informatici o telematici , di comunicazioni informatiche o telematiche, di informazioni, dati e programmi informatici

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 - quinquies c.p.)
Commette il delitto chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 – quater c.p.)
Il delitto, che può essere commesso da chiunque, consiste nella fraudolenta intercettazione ovvero nell'impedimento o nell'interruzione di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 - quinquies c.p.)
Compie il delitto chiunque, 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.

Danneggiamento di informazioni, dati e programmi informatici (art. 635 - bis c.p.)
Il delitto, salvo che il fatto costituisca più grave reato, consiste nella distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui, da chiunque posta in essere.

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.)
Il delitto, che può essere commesso da chiunque, consiste, salvo che il fatto costituisca più grave reato, nella commissione di 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.

Danneggiamento di sistemi informatici e telematici (art. 635 - quater c.p.)
Il delitto, salvo che il fatto costituisca più grave reato, è commesso da chiunque, mediante le condotte di cui all'articolo 635 - bis c.p., 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.

Danneggiamento di sistemi informatici e telematici di pubblica utilità (art. 635 - quinquies c.p.)
Il delitto è commesso se il fatto di cui all'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.

2.4 Reato di frode informatica del certificatore di firma elettronica

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 - quinquies c.p.)
Commette il delitto il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

3 LE ATTIVITAôSENSIBILI AI FINI DEL D.LGS. 231/2001

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'individuazione delle attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24 - *bis* del d.lgs. n. 231/2001, è stata ottenuta attraverso l'analisi puntuale dei processi della Società (così come riportati in All. A della Parte Generale del Modello) , individuando quelle condotte astrattamente ipotizzabili che determinerebbero la commissione dei reati previsti dal Decreto. L'individuazione puntuale dei processi a rischio è riportata in Allegato 2.D al presente documento.

Le attività sensibili individuate attraverso tale processo sono, pertanto:

1. Gestione dei profili utente e controllo degli accessi logici (autenticazione)

2. Risorse umane e sicurezza informatica

3. Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio

4. Acquisizione, sviluppo e manutenzione sw & sistemi

5. Gestione operativa dei sistemi informativi

6. Gestione degli accessi fisici alla infrastruttura ICT

4 PROTOCOLLI PER LA FORMAZIONE E LôATTUAZIONE DELLE DECISIONI E SISTEMA DI CONTROLLO

4.1 Principi specifici di comportamento

Gli obiettivi fondamentali di sicurezza informatica che la Società si pone sono:

- ✓ ***Integrità*** ovvero la garanzia che ogni dato aziendale sia realmente e completamente rappresentativo, in maniera oggettiva e senza interpretazioni, dei contenuti a cui si riferisce. Tale obiettivo si persegue tramite l'adozione di opportune contromisure che impediscano alterazioni incidentali o intenzionali che ne possono mutare il significato originale o, in alternativa, forniscano la possibilità di rilevare la suddetta alterazione del dato e di recuperare il dato integro.
- ✓ ***Riservatezza*** ovvero la garanzia che un dato aziendale venga reso disponibile solamente alle applicazioni ed agli utenti incaricati e autorizzati al suo utilizzo;
- ✓ ***Disponibilità*** ovvero la garanzia di reperibilità dei dati aziendali in funzione delle esigenze di continuità dei processi aziendali e di rispetto delle norme (di legge e non) che impongono la conservazione storica o determinati livelli di servizio.

Rispetto a questi obiettivi, la presente Parte Speciale prevede l'espresso divieto – a carico degli esponenti aziendali (Organi sociali e personale), in via diretta, e a carico dei Collaboratori esterni e Fornitori, tramite apposite clausole contrattuali – di

- porre in essere comportamenti che possano rientrare nelle fattispecie di reato richiamate dall'articolo 24–bis d.lgs. 231/2001.
- violare i principi e le procedure aziendali previste nella presente Parte Speciale

Ne consegue che ai Destinatari è fatto, in particolare, **DIVIETO** di: :

1. alterare (o concorrere [4]ad alterare, con un pubblico ufficiale o incaricato di pubblico servizio) documenti informatici, pubblici o privati, aventi efficacia probatoria;

2. distruggere, sopprimere, occultare in tutto o in parte una scrittura privata o un atto pubblico veri, sotto forma di documento informatico;

3. utilizzare abusivamente la firma digitale aziendale o, comunque, in violazione delle procedure che ne regolamentano l'utilizzo

4. accedere abusivamente o permanere contro la volontà espressa o tacita dell'avente diritto, in un sistema informatico o telematico protetto da misure di sicurezza

5. procurarsi, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo.

6. procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare, mettere a disposizione apparecchiature dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico o le informazioni, i dati o i programmi ivi contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale o l'alterazione del suo funzionamento;

7. intercettare illegittimamente o abusivamente, impedire, interrompere fraudolentemente o illegittimamente comunicazioni informatiche o telematiche;

8. installare illegittimamente o abusivamente apparecchiature atte ad intercettare, impedire, interrompere comunicazioni informatiche o telematiche;

9. distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui, o utilizzati dallo Stato, dalla Regione Puglia o da altro ente pubblico o ad essi pertinenti o comunque di pubblica utilità;

10. distruggere, danneggiare, rendere in tutto o in parte inservibili sistemi informatici o telematici altrui, ovvero ostacolarne gravemente il funzionamento mediante distruzione, deterioramento, cancellazione, alterazione, soppressione di informazioni, dati o programmi informatici altrui o attraverso l'introduzione o la trasmissione di dati, informazioni o programmi;

11. distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o introdurre o trasmettere dati, informazioni o programmi al fine distruggere, danneggiare, o causare l'inutilizzabilità in tutto o in parte di sistemi informatici o telematici ovvero al fine di ostacolarne gravemente il loro funzionamento.

[4] La definizione di ñconcorsoò di persone del reato data dal codice penale ricomprende nel ñcontributo obiettivamente rilevanteò ogni forma di collaborazione, anche ñmoraleò, idonea, cioè, a determinare o a rafforzare il proposito criminoso di altri soggetti (e.g. istigazione)

12. introdurre e/o conservare applicazioni/software la cui provenienza sia dubbia o sconosciuta e, comunque, senza averne data opportuna informativa al responsabile della funzione competente
13. trasferire all'esterno di InnovaPuglia e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà di InnovaPuglia, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni

14. lasciare accessibile ad altri il proprio PC senza rispettare le indicazioni della "Politica per schermo e scrivania puliti" del SGSI oppure consentire l'utilizzo dello stesso ad altre persone (parenti, amici, ecc.) senza un adeguato controllo sulle azioni svolte;

15. utilizzare password di altri utenti aziendali, neppure per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del responsabile della funzione competente;

- è fatto **OBBLIGO** di:

16. attenersi alle istruzioni impartite ai sensi del D.Lgs 163/03 in tema di trattamento dei dati personali ed, in generale, a quanto definito nel Documento Programmatico sulla Sicurezza di InnovaPuglia;

17. attenersi a quanto disposto dalle procedure aziendali relative al Sistema di Gestione della Sicurezza delle Informazioni (SGSI) e linee guida in materia di:
    a. utilizzo del personal computer;
    b. utilizzo della rete aziendale;
    c. gestione delle password;
    d. utilizzo dei supporti magnetici e dei PC portatili;
    e. utilizzo della posta elettronica;
    f. utilizzo della rete internet e dei relativi servizi;
    g. ogni altra attività svolta mediante strumentazioni, piattaforme o sistemi informatici

18. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta dalla Società;

19. non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile della funzione competente alla gestione dei relativi sistemi informatici;

20. in caso di smarrimento o furto di qualsiasi apparecchiatura informatica della Società o delle Pubbliche Amministrazioni coinvolte, informare tempestivamente il responsabile della funzione competente alla gestione dei relativi sistemi informatici e presentare denuncia all'autorità giudiziaria;

21. rispettare le procedure e gli standard previsti in materia di utilizzazione delle risorse informatiche, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali di queste ultime;

22. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni di InnovaPuglia;

23. in ogni caso osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

Le condotte di ordine generale descritte integrano e non sostituiscono i principi previsti dal Codice Etico, nonché le eventuali procedure di maggiore tutela previste all'interno di InnovaPuglia e relative alle attività sensibili.

4.2 Protocolli Specifici

Per il raggiungimento degli obiettivi di prevenzione relativi a questa Parte Speciale, costituisce preciso obbligo per tutti i Destinatari del presente Modello rispettare e **attenersi** con il massimo rigore **a tutte le *policies* aziendali e procedure facenti parte del Sistema di Gestione della Sicurezza delle Informazioni basato sullo standard ISO/IEC 27001 oltre che del Documento Programmatico sulla Sicurezza redatto in conformità al D.Lgs 196/2003.** Vengono, inoltre, definiti i seguenti protocolli specifici, funzionali agli obiettivi di prevenzione propri della presente Parte speciale :

4.2.1 Gestione dei profili utente e controllo degli accessi logici (autenticazione)

Processi di interesse	- Attribuzione & gestione credenziali di accesso ai sistemi / reti (AdS,…) - Attribuzione credenziali accesso utenti ai servizi - Gestione conti correnti (home banking) - Gestione credenziali servizi EmPULIA (Albo fornitori, piattaforma e-procurement,..) - …
Procedure/ regolamenti applicabili	✓ *Politica SGSI Controllo degli accessi logici* ✓ *Procedura di rilascio credenziali PR SGSI RilCred* ✓ *Politica SGSI per virus e malware* ✓ *Regolamento Albo online fornitori Regione Puglia (EmPULIA)* ✓ *…*
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ dare agli utenti una comunicazione scritta sui loro diritti di accesso alle infrastrutture ICT e richieder loro di firmare dichiarazione in cui indicano di aver compreso le condizioni di accesso ✓ i diritti di accesso legati ad ogni specifico ruolo devono essere i minimi necessari per lo svolgimento della funzione (principio del privilegio minimo) ✓ l'Ufficio Personale e/o il Responsabile di Servizio informano prontamente l'Ufficio Gestione Operativa di ogni modifica di rapporto lavorativo o di ruolo aziendale per modificare di conseguenza le credenziali ✓ limitare al massimo e, comunque controllare, l'assegnazione e l'utilizzo di accessi privilegiati ✓ ogni modifica di profilo di accesso deve essere autorizzata e registrata in archivio ✓ per le risorse esterne che devono operare sulla infrastruttura, comunicazione, da parte della società esterna, dei dati utili ad assegnare i profili adeguati

	✓ lista delle modifiche di attribuzione di ruolo aziendale e relativa evidenza delle modifiche dei profili di accesso al sistema ✓ Servizio EmPULIA/ gestione Albo online fornitori Regione Puglia: nessun utente autorizzato (operatori EmPULIA, stazioni appaltanti) può concedere a terzi i codici di accesso all'Albo ✓ Servizio EmPULIA / piattaforma di e-procurement : nell' espletamento delle procedure di gara deve essere precluso (anche al RUP) , prima della chiusura dei termini, l'accesso all'archivio delle offerte pervenute ✓ Il possesso delle credenziali per i servizi di home banking per i c.c. InnovaPuglia deve essere formalizzato con specifica lettera di attribuzione

4.2.2 Risorse umane e sicurezza informatica

Processi di interesse	- assegnazione responsabilità (progetto, ufficio,….) - assegnazione dotazioni individuali (notebook, desktop, token,. …) - assegnazioni credenziali di identificazione e accesso ai sistemi - formazione del personale - ….
Procedure/ regolamenti applicabili	✓ *Politica SGSI Schermo Scrivania Pulita* ✓ *Politica SGSI Telecomunicazioni, email e internet* ✓ *Politica SGSI di uso della password* ✓ *Politica SGSI per Virus e Malware* ✓ *Politica SGSI per Mobile Computing* ✓ *Procedure del DPS*
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza dei sistemi informativi, e che tenga conto della normativa applicabile in materia, dei principi etici e della classificazione delle informazioni a cui i predetti soggetti avranno accesso; ✓ specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza informatica per tutti i dipendenti e, dove rilevante, per i terzi; ✓ dare evidenza della attività formativa per la sicurezza, adeguata al ruolo svolto ✓ obbligo di restituzione dei beni forniti per lo svolgimento dell'attività

	lavorativa (ad es. PC, telefoni cellulari, token di autenticazione, etc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto; ✓ destituzione, per tutti i dipendenti e i terzi, dei diritti di accesso alle informazioni, ai sistemi e agli applicativi al momento della conclusione del rapporto di lavoro e/o del contratto o in caso di cambiamento della mansione svolta

4.2.3 Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio

Processi di interesse	- gestione documenti in uscita - archiviazione documenti / dati interni - rilevazione/ elaborazione dati del personale - redazione del DVR
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ definizione di un regolamento per la gestione dei flussi documentali aziendali (uso della firma digitale, PEC, protocollo, sistema di gestione documentale) ✓ definizione di un regolamento per l'acquisizione / gestione delle firme digitali ✓ adozione, per il protocollo generale aziendale, del sistema di protocollo informatico RUPAR ✓ Inclusione dell'archivio dei documenti interni nel perimetro del SGSI ✓ rendere non modificabile / tracciabile ogni modifica sugli archivi interni : personale [presenze, ferie/permessi, missioni], Albo consulenti, contabilità ✓ garantire un elevato livello di efficacia dei piani di conservazione degli archivi interni ✓ centralizzazione (e relativa indicizzazione e classificazione) di tutti gli archivi interni (inclusi archivi documentali progettuali) ✓ introdurre modalità di data certa (e non modificabilità) per il DVR

4.2.4 Acquisizione, sviluppo e manutenzione sw & sistemi

Processi di interesse	- Redazione capitolati tecnici per appalti ICT - Manutenzione della configurazione - Assistenza tecnica alla manutenzione correttiva / evolutiva delle piattaforme ICT - sviluppo interno di componenti sw - controllo attività ICT appaltate
Procedure/ regolamenti applicabili	✓ *Procedura SGSI ChaMan* ✓ *Procedura Qualità / Gestione Azioni Correttive PRQ GEN 05* ✓ *Procedura Qualità / Gestione Azioni preventive PRQ GEN 06* ✓ *Procedura qualità Help Desk PRQ SIhd (sistema ticketing / RfC)* ✓
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ assicurazione che il sw da installare sui server aziendali sia verificato per la sicurezza ✓ nello sviluppo di componenti sw , adottare le indicazioni della Politica SGSI di Uso delle password ✓ inclusione della sicurezza del sw tra le clausole per l'accettazione di sw sviluppato su appalti esterni

4.2.5 Gestione operativa dei sistemi informativi

Processi di interesse	- monitoraggio piattaforme dei Centri servizio & problem solving di 1° livello - conservazione archivi servizi Regione Puglia - monitoraggio sicurezza & problem management - help desk - gestione piattaforme di sicurezza per protezione reti - monitoraggio livelli di servizio
Procedure/ regolamenti applicabili	✓ *Politica SGSI Back-up e restore* ✓ *Procedura SGSI Gestione Incidenti PR SGSI GesInc* ✓ *Piano Continuità Operativa (Piano CO)* ✓ *Procedure del DPS* ✓ *Procedura Help Desk PRQ SIhd* ✓ *Procedura Sistema Qualità Servizi Infotelematici – Misura della qualità per i processi di erogazione dei servizi infotelematici PRQ SImisqual* ✓ *Istruzioni Operative Monitoraggio del processo di erogazione dei servizi infotelematici IOQ SImonit*
Poteri autorizzativi e di firma rilevanti per l'attività	

Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ predisporre procedura di allerta e agreement operativo tra gestori infrastruttura ICT e Centri Servizio (EmPULIA, Sistema Puglia,..) in previsione di situazioni di sovraccarico e/o di criticità operativa (es: allineamento tra operazioni di manutenzione infrastruttura rispetto a scadenze di bandi, etc) ✓ archiviazione (in formato non modificabile) dei file di log degli eventi riguardanti la sicurezza ✓ procedura di analisi di tutti gli incidenti

4.2.6 Gestione degli accessi fisici alla infrastruttura ICT

Processi di interesse	- inventariazione - manutenzione hw - dismissione di sistemi / dispositivi - controllo degli accessi fisici - gestione infrastrutture tecniche di supporto
Procedure/ regolamenti applicabili	✓ *Politica SGSI Sicurezza fisica* ✓ *Procedura SGSI Dismissione asset* ✓ *Procedura SGSI Asset managemen* ✓ *Piano Sicurezza PEC* ✓ *DPS*
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ Conservare in ambiente sicuro (per una durata non inferiore a una settimana) i file di log degli accessi fisici / i file di videorveglianza

5 FLUSSI INFORMATIVI SPECIFICI VERSO LôODV

L'attività dell'OdV è svolta in stretta collaborazione tra i vari responsabili delle Aree interessate alla parte speciale.
I controlli svolti dall'Organismo di Vigilanza sono diretti a verificare la conformità delle attività aziendali ai principi espressi nella presente Parte Speciale e, in particolare, alle procedure interne in essere ed a quelle che saranno adottate in futuro, in attuazione della presente Parte Speciale.
In tal senso devono essere previsti flussi informativi completi e costanti tra tali soggetti e l'Organismo di Vigilanza, al fine di ottimizzare le attività di verifica; più in particolare, in presenza di un complesso sistema di risorse tecnologiche dedicate alla sicurezza e di un relativo sistema procedurale, ben strutturato, il controllo operato dall'OdV è focalizzato sulla corretta gestione e aggiornamento dello specifico sistema di risorse e procedure.

PROCESSO DA VERIFICARE	FLUSSO INFORMATIVO VERSO OdV	FREQUENZA
Implementazione del SGSI e del DPS	- relazioni degli audit del Sistema di Gestione della Sicurezza delle Informazioni	- semestrale
	- relazione degli audit del Sistema Qualità dei Sistemi Informativi	- semestrale
	- informativa sull'aggiornamento del contenuto del DPS ex-D.Lgs 196/2003	- annuale
	- copia delle lettere di incarico dei ruoli previsti dal SGSI	- annuale (aggiornamenti)
	- lista degli eventi formativi in materia di SGSI e privacy	- annuale
	- informativa su eventuali nuove normative in tema di sicurezza informatica e sui conseguenti aggiornamenti operati su sistemi e procedure	- annuale
	- informativa su attuazione dei protocolli previsti dalla Parte Speciale	- annuale
Gestione esercizio sistemi, reti e servizi informatici	- lista delle segnalazioni di anomalie dei sistemi informatici (dalle quali possano evincersi accessi o tentativi di accessi abusivi, danneggiamenti, violazione delle procedure interne IT, cancellazione dei dati, ecc.)	trimestrale
	- relazione su incidenti informatici verificatisi e sulla loro gestione da parte dell'Incident Response Team;	annuale
	- lista dei reclami / ricorsi, da parte di utenti della piattaforma di e-procurement, per danni da disservizi di natura informatica	semestrale
Gestione documentazione aziendale	- Lista delle firme digitali esistenti in Società con firma, per accettazione, del relativo regolamento di utilizzo	Semestrale
	- Copia lettera di attribuzione della responsabilità per la gestione delle credenziali per l'home banking	Annuale
Sviluppo componenti sw / appalti esterni	- Copia dei contratti di appalto con evidenza dei requisiti sulla sicurezza del sw	Semestrale

6 DEFINIZIONI

DOCUMENTO INFORMATICO

La definizione di "documento informatico" fornita dal D.P.R. 10 novembre 1997, n. 513, accolta nel D.Lgs. 7 marzo 2005, n. 82 (cd. Codice dell'Amministrazione Digitale) si riferisce a "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti". I documenti informatici rilevanti ai fini delle norme in questione sono quelli pubblici o privati, dotati di efficacia probatoria, cioè con firma elettronica qualificata o emessi nel rispetto di quelle regole tecniche finalizzate a garantirne paternità, provenienza, integrità e immodificabilità.
La nozione di atto pubblico, ai fini della tutela penale, è certamente più ampia di quella del codice civile, poiché sono ricompresi non solo i documenti redatti con le debite formalità prescritte dalla legge da un notaio o da un pubblico ufficiale autorizzato ad attribuire pubblica fede al documento, ma vi sono ricompresi tutti i documenti formati da un pubblico ufficiale o da un pubblico impiegato o incaricato di un pubblico servizio e compilato, con le formalità previste dalla legge, al fine di comprovare un fatto giuridico o al fine di attestare fatti da lui compiuti o avvenuti in sua presenza e destinato ad assumere rilevanza giuridica.

Può trattarsi di qualunque atto scritto, file o altro contenuto di un programma informatico, del quale sia riconoscibile l'autore che in esso si palesa, contenente una dichiarazioni di scienza (esposizione di dati o fatti) o manifestazioni di volontà.

Ne deriva una nuova e più completa definizione di documento informatico, sostanzialmente equiparato a quello cartaceo, che si riflette nell'estensione dell'applicabilità delle norme relative alla falsità in atti (scritti), di cui al capo III del titolo VII, libro II del codice penale (**), ai reati commessi in danno di qualunque documento informatico, sia esso pubblico o privato, purché lo stesso abbia efficacia probatoria (si veda il primo comma dell'art. 491-bis).

DANNEGGIAMENTO / DISTRUZIONE / DETERIORAMENTO

Per "danneggiamento" si intende sia un danneggiamento fisico, sia un danneggiamento dei sistemi nelle loro componenti immateriali. Questa condotta danneggiatrice può riguardare sia il sistema nella sua complessità, sia una o più delle sue singole componenti materiali e i dati "aggrediti" possono avere diversa natura: può trattarsi di dati immagazzinati nella memoria interna dell'elaboratore o su un supporto esterno, o di dati in transito da un computer all'altro.
Il termine "danneggiamento" racchiude un concetto molto ampio, che comprende la distruzione di dati o programmi, il loro deterioramento e la loro resa inservibilità totale o parziale.
Per "**distruzione**" si intende un'eliminazione definitiva dei dati o dei programmi; per "**deterioramento**" ci si riferisce ad una notevole diminuzione della loro utilizzabilità, e infine la resa "inservibilità totale o parziale" consiste in tutte quelle condotte danneggiatrici diverse dalla mera cancellazione e deterioramento dei dati.

Sussiste il reato di danneggiamento informatico anche quando i file cancellati possono essere recuperati.
La locuzione 'cancellazione' deve essere interpretata - dice la Cassazione – nella accezione informatica e non semantica del termine, ossia come la "rimozione da un certo ambiente di determinati dati, in via provvisoria attraverso il loro spostamento nell'apposito cestino o in via 'definitiva' mediante il successivo svuotamento dello stesso".
Del tutto irrilevante, ai fini della sussistenza del reato, il fatto che i files cancellati possano essere recuperati ex post attraverso una specifica procedura tecnico-informatica.
(Cass., Sez. V, 18 novembre 2011)

INTERCETTAZIONE

E' quella speciale ipotesi che concerne la "presa di cognizione" e che si realizza attraverso la particolare modalità della intromissione nella comunicazione in corso tra terzi. Deve avere ad oggetto il contenuto di una comunicazione

informatica o telematica in atto, nel momento dinamico della sua trasmissione, trovando invece tutela nell'art. 616, 1° e 4° comma c.p., l'illecita presa di cognizione del contenuto di una comunicazione ormai avvenuta o già fissata in un supporto fisico (come ad esempio un floppy disk o un cd rom).

SISTEMA TELEMATICO

E' stato riconosciuto il carattere di sistema telematico anche alla telefonia mobile (GSM o UMTS), sia cellulare sia satellitare, in quanto sistema atto alla trasmissione del segnale (comportante anche la possibilità di invio di messaggi di testo - gli SMS - ovvero anche, audio-video) con tecnologia digitale.

FIRMA ELETTRONICA / FIRMA DIGITALE

All'art. 1 del Codice dell'amministrazione digitale sono rinvenibili le definizioni di firma elettronica, firma elettronica avanzata, firma elettronica qualificata e firma digitale, che costituisce una specificazione maggiormente articolata di quella elettronica avanzata. E' possibile ricomprendere nella categoria più generale della firma elettronica sia la firma elettronica avanzata/qualificata (o forte, includendo al suo interno anche la firma digitale) sia quella non qualificata (o leggera).
La firma elettronica qualificata e/o digitale è basata sulla tecnologia della crittografia a chiavi asimmetriche ovvero su un sistema di coppie di chiavi asimmetriche che consentono di ricondurre il contenuto di un documento allo specifico utente che l'ha prodotto e sottoscritto. Tali chiavi certificate, se in possesso dei requisiti di cui all'allegato I della direttiva europea sono definite **certificati qualificati** e devono necessariamente essere prodotte da un certificatore qualificato o accreditato sottoposto alla vigilanza della Agenzia per l'Italia Digitale.
La certificazione è un elemento essenziale per garantire l'**integrità** dei dati contenuti nel documento informatico, l'**autenticità** delle informazioni relative al sottoscrittore e il **non ripudio** del contenuto del documento da parte dell'autore stesso. Il valore probatorio del documento informatico sottoscritto con firma elettronica si differenzia a seconda della tipologia di firma apposta

PARTE SPECIALE E : REATO DI INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALLôAUTORITAôGIUDIZIARIA

InnovaPuglia S.p.A.
Società assoggettata alla direzione e controllo della Regione Puglia
Strada Provinciale per Casamassima Km. 3 70010 - Valenzano Bari
CCIAA di Bari n. 513395 - P.Iva 06837080727
Capitale Sociale Euro 1.434.576,00 i.v. a socio unico

tel. +39 080.46.70.418
fax +39 080.45.51.868
info@innova.puglia.it
www.innova.puglia.it

1 AMBITO APPLICATIVO ED OBIETTIVI

La presente Parte Speciale riguarda il reato di ***Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorita' giudiziaria***, contemplati all'art. 25 *decies* del D. Lgs. n. 231/2001.

2 LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d.lgs. n. 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.
Si riporta, pertanto, di seguito una breve descrizione dei reati richiamati dall'art. 25-*decies* del d.lgs. n. 231/2001; una discussione più puntuale è riportata in Allegato 1.E.

L'art 377-bis del codice penale individua come reato l'induzione, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere.

3 LE ATTIVITAôSENSIBILI AI FINI DEL D.LGS. 231/2001

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'individuazione delle attività "sensibili", nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-*decies* del d.lgs. n. 231/2001, è stata ottenuta attraverso l'analisi puntuale dei processi della Società (così come riportati in All. A della Parte Generale del Modello) , individuando quelle condotte astrattamente ipotizzabili che determinerebbero la commissione dei reati previsti dal Decreto. L'individuazione puntuale dei processi a rischio è riportata in Allegato 2.E al presente documento.

Le attività sensibili individuate attraverso tale processo sono:

1. Gestione del contenzioso giudiziario

4 PROTOCOLLI PER LA FORMAZIONE E LôATTUAZIONE DELLE DECISIONI E SISTEMA DI CONTROLLO

4.1 Principi specifici di comportamento

I seguenti principi di comportamento si applicano ai Destinatari che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto ai delitti in materia di violazione del diritto d'autore di cui all'art. 25 *decies* del D.Lgs. 231/2001. In via generale, a tali soggetti è richiesto di:

- evadere con tempestività, correttezza e buona fede tutte le richieste provenienti dagli organi di polizia giudiziaria e dall'autorità giudiziaria inquirente e giudicante, fornendo tutte le informazioni, i dati e le notizie eventualmente utili;
- mantenere, nei confronti degli organi di polizia giudiziaria e dell'autorità giudiziaria, un comportamento disponibile e collaborativo in qualsiasi situazione.

È fatto espresso divieto ai Destinatari di ricorrere a minacce oppure promettere, offrire o concedere un'indebita utilità per indurre chi può avvalersi della facoltà di non rispondere nel procedimento penale, a non rendere dichiarazioni o a rendere false dichiarazioni all'autorità giudiziaria, con l'intento di ottenere una pronuncia favorevole alla Società o determinare il conseguimento di altro genere di vantaggio.

È inoltre vietato:

- intrattenere rapporti con persone sottoposte alle indagini preliminari e imputati nel processo penale al fine di turbare la loro libertà di autodeterminazione;
- riconoscere forme di liberalità o altre utilità a dipendenti o terzi che siano persone sottoposte alle indagini preliminari e imputati nel processo penale per indurli a omettere dichiarazioni o a falsare le stesse, in favore della Società;
- riconoscere progressioni in carriera, scatti retributivi o incentivi premianti a dipendenti o collaboratori che non trovino adeguata corrispondenza nei piani di sviluppo delle risorse umane aziendali, nelle politiche remunerative e di incentivazioni aziendali o che comunque non rispondano a ragioni obiettive che giustifichino l'assunzione di dette iniziative.

4.2 Protocolli Specifici

4.2.1 Gestione contenzioso giudiziario

Processi di interesse	- gestione del contenzioso giudiziario
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ in caso di visite/ispezioni da parte di autorità pubbliche dovranno essere immediatamente contattati, a seconda dell'autorità procedente, i responsabili della funzione aziendale competente in materia;

	✓ ogniqualvolta un dipendente o collaboratore della Società, in virtù dei propri rapporti con la stessa, venga chiamato a rendere dichiarazioni davanti all'autorità giudiziaria nell'ambito di un procedimento penale, é tenuto ad informarne la Direzione Generale e la Direzione Affari Generali, nel rispetto dell'eventuale segreto istruttorio; ✓ é fatto espresso divieto di indurre, con violenza o minaccia, con offerta o promessa di denaro o di altra utilità, una persona chiamata a rendere davanti all'autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa abbia la facoltà di non rispondere, a non rendere dichiarazioni o a renderne di mendaci; ✓ ogniqualvolta un soggetto chiamato a rendere dichiarazioni davanti all'autorità giudiziaria nell'ambito di un procedimento penale in cui la società abbia un interesse sia vittima di violenza o minaccia o riceva un'offerta o promessa di denaro od altra utilità al fine di non rendere dichiarazioni o di renderne di mendaci, é tenuto ad avvisare immediatamente l'OdV, la Direzione Generale e la Direzione Affari Generali ✓ qualora un amministratore, un dirigente o un dipendente sia chiamato (rispettivamente nella veste di indagato/imputato, persona informata sui fatti/testimone o teste assistito/imputato in procedimento connesso) a rendere dichiarazioni innanzi all'Autorità Giudiziaria in merito ad attività connessa alla gestione ed all'amministrazione societaria, è tenuto a mantenere il massimo riserbo relativamente alle dichiarazioni rilasciate ed al loro oggetto, ove le medesime siano coperte da segreto investigativo oltre all'obbligo di rigettare qualsiasi tentativo proveniente da altri amministratori o dipendenti volto a condizionare il contenuto delle proprie dichiarazioni o ad indurlo ad avvalersi della facoltà di non rispondere.

Gli stessi principi, in quanto applicabili, sono osservati anche da terzi interessati in relazione alle dichiarazioni dai medesimi rilasciate all'Autorità Giudiziaria in merito a vicende di qualsiasi natura inerenti a InnovaPuglia di cui gli stessi siano a conoscenza.

5 FLUSSI INFORMATIVI SPECIFICI VERSO L'OdV

PROCESSO DA VERIFICARE	FLUSSO INFORMATIVO VERSO OdV	FREQUENZA
Gestione contenzioso giudiziario	- lista dei contenziosi giudiziari che abbiano richiesto testimonianze da parte di personale della Società - lista del personale coinvolto - legali che assistono la società - esiti dei procedimenti (data comparsa e/o comunicazioni dei legali, …) -	Annuale

PARTE SPECIALE F : DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO DâAUTORE

1 AMBITO APPLICATIVO ED OBIETTIVI

La presente Parte Speciale riguarda i reati di violazione del diritto d'autore, contemplati all'art. 25 *novies* del D. Lgs. n. 231/2001.

2 LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d.lgs. n. 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.
Si riporta, pertanto, di seguito una breve descrizione dei reati richiamati dall'art. 25 *novies* (*Violazione del diritto d'autore*) del d.lgs. n. 231/2001 e che fanno riferimento alla Legge 633/1941; una discussione più puntuale è riportata in Allegato 1.F.

Va premesso che le norme in esame tutelano il *diritto morale* e di *utilizzo economico,* da parte del loro autore:

- delle *opere dell'ingegno* aventi carattere *creativo* che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione;
- dei *programmi per elaboratore* come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con l. 20 giugno 1978, n. 399, nonché le *banche di dati* che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

I *diritti morali* sorgono in capo all'autore dell'opera dell'ingegno per il mero fatto della creazione. A differenza dei d*iritti di utilizzazione economica*, sono inalienabili e possono essere fatti valere in qualunque tempo, anche quando ci si sia spogliati della possibilità di disporre economicamente del bene oggetto di tutela.
Anche i diritti di utilizzazione economica, come i diritti morali, sorgono generalmente dal solo fatto della creazione; fanno però eccezione la creazione di banche dati, di programmi per elaboratore e di opere di disegno industriale da parte del lavoratore dipendente. In questi casi, mentre restano intrasferibili i diritti morali dell'autore-dipendente, i diritti di utilizzazione vengono invece acquisiti a titolo originario dal datore di lavoro.

2.1 Messa a disposizione del pubblico, su rete telematica o altre connessioni, di opere dell'ingegno, senza averne diritto

art 171, comma 1, lett. a-bis)
La norma punisce la messa a disposizione del pubblico, mediante immissione in un sistema di reti telematiche e/o con connessioni di qualunque genere, di un'opera dell'ingegno protetta o anche solo una parte di essa (con l'aggravante dell'usurpazione della paternità dell'opera) (una qualunque opera dell'ingegno prodotta da terzi, quali ad esempio un ricerca, uno studio, una raccomandazione, un articolo, una banca dati, una generica pubblicazione, sulla quale l'intermediario non vanta alcun diritto)

Art 171-ter

Tra le condotte previste dalla normativa vi è (comma ii) la riproduzione, trasmissione o diffusione in pubblico di opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati.

Le condotte abusive di cui al punto (ii) (abusiva riproduzione, trasmissione o diffusione in pubblico) hanno ad oggetto opere, o parti di opere, letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico - musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati.

A differenza dell'art 171, l'elemento caratterizzante l'art 171-ter è il dolo specifico costituito dal fine di lucro. Tale fine presuppone il perseguimento, da parte dell'agente, di un vantaggio diretto di carattere economico patrimoniale. In questo senso, nel contesto societario di InnovaPuglia la perseguibilità ai sensi del D.Lgs 231/01 può assumere rilevanza per l'utilizzo di materiali didattico-scientifici (e.g. materiali resi disponibili su piattaforme di e-learning) creati per la formazione del personale e/o dei clienti coperti dal diritto d'autore.

2.2 Duplicazione abusiva di programmi e reimpiego di banche dati

Si fa riferimento a tutti i casi in cui si arreca un pregiudizio agli interessi patrimoniali facenti capo al titolare dei relativi diritti di sfruttamento

Art. 171-bis

Le condotte alternative di reato si realizzano nei casi di:

(i) duplicazione abusiva di programmi per elaborare contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (S.I.A.E.) ovvero effettuata al di fuori delle condizioni contrattuali che regolano i rapporti tra il titolare dei corrispondenti diritti e il fruitore del programma.
(ii) importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale (anche quei casi in cui la detenzione del software sia destinata a svolgere una qualsiasi funzione interna nello svolgimento dell'attività imprenditoriale del detentore),concessione in locazione di programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (S.I.A.E.); o
(iii) rimozione arbitraria o elusione di dispositivi applicati a protezione di un programma; o
(iv) trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca di dati; o
(v) esecuzione dell'estrazione o del reimpiego della banca di dati; o
(vi) distribuzione, vendita o concessione in locazione di una banca di dati.

Le violazioni considerate devono essere dirette ad un fine di profitto, concetto che va oltre il fine di lucro, non esaurendosi in una finalità di guadagno, bensì caratterizzando anche le condotte ispirate da una finalità di risparmio, nel senso di una mancata diminuzione patrimoniale (es. l'utilizzazione dello stesso programma su più postazioni).

3 LE ATTIVITAôSENSIBILI AI FINI DEL D.LGS. 231/2001

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 potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 25-*novies* del d.lgs. 231/2001:

1. Gestione software aziendali, con particolare riferimento ai processi di

- configurazione sw dispositivi individuali
- sviluppo componenti sw
- acquisto di beni (sw)

2. Gestione dei processi di comunicazione aziendale, includendo i processi di

- gestione portali servizi applicativi Regione Puglia
- gestione portale istituzionale InnovaPuglia
- produzione pubblicazioni
- organizzazione eventi

4 PROTOCOLLI PER LA FORMAZIONE E LôATTUAZIONE DELLE DECISIONI E SISTEMA DI CONTROLLO

4.1 Principi specifici di comportamento

I seguenti principi di comportamento si applicano ai Destinatari che, a qualunque titolo, siano coinvolti nelle attività "sensibili" rispetto ai delitti in materia di violazione del diritto d'autore di cui all'art. 25-*novies* del D.Lgs. 231/2001.

In via generale, a tali soggetti è richiesto di:

- assicurare il rispetto delle normative interne, comunitarie e internazionali poste a tutela della proprietà intellettuale;
- utilizzare opere di carattere scientifico protette dal diritto d'autore sulla base di accordi formalizzati per iscritto con il legittimo titolare per il relativo sfruttamento e in ogni caso nei limiti di detti accordi;
- curare diligentemente gli adempimenti di carattere amministrativo connessi all'utilizzo di opere protette dal diritto d'autore (es. scientifiche o di *software*) nell'ambito della gestione del sistema IT aziendale e nell'utilizzo sul *web*
- nel caso di necessità di utilizzo di sistemi sw per cui è richiesta una licenza d'uso, impiegare sui dispositivi di InnovaPuglia soltanto prodotti per cui la Società dispone di regolare licenza ;

È fatto espresso divieto ai Destinatari, di:

- diffondere e/o trasmettere, attraverso siti internet opere di terzi tutelate dal diritto d'autore in mancanza di accordi con i relativi titolari, o in violazione dei termini e delle condizioni previste in detti accordi;
- realizzare qualunque condotta finalizzata, in generale, alla duplicazione, di programmi per elaboratore protetti dal diritto d'autore o le banche di dati sulla memoria fissa del computer;
- scaricare dal web e installare programmi o applicazioni coperti dal diritto d'autore

4.2 Protocolli Specifici

4.2.1 Gestione software aziendali

Processi di interesse	- configurazione sw dispositivi individuali - sviluppo componenti sw

	- acquisto di beni (sw)
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ identificazione dei ruoli e delle responsabilità delle strutture aziendali che, per materia di competenza, i) gestiscono contratti che disciplinano la duplicazione, riproduzione, trasmissione o diffusione al pubblico di materiale/opere dell'ingegno protette da diritti d'autore o altri diritti connessi e ne verificano la corretta esecuzione; ii) verificano la corretta esecuzione dei contratti; iii) gestiscono le attività di autorizzazione al pagamento dei diritti d'autore ai titolari; iv) effettuano il pagamento dei diritti; ✓ regolamentazione delle modalità operative per lo svolgimento delle seguenti attività di: i) verifica, prima della duplicazione, riproduzione, trasmissione o diffusione al pubblico di opere dell'ingegno protette da diritti d'autore, del possesso delle autorizzazioni necessarie e del pagamento dei diritti d'autore o altri diritti connessi; ii) di attività di verifica sull'utilizzo delle opere dell'ingegno con le modalità e nei tempi contrattualizzati; ✓ prevedere, quale procedura base, l'utilizzo di hardware fornito direttamente dall'azienda ✓ nel caso di fabbisogno di software e/o di banche dati dotati di licenza d'uso, prevedere, quale procedura base, l'acquisizione da parte della società; nei casi in cui il dipendente intenda acquisire autonomamenteil prodotto, definire specifici criteri/protocolli autorizzativi che prevedano, comunque, creazione di copia del prodotto per i servizi centrali della società e tracciabilità della autorizzazione ✓ introdurre modalità operative per la gestione della protezione di licenze software, in particolare attraverso i) modalità e controlli applicabili sia in fase di individuazione dell'esigenza di acquisto di una licenza software sia in fase di implementazione della stessa; ii) criteri di identificazione/individuazione delle risorse aziendali a cui distribuire le licenze acquisite; iii) controlli periodici di corrispondenza tra le licenze acquisite e le licenze implementate a cura di un soggetto diverso dal responsabile della distribuzione/implementazione delle licenze; ✓ introduzione di una policy che regoli l'acquisto/l'utilizzo/la diffusione di banche dati o programmi di e-learning e materiale didattico scientifico

4.2.2 Gestione processi comunicazione aziendale

Processi di interesse	- gestione portali servizi applicativi Regione Puglia - gestione portale istituzionale Innova Puglia - produzione pubblicazioni - organizzazione eventi
Procedure/ regolamenti applicabili	
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	
Ulteriori protocolli da adottare	✓ tutti gli utenti coinvolti nei processi di upload/diffusione di documenti protetti da copyright dovrebbero essere debitamente autorizzati da livelli gerarchici superiori ; tali autorizzazioni dovrebbero essere periodicamente riviste e controllate ✓ tutto il personale che gestisce portali (aziendale, servizi applicativi regionali,..) ovvero che produce pubblicazioni, deve verificare attentamente l'esistenza di copyright su materiale di terzi utilizzato e agire conseguentemente nel rispetto della normativa ✓ riportare dati del copyright in pubblicazione portali, etc ✓ i processi di pubblicazione su portale devono sempre permettere di risalire all'autore materiale della specifica pagina ✓ definire clausole nei contratti con società esterne che curano la organizzazione di eventi o la produzione di pubblicazioni con cui i terzi si obbligano a non porre in essere alcun atto od omissione, a non dare origine ad alcun fatto, in particolare con riferimento all'utilizzo di materiale audio-visivo, da cui possa derivare una responsabilità ai sensi del d.lgs.231/01 ✓

5 FLUSSI INFORMATIVI SPECIFICI VERSO L'OdV

PROCESSO DA VERIFICARE	FLUSSO INFORMATIVO VERSO OdV	FREQUENZA
Gestione software aziendali	- elenco dei software licenziati utilizzati in azienda / numero di licenze relativo / scadenze ; - elenco delle banche dati licenziate utilizzate in azienda	Semestrale

Gestione processi comunicazione aziendale	- copia dei contratti a società di comunicazione (per eventi, pubblicazioni, etc) con clausola 231 per violazione diritti d'autore -	Annuale

6 DEFINIZIONI

OPERE DELL'INGEGNO PROTETTE : Ai fini della L.633/41 si intendono "*le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione.*
Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore"
Le opere dell'ingegno rientrano nella categoria dei beni immateriali che consistono in una creazione intellettuale ospitata su un supporto materiale.

PARTE SPECIALE G : REATI AMBIENTALI

1 AMBITO APPLICATIVO ED OBIETTIVI

Il decreto legislativo 7 luglio 2011, n. 121 (art. 2, comma 2) ha introdotto i reati ambientali nel d.lgs. 231/2001, con l'inserimento dell'art. 25-*undecies*.

2 LE FATTISPECIE DI REATO RICHIAMATE DAL D.LGS. 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati *ex* art. 5 del d.lgs. n. 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.

Al fine pertanto di divulgare la conoscenza degli elementi essenziali delle singole fattispecie di reato punibili ai sensi del d.lgs. 231/2001, si riporta di seguito una breve descrizione delle richiamate fattispecie di reato introdotte dal D.lgs. 121/2011 (con esclusione della disciplina di cui al d.lgs. 6 novembre 2007, n. 202, in quanto concernente esclusivamente l'inquinamento provocato da navi e dunque non rilevante per la Società).

Maggiori dettagli sono riportati in Allegato 1.G .

art. 727-*bis* c.p.	Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette
art. 733-*bis* c.p	Distruzione o deterioramento di habitat all'interno di un sito protetto
D.Lgs. 3 aprile 2006, n. 152, artt. 137,	(norme su acque reflue industriali)
D.Lgs. 3 aprile 2006, artt. 256, 257, 258, 259, 260, 260-*bis*, 279	Norme su gestione rifiuti : art 256 - Attività di gestione dei rifiuti non autorizzata art 257 - Bonifica dei siti Art.259 - Traffico illecito di rifiuti Art.260 - Attività organizzate per il traffico illecito di rifiuti Art.260-bis - Sistema informatico di controllo della tracciabilità dei rifiuti
Legge 7 febbraio 1992, n. 150, artt. 1 e 3-*bis*	Commercio internazionale di specie animali e vegetali minacciate di estinzione
Legge 28 dicembre 1993, n. 549, art. 3	(Misure a tutela dell'ozono stratosferico e dell'ambiente)
D.Lgs. 6 novembre 2007, n. 202, artt. 8 e 9	(inquinamento provocato dalle navi)

3 LE ATTIVITAôSENSIBILI AI FINI DEL D.LGS. 231/2001

L'art. 6, comma 2, lett. a) del Decreto indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo, 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 .

La complessiva analisi svolta con riferimento ad InnovaPuglia ha consentito, quindi, di individuare i processi "sensibili" in relazione alle aree di rischio correlate ai reati previsti dall'art. 25-*undecies* del D.Lgs 231/01.

1. **Smaltimento dei rifiuti**, con riferimento ai processi di :
   – dismissione strumentazione / dispositivi informatici e smaltimento materiali di consumo
   – gestione impiantistica e ambienti di lavoro

4 PROTOCOLLI PER LA FORMAZIONE E LôATTUAZIONE DELLE DECISIONI E SISTEMA DI CONTROLLO

4.1 Principi specifici di comportamento

Divieti

La presente Parte Speciale prevede l'espresso divieto - a carico degli Esponenti Aziendali, in via diretta, ed a carico dei Collaboratori esterni e Partner, tramite apposite clausole contrattuali - di:

- ✓ porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali da integrare le fattispecie di reato sopra considerate (art. 25-undecies del d.lgs. 231/2001);
- ✓ porre in essere, collaborare o dare causa alla realizzazione di comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato rientranti tra quelle sopra considerate, possano potenzialmente diventarlo.

Doveri

La presente sezione prevede l'espresso obbligo a carico dei soggetti sopra indicati di conoscere e rispettare tutte le misure atte a garantire la corretta gestione e smaltimento dei rifiuti.

4.2 Protocolli Specifici

4.2.1 Smaltimento dei rifiuti

Processi di interesse	– dismissione strumentazione / dispositivi informatici – gestione impiantistica e ambienti di lavoro
Procedure/ regolamenti	✓ *Manuale delle istruzioni operative per il controllo e le gestione dei rifiuti*

applicabili	*(ed. 1, rev 1, 11/2/2013)* ✓ Capitolato tecnico del contratto di "global service"
Poteri autorizzativi e di firma rilevanti per l'attività	
Tracciabilità nel sistema informativo aziendale	✓ Registro carico / scarico dei rifiuti ✓ Modulo FIR (Formulario Identificazione Rifiuti) ✓ Comunicazione periodica del MUD alla CCIAA ✓ Iscrizione al SISTRI
Ulteriori protocolli da adottare	✓ formalizzazione: (i) delle modalità di selezione e contrattualizzazione dei fornitori, con particolare riferimento alla verifica delle specifiche autorizzazioni; in particolare devono essere verificate a) la data di validità dell'autorizzazione, b) la tipologia e la quantità di rifiuti per i quali è stata rilasciata l'autorizzazione ad esercitare attività di smaltimento o recupero; c) la localizzazione dell'impianto di smaltimento d) il metodo di trattamento o recupero; Le verifiche preliminari e/o periodiche dovrebbero avere anche ad oggetto il tipo di manodopera utilizzata dal fornitore (con esclusione, ad esempio, delle imprese con alta incidenza di manodopera non qualificata) nonché una comparazione dei prezzi offerti rispetto a quelli di mercato, in modo da escludere fornitori che propongano prezzi immotivatamente bassi rispetto alla media di settore (ii) di divieti e prescrizioni comportamentali per i dipendenti e fornitori esterni; (iii) delle modalità di effettuazione delle comunicazioni alle Autorità competenti e delle istruzioni operative per effettuare la bonifica di siti nell'eventualità di inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee; (iv) dei controlli in merito al conferimento dei rifiuti prodotti da Emmegiesse nelle attività di manutenzione in canone ed extracanone

5 FLUSSI INFORMATIVI SPECIFICI VERSO L'OdV

All'OdV deve essere inviata copia dei reports periodici in materia ambientale segnatamente oltre che:

PROCESSO DA VERIFICARE	FLUSSO INFORMATIVO VERSO OdV	FREQUENZA
Smaltimento dei rifiuti	- copia dell'ordine al fornitore incaricato dei servizi di smaltimento dei rifiuti; - verbali di ispezione in materia ambientale da parte di Enti Pubblici e/o Autorità di controllo (es. ARPA, ASL, etc.); - segnalazione di modifica degli impianti tecnologici, dei macchinari, dei processi produttivi, idonea ad alterare l'impatto ambientale	Annuale annuale (ovvero a seguito di ispezioni) annuale

6 DEFINIZIONI

ACQUE REFLUE INDUSTRIALI: "qualsiasi tipo di acque reflue scaricate da edifici od impianti in cui si svolgono attività commerciali o di produzione di beni, diverse dalle acque reflue domestiche derivanti da insediamenti di tipo residenziale) e dalle acque meteoriche di dilavamento".

RIFIUTI : "qualsiasi sostanza od oggetto di cui il detentore si disfi o abbia l'intenzione o abbia l'obbligo di disfarsi"

ALLEGATO 1 : LE FATTISPECIE DI REATO

1.A Reati nei rapporti con la P.A.

art. 24 *Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico*

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
art 316 bis c.p.	***Malversazione a danno dello Stato o dell'Unione Europea***	"Chiunque, estraneo alla pubblica amministrazione, avendo ottenuto dallo Stato o da altro ente pubblico o dalle Comunità europee contributi, sovvenzioni o finanziamenti destinati a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse, non li destina alle predette finalità, è punito con la reclusione da sei mesi a quattro anni."	Questo delitto consiste nell'effettuare un mutamento di destinazione di contributi, sovvenzioni o finanziamenti ottenuti dallo Stato, da altri enti pubblici o dalle Comunità europee, per il fine di impiegarli nella realizzazione di opere o nello svolgimento di attività di pubblico interesse. Il delitto si consuma anche se solo una parte dei fondi viene distratta ed anche nel caso in cui la parte correttamente impiegata abbia esaurito l'opera o l'iniziativa cui l'intera somma era destinata. La condotta criminosa prescinde dal modo in cui sono stati ottenuti i fondi e si realizza solo in un momento successivo all'ottenimento dei fondi stessi. Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea, non si 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). Il reato può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che non vengano successivamente destinati alle finalità per cui erano stati erogati. Dalla lettura del predetto articolo si evince che si tratta di un reato comune, ove il soggetto attivo può essere qualsiasi privato estraneo alla pubblica amministrazione. Più in particolare, il soggetto attivo deve necessariamente essere estraneo alla pubblica amministrazione ossia non deve essere un pubblico ufficiale o un incaricato di un pubblico servizio. Invece, **il soggetto passivo del delitto di cui all'art. 316 c.p. è l'organismo pubblico che ha erogato il finanziamento (Stato, Regione, Provincia, Comune, un ente pubblico o le Comunità europee).**

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			Inoltre, **il bene giuridico protetto dalla fattispecie penale incriminatrice della "Malversazione a danno dello Stato" è costituito dagli interessi economici e finanziari della Pubblica Amministrazione.** Più in dettaglio, la norma si prefigge la finalità di tutelare il buon andamento della Pubblica Amministrazione sotto il particolare profilo della corretta gestione ed allocazione delle risorse pubbliche. Inoltre, è un reato senza evento naturalistico, di danno, di mera condotta (omissiva) ed a forma libera, in quanto la legge non tipizza le modalità della sua esecuzione, dove il tentativo è ammissibile. **La condotta omissiva di questo delitto consiste nel non destinare i contributi, le sovvenzioni oppure i finanziamenti ricevuti alle finalità di pubblico interesse, per cui erano stati erogati.** L'oggetto materiale del reato di cui in oggetto viene rappresentato dai contributi, dalle sovvenzioni e dai finanziamenti destinati dallo Stato, da altro ente pubblico, dalle Comunità Europee, a favorire iniziative dirette alla realizzazione di opere o allo svolgimento di attività di pubblico interesse. Più in dettaglio, si osserva che i contributi e le sovvenzioni costituiscono attribuzioni patrimoniali a fondo perduto mentre, invece, i finanziamenti sono degli atti negoziali generalmente caratterizzati da un obbligo di restituzione totale o parziale. Inoltre, si deve rilevare, altresì, che le predette erogazioni di somme di denaro devono essere concesse a condizioni più favorevoli di quelle di mercato. Tuttavia, si osserva, altresì, che l'elemento oggettivo del reato di cui all'art. 316 bis c.p. (Malversazione a danno dello Stato) si compone di un presupposto e della condotta. Il presupposto consiste nell'avere l'agente, estraneo alla pubblica amministrazione, ottenuto dallo Stato o da altro ente pubblico un contributo, una sovvenzione o un finanziamento destinati a una determinata finalità pubblica. La condotta consiste nell'avere distratto, anche parzialmente, la somma ottenuta dalla predetta finalità, senza che rilevi che l'attività programmata si sia comunque svolta. *(Cassazione penale, sezione VI, sentenza 17 settembre 1998, n. 9881)* Inoltre, il delitto previsto dall'art. 316 bis c.p. – che consiste nella elusione del vincolo di destinazione gravante sui finanziamenti erogati per la realizzazione di una determinata finalità pubblica – si perfeziona nel momento in cui si attua la mancata destinazione dei fondi allo scopo per il quale erano stati ottenuti. *(Cassazione penale, sezione VI, sentenza 28 novembre 2002, n. 40375)* Fonte: http://www.overlex.com/leggiarticolo.asp?id=1808
	Indebita percezione	"Salvo che il fatto costituisca il reato previsto dall'articolo 640-bis, chiunque mediante l'utilizzo o la presentazione di	La fattispecie di delitto si realizza qualora la società - tramite chiunque (anche un soggetto esterno alla società stessa) - consegua per sé o per altri erogazioni dallo

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
art 316 ter c.p	***di erogazioni in danno dello Stato o delle Comunità europee***	dichiarazioni o di documenti falsi o attestanti cose non vere, ovvero mediante l'omissione di informazioni dovute, consegue indebitamente, per sé o per altri, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati dallo Stato, da altri enti pubblici o dalle Comunità europee è punito con la reclusione da sei mesi a tre anni. Quando la somma indebitamente percepita è pari o inferiore a euro 3.999,96 si applica soltanto la sanzione amministrativa del pagamento di una somma di denaro da euro 5.164 a euro 25.822. Tale sanzione non può comunque superare il triplo del beneficio conseguito.	Stato, da altri enti pubblici o dalle Comunità europee, mediante una condotta consistente in qualsiasi tipo di utilizzo (ad es. presentazione) di dichiarazioni (scritte o orali), o di altra documentazione materialmente e/o ideologicamente falsa ovvero attraverso l'omissione di informazioni dovute. La fattispecie si consuma con l'avvenuto ottenimento delle erogazioni (che costituisce l'evento tipico del reato). Questa fattispecie costituisce una "ipotesi speciale" rispetto alla più ampia fattispecie di truffa aggravata per il conseguimento di erogazioni pubbliche di cui all'art. 640-*bis* c.p. Si applicherà la norma qui in esame (e cioè l'art. 316-*ter* c.p.) tutte le volte che ne ricorrano i requisiti specifici da essa contemplati; si ricade, invece, nell'ipotesi della fattispecie più generale (e più grave) solo qualora gli strumenti ingannevoli usati per ottenere le erogazioni pubbliche siano diversi da quelli considerati nell'art. 316-*ter* ma comunque riconducibili alla nozione di "artifici o raggiri" richiamata dall'art. 640-*bis* c.p.. Il reato qui in esame (art. 316-*ter* c.p.) si configura come ipotesi speciale anche nei confronti dell'art. 640, comma 2, n. 1, c.p. (truffa aggravata in danno dello Stato), rispetto al quale l'elemento "specializzante" è dato non più dal tipo di artificio o raggiro impiegato, bensì dal tipo di profitto conseguito ai danni dell'ente pubblico ingannato. Profitto che nella fattispecie più generale, testé richiamata, non consiste nell'ottenimento di una erogazione ma in un generico vantaggio di qualsiasi altra natura. *T*ale ipotesi di reato si configura nei casi in cui – mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi ovvero 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. Il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti. Il delitto di indebita percezione di erogazioni a danno dello Stato è in rapporto di sussidiarietà, e non di specialità, con quello di truffa aggravata per il conseguimento di erogazioni pubbliche, con la conseguenza che il primo è configurabile soltanto laddove difettino nella condotta gli estremi del secondo. (*Fonte: Altalex Massimario. Cfr. nota su Altalex Mese)*
art 640 c. 2 c.p.	***Truffa in danno dello Stato o di altro ente***	Chiunque, con artifizi o raggiri, inducendo taluno in errore,procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre	La norma fa riferimento alla generica ipotesi di truffa (art. 640 c.p.), aggravata dal fatto che il danno economico derivante dall'attività ingannatoria del reo ricade sullo Stato o su altro ente pubblico.

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
	pubblico o delle Comunità europee	anni e con la multa da € 5 1,00 a € 1.032,00. La pena è della reclusione da uno a cinque anni e della multa da € 309,00 a € 1.549,00: se il fatto, è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare; se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante.	La condotta consiste, sostanzialmente, in qualsiasi tipo di menzogna (compreso l'indebito silenzio su circostanze che devono essere rese note) tramite la quale si ottiene che taluno cada in errore su qualcosa e compia, di conseguenza, un atto di disposizione che non avrebbe compiuto se avesse conosciuto la verità. Per la consumazione del reato occorre che sussista, oltre a tale condotta, il conseguente profitto di qualcuno (chiunque esso sia, anche diverso dall'ingannatore) e il danno dello Stato o dell'ente pubblico. 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 o ad altro Ente Pubblico o all'Unione Europea. Esempio: nella preparazione di documenti per la partecipazione a procedure di gara, si forniscano informazioni non veritiere (supportate da documentazione falsificata), al fine di conseguire l'aggiudicazione della gara stessa.
art 640 bis c.p.	***Truffa aggravata per il conseguimento di erogazioni pubbliche***	La pena è della reclusione da uno a sei anni e si procede d'ufficio se il fatto di cui all'articolo 640 riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee.	La fattispecie si realizza se il fatto previsto dall'art. 640 c.p. (ossia la truffa) riguarda contributi, finanziamenti, mutui agevolati ovvero altre erogazioni dello stesso tipo, comunque denominate, concessi o erogati da parte dello Stato, di altri enti pubblici o delle Comunità europee. 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.
art. 640 ter c.p.	***Frode informatica in danno dello Stato o di altro Ente Pubblico***	Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma	

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
		dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante	

Art. 25 *Concussione, induzione indebita a dare o promettere utilità e corruzione*

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
a***rt. 317 c.p***.	***Concussione***	Il pubblico ufficiale che, abusando della sua qualità o dei suoi poteri, costringe taluno a dare o a promettere indebitamente, a lui o a un terzo, denaro o altra utilità è punito con la reclusione da sei a dodici anni (art. modificato dalla Legge Anticorruzione del Novembre 2012)	Il reato di concussione è distinto dalla corruzione per il soggetto attivo: nella concussione è il pubblico ufficiale che costringe, abusando dei suoi poteri, il privato a pagare la tangente; nella corruzione è il privato che "convince" con denaro o altra utilità il pubblico ufficiale ad agire nel suo interesse. Il reato di concussione,pertanto, si configura nel caso in cui il funzionario dell'ente abusando della sua qualità o dei suoi poteri, costringe un soggetto privato a dare, a lui o a terzi, denaro o altre utilità. In tale ipotesi di illecito assume un ruolo prevalente la prevaricazione esercitata dal funzionario pubblico sul privato per dare origine ovvero incuneare nel soggetto passivo uno stato di timore idoneo a rimuovere la volontà. Le ipotesi di responsabilità dell'ente per concussione sono poco significative, in quanto il comportamento concussivo dovrebbe essere realizzato nell'interesse o a vantaggio dell'ente e non, come accade di solito, nell'esclusivo interesse del concussore.
art. 318 c.p.	***Corruzione per l'esercizio della funzione***	Il pubblico ufficiale che, per l'esercizio delle sue funzioni o dei suoi poteri, indebitamente riceve, per sé o per un terzo, denaro o altra utilità o ne accetta la promessa è punito con la reclusione da uno a cinque anni. (art. modificato dalla Legge Anticorruzione del Novembre 2012)	Tale ipotesi di reato si configura nel caso in cui un pubblico ufficiale riceva, per sé o per altri, denaro o altri vantaggi per compiere, omettere o ritardare atti del proprio ufficio (determinando un vantaggio in favore dell'offerente). Qui, come è chiaro, si tratta di atti che non contrastano con i doveri d'ufficio. Il reato può essere integrato anche quando il pubblico ufficiale riceve la retribuzione

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			per un atto d'ufficio da lui già compiuto.
art 319 c.p.	***Corruzione per un atto contrario ai doveri di ufficio***	Il pubblico ufficiale che, per omettere o ritardare o per aver omesso o ritardato un atto del suo ufficio, ovvero per compiere o per aver compiuto un atto contrario ai doveri di ufficio, riceve, per sé o per un terzo, denaro od altra utilità, o ne accetta la promessa, è punito con la reclusione da quattro a otto anni. (art. modificato dalla Legge Anticorruzione del Novembre 2012)	
art. 319-bis c.p.	***Circostanze aggravanti.***	La pena è aumentata se il fatto di cui all'art. 319 ha per oggetto il conferimento di pubblici impieghi o stipendi o pensioni o la stipulazione di contratti nei quali sia interessata l'amministrazione alla quale il pubblico ufficiale appartiene	
art. 319-ter c.p.	***Corruzione in atti giudiziari***	Se i fatti indicati negli articoli 318 e 319 sono commessi per favorire o danneggiare una parte in un processo civile, penale o amministrativo, si applica la pena della reclusione da quattro a dieci anni. Se dal fatto deriva l'ingiusta condanna di taluno alla reclusione non superiore a cinque anni, la pena è della reclusione da cinque a dodici anni; se deriva l'ingiusta condanna alla reclusione superiore a cinque anni o all'ergastolo, la pena è della reclusione da sei a venti anni (art. modificato dalla Legge Anticorruzione del Novembre 2012)	Tale ipotesi di reato si configura nel caso in cui la società sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso, corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro pubblico ufficiale).
art 319 quater c.p	***Induzione indebita a dare o promettere utilità***	Salvo che il fatto costituisca più grave reato, il pubblico ufficiale o l'incaricato di pubblico servizio che, 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 è punito con la reclusione da tre a otto anni. Nei casi previsti dal primo comma, chi dà o promette denaro o altra utilità è punito con la reclusione fino a tre anni» (art. aggiunto dalla Legge Anticorruzione del Novembre 2012)	Dal punto di vista della responsabilità amministrativa degli enti, il reato in materia di corruzione tra privati, di cui al terzo comma dell'articolo 2635 c.c. richiamato dal Decreto, contempla quindi la sola ipotesi di Soggetti Apicali o Soggetti Subordinati che, quali soggetti attivi, diano o promettano denaro o altra utilità a: (i) amministratori, direttori generali, dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori; o (ii) coloro che sono sottoposti alla direzione o alla vigilanza di uno dei soggetti di cui al punto (i) che precede.

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
art 320 c.p	***Corruzione di persona incaricata di un pubblico servizio***	Le disposizioni degli artt. 318 e 319 si applicano anche all'incaricato di pubblico servizio. (art. modificato dalla Legge Anticorruzione del Novembre 2012)	
art 321 c.p.	***Pene per il corruttore***	Le pene stabilite nel primo comma dell'articolo 318, nell'articolo 319, nell'articolo 319-bis, nell'art. 319-ter, e nell'articolo 320 in relazione alle suddette ipotesi degli articoli 318 e 319, si applicano anche a chi dà o promette al pubblico ufficiale o all'incaricato di un pubblico servizio il denaro od altra utilità.	
art 322 c.p.	***Istigazione alla corruzione***	Chiunque offre o promette denaro od altra utilità non dovuti ad un pubblico ufficiale o ad un incaricato di un pubblico servizio, per l'esercizio delle sue funzioni o dei suoi poteri, soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nel primo comma dell'articolo 318, ridotta di un terzo. Se l'offerta o la promessa è fatta per indurre un pubblico ufficiale o un incaricato di un pubblico servizio ad omettere o a ritardare un atto del suo ufficio, ovvero a fare un atto contrario ai suoi doveri, il colpevole soggiace, qualora l'offerta o la promessa non sia accettata, alla pena stabilita nell'articolo 319, ridotta di un terzo. La pena di cui al primo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro o altra utilità per l'esercizio delle sue funzioni o dei suoi poteri. La pena di cui al secondo comma si applica al pubblico ufficiale o all'incaricato di un pubblico servizio che sollecita una promessa o dazione di denaro od altra utilità da parte di un privato per le finalità indicate dall'articolo 319. (art. modificato dalla Legge Anticorruzione del Novembre 2012)	Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale o incaricato di pubblico servizio rifiuti l'offerta illecitamente avanzatagli.
art 322 bis c.p	***Peculato,***	Le disposizioni degli articoli 314, 316, da 317 a 320 e 322,	

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
	concussione, corruzione e istigazione alla corruzione di membri degli organi delle Comunità Europee e di funzionari delle Comunità Europee e di Stati Esteri	terzo e quarto comma, si applicano anche: 1) ai membri della Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei conti delle Comunità europee; 2) ai funzionari e agli agenti assunti per contratto a norma dello statuto dei funzionari delle Comunità europee o del regime applicabile agli agenti delle Comunità europee; 3) alle persone comandate dagli Stati membri o da qualsiasi ente pubblico o privato presso le Comunità europee, che esercitino funzioni corrispondenti a quelle dei funzionari o agenti delle Comunità europee; 4) ai membri e agli addetti a enti costituiti sulla base dei Trattati che istituiscono le Comunità europee; 5) a coloro che, nell'ambito di altri Stati membri dell'Unione europea, svolgono funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio; 5-bis) ai giudici, al procuratore, ai procuratori aggiunti, ai funzionari e agli agenti della Corte penale internazionale, alle persone comandate dagli Stati parte del Trattato istitutivo della Corte penale internazionale le quali esercitino funzioni corrispondenti a quelle dei funzionari o agenti della Corte stessa, ai membri ed agli addetti a enti costituiti sulla base del Trattato istitutivo della Corte penale internazionale . Le disposizioni degli articoli 319-quater, secondo comma, 321 e 322, primo e secondo comma, si applicano anche se il denaro o altra utilità è dato, offerto o promesso: 1) alle persone indicate nel primo comma del presente articolo; 2) a persone che esercitano funzioni o attività corrispondenti a quelle dei pubblici ufficiali e degli incaricati di un pubblico servizio nell'ambito di altri Stati esteri o organizzazioni pubbliche internazionali, qualora il fatto sia commesso per procurare a sé o ad altri un indebito vantaggio in operazioni economiche	

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
		internazionali ovvero al fine di ottenere o di mantenere un'attività economica finanziaria. Le persone indicate nel primo comma sono assimilate ai pubblici ufficiali, qualora esercitino funzioni corrispondenti, e agli incaricati di un pubblico servizio negli altri casi. (art. modificato dalla Legge Anticorruzione del Novembre 2012 e da L237/2012 art 10, c. 1)	

1.B Reati societari

art. 25-ter *Reati societari*

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
Art. 2621 c.c.	***False comunicazioni sociali***	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 valutazioni 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 od amministrati dalla società per conto di terzi. La punibilità è esclusa se le falsità o le omissioni non alterano in modo sensibile la rappresentazione della situazione economica, patrimoniale o finanziaria della società o del gruppo al quale essa appartiene. La punibilità è comunque esclusa se le falsità o le omissioni determinano una variazione del risultato economico di esercizio, al lordo delle imposte, non superiore al 5% o una variazione del patrimonio netto non superiore all'1%. In ogni caso il fatto non è punibile se conseguenza di	Tale ipotesi di reato si configura nei casi in cui, con l'intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri ingiusto profitto, nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico, si espongono fatti materiali non rispondenti al vero ancorché oggetto di valutazioni, ovvero si 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 a indurre in errore i Destinatari sulla predetta situazione. La condotta deve essere rivolta a conseguire per se o per altri un ingiusto profitto. Le informazioni false o omesse devono essere rilevanti e tali da alterare sensibilmente la rappresentazione della situazione economica, patrimoniale o finanziaria della società. Si tratta di reato proprio in quanto i soggetti attivi della condotta illecita possono essere esclusivamente: (i) gli amministratori (coloro che fanno parte dell'organo della società che svolge attività di gestione e di rappresentanza.) (ii) i direttori generali;

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
		valutazioni estimative che, singolarmente considerate, differiscono in misura non superiore al 10% da quella corretta.	(iii) i sindaci; (iv) i liquidatori; (v) i dirigenti preposti alla redazione dei documenti contabili societari (limitatamente alle sole società che siano obbligate per legge alla tenuta di documentazione contabile). Fattispecie oggettiva del reato: le condotte alternative di reato sono le seguenti: (i) esposizione di fatti materiali non rispondenti al vero ancorché oggetto di valutazioni; o (ii) omissione di informazioni la cui comunicazione è imposta per legge in merito alla situazione economica, patrimoniale, o finanziaria della società. La condotta decettiva di cui al punto (i) si sostanzia nell'attestare falsamente la veridicità delle voci contenute nel bilancio o in altri documenti contabili, ovverosia che queste ultime corrispondono alla reale situazione economica, patrimoniale, o finanziaria della società. La mancata corrispondenza è il risultato di una scelta non consentita dalla legge in merito criteri da seguire nella valutazione delle poste di bilancio relative alla condizione economica della società. Posto il dato letterale, che effettua un esplicito riferimento a "fatti materiali" ancorché oggetto di valutazione, si ritiene che siano prive di rilevanza le mere valutazioni/opinioni eventualmente contenute in altri documenti contabili. In riferimento alla condotta sub (ii), l'omissione deve avere ad oggetto informazioni che derivano da obblighi giuridici di comunicazione; la violazione di un simile obbligo è ravvisabile in tutti quei casi in cui l'omissione determini l'impossibilità, per i soci e/o per i terzi, di avere contezza degli accadimenti societari. Posto che la radicale assenza di comunicazione è autonomamente sanzionata come illecito amministrativo ai sensi dell'art. 2630 c.c.187, si ritiene che l'omissione rilevante ai sensi dell'art. 2621 c.c. non possa essere totale ma piuttosto parziale, concretizzandosi in una sorta di reticenza realizzata con l'occultamento di informazioni rilevanti e finalizzata ad alterare il quadro complessivo della situazione economica, patrimoniale e finanziaria della società. Le condotte in oggetto riguardano i **bilanci**, le relazioni e le altre

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			comunicazioni sociali previste dalla legge e dirette ai soci o al pubblico: sono pertanto escluse dall'ambito di applicazione della norma quelle condotte illecite aventi ad oggetto le comunicazioni interorganiche ancorché quelle rivolte ad un unico destinatario. Per quanto concerne le **relazioni**, esse possono costituire una sorta di documento informativo riconducibile a particolari atti della vita societaria; tra le relazione idonee allo scopo si annoverano, a titolo di esempio, la relazione sulla gestione e quella che accompagna il bilancio straordinario. L'ultima categoria, quella delle **comunicazioni sociali**, costituisce categoria residuale in cui è possibile collocare tutte le altre comunicazione "tipiche" previste dalla legge. La punibilità delle condotte sopra descritte è subordinata alla verifica dell'effettiva capacità ingannatoria delle stesse che deve essere tale da indurre in errore i destinatari per quanto concerne la situazione economica, patrimoniale e/o finanziaria della società. Inoltre, i commi 3 e 4 introducono soglie di rilevanza penale al di sotto delle quali la punibilità delle condotte (sub (i) e (ii)) è esclusa; tali soglie si configurano come: * **qualitative**, ovvero è prevista l'esclusione della punibilità nel caso in cui la falsità o le omissioni non siano tali da alterare in modo sensibile la rappresentazione della situazione economica, patrimoniale e finanziaria della società; e/o * **quantitative**, con l'indicazione di specifiche soglie percentuali di rilevanza che escludono la perseguibilità del falso che abbia determinato una variazione del risultato economico di esercizio al lordo delle imposte non superiore al 5% o una variazione del patrimonio netto non superiore all'1% Le soglie qualitative e quelle quantitative devono operare congiuntamente ritenendosi esclusa la punibilità di un'alterazione che superi le percentuali stabilite senza però determinare anche un'alterazione sensibile della situazione economica, patrimoniale e finanziaria della società. Qualora tali soglie non vengano congiuntamente superate le condotte delittuose descritte potranno dare luogo all'insorgere di una ipotesi di illecito amministrativo (e non penale) punibile con sanzioni interdittive e pecuniarie, la cui quantificazione non è espressamente stabilita dalla norma.

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			La fattispecie di cui all'art. 2621 cod. civ. sanziona la condotta ivi indicata a prescindere dal verificarsi del danno per soci o creditori. **Elemento soggettivo**: rispetto all'induzione in errore dei destinatari della comunicazione (i soci o il pubblico), si tratta di **dolo intenzionale** mentre, in relazione al conseguimento di un ingiusto profitto, per sé o per gli altri, si configura il **dolo specifico**.
Art. 2622 c.c.	***False comunicazioni sociali in danno della società, dei soci o dei creditori***	*(si riportano solo i commi rilevanti ai fini D.Lgs 231/2001)* 1. 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 valutazioni, 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. 3. 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, (*società quotate*) la pena per i fatti previsti al primo comma è da uno a quattro anni e il delitto è procedibile d'ufficio.	Tale reato si realizza nel caso in cui a seguito della tenuta di una della condotte previste dall'articolo 2621 c.c. si cagioni un danno patrimoniale alla società, ai soci o ai creditori. Tale reato è procedibile a querela salvo che riguardi società quotate, nel qual caso è procedibile d'ufficio, caso che, comunque, non è applicabile a InnovaPuglia. L'oggetto materiale della condotta e le soglie di rilevanza sono le medesime già analizzate in sede di commento dell'art. 2621 c.c.; le due fattispecie sono infatti complementari. Ai sensi dei commi 1 e 3 dell'articolo in commento, gli illeciti possono essere perpetrati rispettivamente nell'ambito di società non quotate o, piuttosto, nell'ambito di società quotate, soggette alle disposizioni della parte IV, titolo III, capo II, del TUF. La scorretta rappresentazione delle poste di bilancio, effettuata attraverso l'esposizione di fatti non corrispondenti al vero e/o con la parziale omissione di informazioni potrebbe potenzialmente tradursi nella creazione di riserve occulte illiquide alimentate dalla sottovalutazione poste attive o dalla sopravvalutazione di poste passive.

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			Posto che le attività rilevanti in tal senso sono connesse alla redazione del bilancio e alla stima delle poste contabili, è opportuno porre attenzione non solo al rispetto delle norme regolamentari previste in materia ma, più in generale, al rispetto del principio di correttezza nella redazione delle comunicazioni sociali. Le funzioni aziendali maggiormente a rischio sono quelle dell'ambito **amministrativo/contabile** coinvolte nella predisposizione dei documenti contabili e delle relazioni societarie aventi ad oggetto la situazione economico/finanziaria della società.
Art. 2625 c.c.	***Impedito controllo***	*(Solo il 2° comma è rilevante ai fini D.Lgs 231/2001)* 1. Gli amministratori che, occultando documenti o con altri idonei artifici, impediscono o comunque ostacolano lo svolgimento delle attività di controllo legalmente attribuite ai soci, ad altri organi sociali, sono puniti con la sanzione amministrativa pecuniaria fino a 10.329 euro. 2. 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.	Gli Amministratori, anche attraverso collaboratori all'uopo istruiti, non rispettando la richiesta di informazioni da parte dei soci e della società di revisione, occultano, anche attraverso artifici e raggiri, documentazione utile a rappresentare i processi aziendali (ad esempio, esibizione parziale o alterata di detta documentazione). **Soggetto attivo:** gli amministratori della società; si tratta di reato proprio. **Fattispecie oggettiva della condotta:** la condotta richiamata dalla norma in commento si sostanzia nell'impedire o nell'ostacolare lo svolgimento delle attività di controllo, legalmente attribuite ai soci, ad altri organi sociali, attraverso l'occultamento di documenti o con altri idonei artifici determinando un danno ai soci. E' esclusa l'applicabilità dell'art. 2625 c.c. nel caso in cui gli ostacoli o gli impedimenti siano facilmente superabili o determinino un ritardo minimo nelle attività di controllo Al primo comma, che esula dalla previsione di un danno, è riconducibile un mero illecito amministrativo non rilevante ai sensi del D.Lgs. 231/2001. Il secondo comma invece sancisce la punibilità di un illecito penale che si fonda sul danno arrecato ai soci per mezzo della condotta illecita. Solo in tale ultima circostanza, qualora l'illecito sia commesso nell'interesse o a vantaggio della società, può ravvisarsi responsabilità dell'ente.

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			Il controllo da parte degli organi societari, dei soci e della società di revisione può avere ad oggetto qualunque aspetto della vita sociale con particolare riferimento però alle attività amministrativo/contabili. Risulta opportuno rafforzare l'attività di *reporting* verso organi di controllo/garanzia quale ad esempio il collegio sindacale in caso di violazioni o presunte tali. Inoltre, il comportamento degli amministratori volto ad impedire ai sindaci e/o ai dipendenti dei sindaci l'accesso e l'analisi di documenti riservati dovrebbe automaticamente determinare l'attivazione di una immediata verifica dai parte dei sindaci stessi.
Art. 2626 c.c.	***Indebita restituzione dei conferimenti***	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.	**Soggetto attivo:** gli amministratori della società; si tratta infatti di reato proprio. Dal novero dei soggetti attivi manca il socio che risulta punibile, per concorso eventuale, solo qualora realizzi una condotta diversa ed ulteriore rispetto a quella tipica dell'articolo in commento (*e.g.* istigazione degli amministratori a commettere il reato) **Fattispecie oggettiva della condotta:** le condotte alternative di reato si articolano nella: (i) restituzione di conferimenti ai soci al di fuori dei casi previsti dalla legge; (ii) liberazione degli stessi dall'obbligo di eseguirli. In riferimento alla condotta *sub* (i), per conferimenti si devono intendere le prestazioni a cui i soci si obbligano al fine di costituire il capitale sociale della società. Non assume pertanto rilevanza, ai sensi dell'articolo in commento, la restituzione di apporti non imputati a capitale. La restituzione può avvenire tanto in forma diretta quanto indiretta nonché, per espressa previsione normativa, in forma simulata. La restituzione simulata può avvenire con comportamenti leciti, quali, ad esempio, (i) la concessione di un prestito senza prospettive di restituzione, (ii) (ii) la stipulazione di contratti a prestazioni sproporzionate in danno della società, e (iii) (iii) attraverso operazioni già autonomamente e penalmente rilevanti (si veda l'articolo 2629).

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			Anche in relazione alla liberazione dei soci dall'obbligo di eseguire integralmente i conferimenti, è possibile ipotizzare ipotesi di simulazione qualora si verifichi, ad esempio, la compensazione del debito di conferimento con un credito fittizio del socio verso la società. Posto che la restituzione di conferimenti grava inizialmente sulla riserva legale e solo successivamente, una volta esaurita questa, va a intaccare il capitale sociale, l'illecito di cui all'articolo 2626 viene in essere solo in tale ultimo momento ovverosia in presenza di una riduzione fraudolenta del capitale. In entrambi i casi, per la sussistenza dell'elemento oggettivo del reato, è necessario che la restituzione avvenga al di fuori dell'ipotesi di legittima riduzione del capitale sociale ovvero una riduzione effettiva e non anche meramente nominale, in presenza di una delibera assembleare di riduzione del capitale sociale. La norma punisce la una condotta volta a minare l'integrità del capitale sociale che si realizza attraverso la "sottrazione" di cespiti dall'attivo a vantaggio dei i soci; ad essere lesa è, *in primis*, la società stessa. Risulta pertanto improbabile che il reato in commento possa essere compiuto nell'interesse o a vantaggio dell'ente, così come richiesto dal decreto al fini dell'autonoma responsabilità dell'ente. Ciò posto, si ritiene che il rischio di commissione del reato di indebita restituzione di conferimenti possa rilevare in relazione ai soli rapporti di gruppo, ovverosia qualora una società venga liberata dall'esecuzione dei conferimenti a cui si era obbligata nei confronti di un'altra società del gruppo e/o riesca a farsi restituire gli *asset* già conferiti.
Art. 2627 c.c.	***Illegale ripartizione degli utili e delle riserve***	Salvo che il fatto non costituisca più grave reato, gli amministratori che ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero che ripartiscono riserve, anche non costituite con utili, che non possono per legge essere distribuite, sono puniti con l'arresto fino ad un anno. La restituzione degli utili o la ricostituzione delle riserve prima	**Soggetto attivo:** gli amministratori della società, titolari del potere di ripartire gli utili sociali; si tratta infatti di reato proprio. Dal novero dei soggetti attivi manca il socio che risulta punibile, per concorso eventuale, solo qualora realizzi una condotta diversa ed ulteriore rispetto a quella tipica dell'articolo in commento (*e.g.* istigazione degli amministratori a commettere il reato).

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
		del termine previsto per l'approvazione del bilancio estingue il reato.	**Fattispecie oggettiva della condotta:** le condotte alternative di reato si articolano nella: (i) ripartizione di utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva; (ii) ripartizione di riserve, anche non costituite con utili, che non possono per legge essere distribuite. La "ripartizione" implica l'effettiva fuoriuscita di mezzi di pagamento dal patrimonio sociale, con la conseguenza che l'iscrizione di un credito per dividendi in favore dei soci non determina l'insorgere di responsabilità ai sensi dell'articolo in commento. L'oggetto materiale della condotta è costituito dagli utili non effettivamente conseguiti o che, per legge, devono essere destinati a riserva; tali utili devono intendersi come gli "utili complessivi di bilancio" che si sostanziano nell'incremento del patrimonio conseguito nell'anno di riferimento e di eventuali utili (o perdite) di esercizi precedenti non distribuiti. La condotta criminosa può avere ad oggetto anche la sola distribuzione di acconti sugli utili, distribuiti ai soci prima della chiusura dell'esercizio di riferimento, purché tali acconti siano riconducibili a utili non effettivamente conseguiti o destinati per legge a riserva. Infine, la presenza della clausola di riserva ("*salvo che il fatto non costituisca più grave reato*") consente di individuare ulteriori illeciti che potrebbero essere perpetrati attraverso le condotte proprie del reato di illegale ripartizione di utili e riserve ovverosia appropriazione indebita (art. 646 c.c.), infedeltà patrimoniale (art. 2634) e aggiotaggio (art. 2637) (il reato di aggiotaggio verrà in essere solo nel caso in cui la ripartizione di utili e/o acconti costituisca un artificio idoneo ad alterare sensibilmente il prezzo delle azioni) Posto che la condotta illecita in commento mina l'integrità del capitale sociale attraverso la "sottrazione" di riserve e/o utili sociali, a essere lesa è, *in primis*, la società stessa. Risulta pertanto improbabile che il reato in commento possa essere compiuto nell'interesse o a vantaggio dell'ente, così come richiesto dal Decreto al fini della sua autonoma responsabilità. Avendo il reato natura contravvenzionale è punibile anche a titolo di colpa (negligenza, imperizia, errore)

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
Art. 2628 c.c.	***Illecite operazioni sulle azioni o quote sociali o della società controllante***	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.	Il reato in commento interessa gli intermediari finanziari in qualità di emittenti e nel caso in cui siano incaricati di acquistare azioni di un emittente con successivo trasferimento della proprietà in capo allo stesso (*e.g.* operazioni di *buy-back*, attività di sostegno della liquidità tramite riacquisto). NON APPLICABILE A INNOVAPUGLIA
Art. 2629 c.c.	***Operazioni in pregiudizio dei creditori***	Gli amministratori che, in violazione delle disposizioni di legge a tutela dei creditori, effettuano riduzioni del capitale sociale o fusioni con altra società o scissioni, cagionando 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.	**Fattispecie oggettiva della condotta:** la condotta criminosa si realizza in presenza di eventi modificativi del capitale che cagionino un danno patrimoniale ai creditori ovverosia: (i) riduzione del capitale sociale; e (ii) fusione, scissione della società. Tali eventi presuppongono una deliberazione assembleare straordinaria che comporta una modifica dell'atto costitutivo effettivamente lesiva per i creditori stessi. Per quanto concerne la riduzione di capitale, non rilevano i casi di riduzione nominale (*e.g.* riduzione per perdite o riduzione al di sotto del limite legale) che si concretizzano in mere operazioni contabili finalizzate ad adeguare il capitale al valore del patrimonio sociale. In relazione alle operazioni di fusione e di scissione, esse si articolano in più fasi (redazione del progetto di fusione/scissione *ex* art. 2501-*ter*; deliberazione dell'assemblea straordinaria *ex* art. 2506-*bis*; stipulazione dell'atto di fusione/scissione *ex* artt. 2504 e 2506-*quater*). I progetti di fusione/scissione fusioni possono pertanto essere attuati dagli amministratori solo dopo che siano trascorsi 60 giorni dall'iscrizione nel registro delle imprese della delibera di approvazione dell'operazione stessa. Entro tale termine i creditori anteriori all'iscrizione del progetto di fusione possono proporre opposizione.

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			L'illecito in commento è, di norma, perpetrato prima che siano trascorsi i 60 giorni concessi ai creditori per l'opposizione. A rilevare sono esclusivamente le condotte che arrechino ai creditori un pregiudizio di natura patrimoniale dovendo verificarsi una lesione effettiva del loro patrimonio; il reato si estingue a seguito del risarcimento del danno cagionato. Tuttavia si precisa che l'eventuale responsabilità dell'ente sussiste anche quando il reato si estingua per il risarcimento del danno ai sensi dell'art. 8, comma 1 lett. b). Le operazioni di riduzione del capitale e, in particolar modo, quelle di fusione e scissione possono assumere rilievo sotto il profilo della strategia aziendale; a titolo di esempio si ricorda come una società potrebbe avere interesse a fondersi con una concorrente per rafforzare la propria posizione di mercato o al fine di migliorare la situazione economico-patrimoniale globale. La rischiosità insita in tali operazioni risiede nella concreta possibilità che esse determinino illeciti annacquamenti del capitale che, affievolendo la garanzia patrimoniale dei creditori, arrecano una effettiva lesione patrimoniale a tali ultimi soggetti. La condotta illecita in commento, qualora posta in essere nell'interesse anche non esclusivo dell'ente, può determinarne responsabilità ai sensi del D.Lgs. 231/2001
Art. 2629-bis c.c.	***Omessa comunicazione del conflitto d'interessi***	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 1o settembre 1993, n. 385, del citato testo unico di cui al decreto legislativo n. 58 del 1998, del decreto legislativo 7 settembre 2005, n. 209 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.	Il reato è applicabile nel caso di * società quotate in mercati regolamentati italiani o di altro Stato dell'Unione europea; * società con azionariato diffuso tra il pubblico in misura rilevante ai sensi dell'art. 116 del TUF; * banche, SIM, SGR, SICAV, intermediari di cui agli articoli 106 e 107 del TUB, assicurazioni, società autorizzate a gestire forme pensionistiche complementari. NON APPLICABILE A INNOVAPUGLIA

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
Art 2632 c.c	***Formazione fittizia del capitale***	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 a un anno.	**Soggetto attivo:** trattandosi di reato proprio, possono commettere il reato in commento: (i) gli amministratori, che possono porre in essere tutte le condotte proprie del reato di formazione fittizia del capitale, e (ii) i soci conferenti, relativamente alla sola sopravvalutazione dei conferimenti. **Fattispecie oggettiva della condotta:** le condotte alternative, finalizzate alla formazione e all'aumento fittizio del capitale, si articolano: (i) nell'attribuzione di azioni o quote in misura complessivamente superiore all'ammontare del capitale sociale; e/o (ii) nella sottoscrizione reciproca di azioni o quote; e/o (iii) nella sopravvalutazione rilevante dei conferimenti di beni in natura o di crediti ovvero del patrimonio della società nel caso di trasformazione La sopravvalutazione punibile dalla norma è esclusivamente quella **rilevante**; la valutazione di rilevanza dovrà essere effettuata caso per caso utilizzando, come criterio orientativo, la soglia individuata all'art. 2343 c.c., comma 4 ("Stima dei conferimenti di beni in natura e di crediti") La rischiosità insita nelle condotte sopra descritte, accomunate dallo specifico fine di aumentare fittiziamente il capitale sociale, risiede nella concreta possibilità che esse determinino illeciti annacquamenti del capitale. L'interesse o il vantaggio dell'ente possono risiedere in una rappresentazione contabile non veritiera e corretta della reale situazione patrimoniale al fine di ampliare la base societaria.
Art 2633 c.c.	***Indebita ripartizione dei beni sociali da parte dei liquidatori***	I liquidatori che, ripartendo i beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie 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.	Possono commettere il reato in commento esclusivamente i liquidatori. Tuttavia, prima della nomina o dell'insediamento dei liquidatori anche gli amministratori potrebbero indebitamente ripartire i beni sociali con conseguente danno per i creditori **Fattispecie oggettiva della condotta:** la condotta rilevante consiste nella ripartizione di beni sociali prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			arrecando loro un danno. Per ripartizione deve intendersi ogni trasferimento effettuato a vantaggio di uno o più soci; ai fini della configurabilità dell'illecito in commento è sufficiente anche un solo atto di riparto L'oggetto materiale della condotta è costituito dalla categoria dei **beni sociali** che comprende qualunque elemento del patrimonio idoneo a soddisfare i creditori (denaro, beni in natura e/o diritti di credito)231. L'illecito non viene in essere qualora la ripartizione avvenga dopo il pagamento dei creditori o l'accantonamento delle somme necessarie a soddisfarli.
Art 2635 c.c.	***Corruzione tra privati***	*(Solo il 3° comma è rilevante ai fini D.Lgs 231/2001)* 1.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, sono puniti con la reclusione da uno a tre anni. 2.Si applica la pena della reclusione fino a un anno e sei mesi se il fatto è commesso da chi è sottoposto alla direzione o alla vigilanza di uno dei soggetti indicati al primo comma. 3.Chi dà o promette denaro o altra utilità alle persone indicate nel primo e nel secondo comma è punito con le pene ivi previste.	**Fattispecie oggettiva della condotta:** la condotta rilevante consiste nel dare o promettere denaro o altra utilità a uno dei soggetti indicati nel primo e nel secondo comma. Il reato si articola in tre fasi: (i) la dazione o la promessa di denaro o utilità senza corrispettivo o ad un prezzo antieconomico per il cedente, (ii) il compimento o l'omissione di atti in violazione degli obblighi d'ufficio o di fedeltà da parte del soggetto che riceve il denaro o accetta la promessa e (iii) il conseguente danno alla società del soggetto corrotto. Il danno patrimoniale alla società del corrotto a seguito della corruzione è elemento costitutivo del reato che evidenzia il bene giuridico tutelato: il patrimonio sociale. Ciò comporta che, a differenza delle ipotesi di corruzione nell'ambito della pubblica amministrazione, in ambito privato non si punisce l'atto corruttivo in sé con anticipazione della soglia di tutela al mero accordo, ma solo la corruzione che abbia causato un danno all'ente di appartenenza del corrotto. Le modifiche introdotte all'art. 2635 c.c. dalla legge 6 novembre 2012, n. 190 - recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"- hanno inasprito la risposta penale nei confronti delle dazioni illecite nel settore privato mediante: a) l'inclusione tra i soggetti attivi di coloro che sono sottoposti a direzione o vigilanza da parte dei soggetti attivi già indicati dalla norma in commento;

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			b) la rilevanza di condotte non solo in violazione degli obblighi del proprio ufficio ma anche degli obblighi di fedeltà c) il procedimento d'ufficio in caso di distorsione della concorrenza nell'acquisizione di beni o servizi; d) la riferibilità anche a soggetti terzi della dazione o promessa di denaro o altra utilità. La rubrica dell'art. 2365 c.c. è stata conseguentemente modificata in "Corruzione tra privati" al fine di rendere immediatamente esplicito l'intento del legislatore di qualificare come corruzione, non solo gli accordi tra il privato e il pubblico ufficiale ma anche tra privati con una conseguente presa di posizione sull'offensività di tali comportamenti a prescindere dal terreno pubblico o privato nel quale si verifichino. Come anticipato, rileva ai fini 231 esclusivamente il comma 3, che sanziona chi dà o promette denaro o altra utilità (corruttore) ad amministratori, direttori, sindaci, o dipendenti dell'impresa (corrotti); la lettera della norma porta pertanto alla conclusione che solo le imprese corruttrici siano sanzionabili mentre nessuna responsabilità penale possa sorgere a fini 231 per le imprese corrotte. **Elemento soggettivo**: **dolo generico**. Il corruttore deve essere consapevole di dare o promettere denaro o altra utilità al fine di far commettere un atto contrario ai doveri d'ufficio o ad omettere un atto d'ufficio, generando un danno patrimoniale per la società del corrotto. I rischi sono legati alla sola ipotesi di corruzione attiva prevista dal terzo comma. Questo significa che l'ente potrà essere chiamato a rispondere solo nell'ipotesi di corruzione attiva, ovvero quando un suo apicale o sottoposto abbia promesso o dato una somma di denaro ad un altro soggetto, così inducendolo a porre in essere atti contrari ai doveri di ufficio e ai doveri di fedeltà. L'ente non potrà, quindi, essere chiamato a rispondere del fatto del corrotto: in questo caso, infatti, la società in cui opera il corrotto subisce, per espressa previsione normativa, un danno a seguito della violazione dei doveri d'ufficio e di fedeltà, che è incompatibile con l'interesse e il vantaggio previsto dal D.Lgs. 231/2001. Posto che la condotta determinante la responsabilità dell'ente può consistere, come detto, nella promessa o nella dazione di denaro o di altra utilità, occorre anzitutto porre attenzione a tutti quei processi che

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			consentano da un lato la materializzazione del beneficio derivante dall'accordo corruttivo e, dall'altro lato, la formazione della provvista di denaro necessaria all'esecuzione dell'attività corruttiva (es. l'accordo corruttivo potrebbe prevedere come beneficio un sovrapprezzo nella vendita di beni o servizi all'ente di appartenenza del corrotto). Inoltre, per il controllo sulla formazione della provvista dovranno essere predisposti appositi protocolli che garantiscano la rispondenza tra beni e servizi acquistati e uscite di cassa (ad esempio protocollo di acquisti di beni e servizi, protocollo per l'affidamento di consulenza ed altre prestazioni professionali, protocollo di gestione del magazzino) nonché protocolli per la concessione di premi e bonus e protocolli per donazioni e sponsorizzazioni a enti o associazioni, diretti a verificare la non riconducibilità degli stessi a controparti o potenziali controparti contrattuali.
Art 2636 c.c.	***Illecita influenza sull'assemblea***	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.	NON APPLICABILE A INNOVAPUGLIA
Art 2637 c.c.	***Aggiotaggio***	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.	NON APPLICABILE A INNOVAPUGLIA
Art 2638 c.c.	***Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza***	Gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza, o tenuti ad obblighi nei loro confronti, i quali nelle	**Fattispecie oggettiva della condotta:** l'articolo in commento prevede due distinte fattispecie di reato: false comunicazioni all'autorità di vigilanza (di cui al primo comma) e ostacolo alle funzioni delle autorità pubbliche e di vigilanza (di cui al secondo comma). In relazione alla fattispecie di false comunicazioni alle autorità di

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
		comunicazioni alle predette autorità previste in base alla legge, al fine di ostacolare l'esercizio delle funzioni di vigilanza, espongono fatti materiali non rispondenti al vero, ancorché oggetto di valutazioni, sulla situazione economica, patrimoniale o finanziaria dei sottoposti alla vigilanza ovvero, allo stesso fine, occultano con altri mezzi fraudolenti, in tutto o in parte fatti che avrebbero dovuto comunicare, concernenti la situazione medesima, sono puniti con la reclusione da uno a quattro anni. La punibilità è estesa anche al caso in cui le informazioni riguardino beni posseduti o amministrati dalla società per conto di terzi. Sono puniti con la stessa pena gli amministratori, i direttori generali, i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci e i liquidatori di società, o enti e gli altri soggetti sottoposti per legge alle autorità pubbliche di vigilanza o tenuti ad obblighi nei loro confronti, i quali, in qualsiasi forma, anche omettendo le comunicazioni dovute alle predette autorità, consapevolmente ne ostacolano le funzioni.	vigilanza, si segnala che essa può articolarsi in due distinte modalità di realizzazione: a) l'esposizione di fatti non rispondenti al vero relativi alla situazione economico-patrimoniale della società; b) l'occultamento, anche parziale, di fatti che avrebbero dovuto essere comunicati alle autorità di vigilanza che riguardino la situazione economico-patrimoniale della società; c) l'esposizione di fatti non rispondenti al vero relativi ai beni posseduti o amministrati dalla società per conto di terzi; d) l'occultamento, anche parziale, di fatti che avrebbero dovuto essere comunicati alle autorità di vigilanza che riguardano i beni posseduti o amministrati dalla società per conto terzi. Per quanto concerne invece la condotta che ostacoli le funzioni delle autorità di vigilanza, l'ostacolo può derivare da qualunque condotta che consista anche nell'omissione di comunicazioni all'Autorità. Si ritiene tuttavia che rilevino i soli ostacoli non irrilevanti e non momentanei.

Come si è potuto rilevare, la maggior parte dei reati societari previsti dall'art. 25 *ter* e, tra questi, il reato di false comunicazioni sociali, sono **reati "propri"** di soggetti apicali. La norma, infatti, menziona espressamente i soggetti che, a causa della loro funzione, possono commettere gli illeciti previsti dall'art 25 ter del D.Lgs 231/2001 (c.d.: reato "tipico"), ovvero:

1. gli Amministratori
2. i Direttori Generali
3. i Dirigenti preposti alla redazione dei documenti contabili societari (nel caso di InnovaPuglia, il Direttore Affari Generali)
4. i Liquidatori *(nel prosieguo la figura del liquidatore non sarà presa in esame non versando InnovaPuglia in una situazione di tal genere, dovendosi ritenere ricompresa allorchè dovesse essere nominato)*

Ciò precisato, la possibilità di commettere il reato sembrerebbe limitata a soggetti ben definiti, il cui comportamento deve essere opportunamente regolato dal presente Modello.

E' evidente, tuttavia, che alcuni reati (ad esempio: false comunicazioni sociali, false comunicazioni sociali in danno di soci e creditori) possono essere commessi da soggetti non apicali.
In questo secondo caso la norma prevede la responsabilità dell'Ente se il comportamento doloso dei subordinati sia stato fatto proprio dai soggetti apicali o reso possibile da un loro negligente controllo.

L'art. 25 ter tiene ferma, infatti, la bipartizione fondamentale dell'art. 5 tra **soggetti "apicali"** e "**sottoposti**" (posta a sua volta a fondamento di un diverso regime di imputazione della responsabilità dell'ente). Tale bipartizione viene però circoscritta ad amministratori, direttori generali e liquidatori (corrispondenti a figure di vertice aziendale) da un lato, ed a tutti coloro che siano soggetti alla loro vigilanza, dall'altro. Si tratta di una specificazione imposta dalla considerazione che buona parte dei reati societari idonei a far scattare la responsabilità amministrativa dell'ente sono reati "propri", appunto, di amministratori, direttori generali e liquidatori (indebita restituzione dei conferimenti, illegale ripartizione di utili, formazione fittizia del capitale, ecc.). Così, il reato di falso in bilancio sussiste se venga commesso da uno di questi soggetti qualificati; se, come pure potrebbe ipotizzarsi, l'elemento di falsità contabile confluito nel bilancio sia frutto dell'operato esclusivo (sia pure doloso) di un soggetto non apicale, ad esempio il responsabile della contabilità piuttosto che dell'ufficio legale interno alla società, non può esservi reato-presupposto e, conseguentemente, non può esservi responsabilità dell'ente. Ciò non vale, naturalmente, in tutte quelle ipotesi (per la verità di gran lunga prevalenti) nelle quali il sottoposto sia compartecipe del reato commesso dall'intraneus poiché, in tal caso, la responsabilità dell'ente si fonda sulla responsabilità individuale per il reato-presupposto accertata in base ai principi ordinari del concorso di persone nel reato.

Altro tema da considerare, rispetto i destinatari della norma, è relativo al **ruolo dei sindaci**. I sindaci, infatti, che - pure - rientrano tra i soggetti ai quali può venire ascritto il reato societario "proprio" non vengono menzionati. L'esclusione è radicale, nel senso che non vengono ricompresi tra i soggetti "apicali", né potrebbero per loro natura e veste "istituzionale" venire ricompresi tra i soggetti sott'ordinati agli apicali. Ci si trova di fronte ad una scelta non tecnica, ma di politica legislativa, fondata sulla considerazione che i sindaci, in quanto svincolati da un vero e proprio rapporto di immedesimazione organica, non formerebbero né esprimerebbero - nemmeno quando commettono dei reati nell'interesse della società - la volontà aziendale. Va però detto che i sindaci debbono escludersi anche dal novero degli esponenti aziendali di cui alla norma-base dell'art. 5 (lett. *a)* e *b)*). E' infatti pacifico che essi non rientrino tra i soggetti con funzioni di "rappresentanza, amministrazione e direzione" dell'ente o di una sua unità organizzativa; né rientrano tra coloro che esercitano, anche di fatto, funzioni di "gestione e controllo" dell'ente stesso. In particolare, il fatto che la previsione normativa richieda l'esercizio non alternativo ma congiunto delle funzioni (apicali) di gestione "e" controllo (intesa quest'ultima nozione in termini di dominio o governo dell'ente), induce ad escludere quei soggetti che, come i componenti del collegio sindacale, sono investiti della sola funzione di controllo (questa volta intesa in senso tecnico di verifica interna di conformità legale e statutaria). Pertanto, pur in presenza di una chiara tendenza legislativa volta a rafforzare il controllo gestionale dei sindaci, specialmente nei casi in cui sussista un controllo contabile affidato a revisori esterni alla società, deve concludersi nel senso che l'omessa indicazione degli stessi nell'art. 25 *ter* non si ponga in discontinuità con lo schema-base di responsabilità amministrativa dell'ente.

Non pare dubbio che sia applicabile anche in caso di responsabilità amministrativa da reato societario il criterio di imputazione soggettiva, insita nella **colpa in organizzazione**, prevista in via generale dagli artt. 6 e 7 del D.Lgs. 231/01.

Infine si fa presente che, benché il D.Lgs 27 gennaio 2010, n. 39 (il "**Decreto della Revisione Legale**") abbia di fatto abrogato l'art. 2624 cod. civ. (Falsità nelle relazioni o nelle comunicazioni della società di revisione), la Società – in via prudenziale - ha comunque deciso di continuare a considerare tra le Aree a Rischio i rapporti con la società di revisione legale, e ciò in virtù del fatto che le fattispecie appena richiamate, sebbene non più inserite nel Decreto, risultano tutt'oggi giuridicamente rilevanti, trovando di fatto spazio all'interno dello stesso Decreto della Revisione Legale agli artt. 27 e 29

Pertanto, al fine di disincentivare comportamenti non corretti, l'incarico di revisione legale:

- non può essere subordinato ad alcuna condizione né può essere stabilito in funzione dei risultati della revisione,
- non può dipendere in alcun modo dalla prestazione di servizi diversi dalla revisione alla società che conferisce l'incarico, alle sue controllate e controllanti, da parte del revisore legale o della società di revisione legale o della loro rete;
- deve essere determinato secondo criteri di congruità tali da garantire la qualità e l'affidabilità dei lavori; i parametri da prendere in considerazione sono le risorse professionali e le ore da impiegare nell'incarico avendo riguardo:
  - ✓ alla dimensione, composizione e rischiosità delle più significative grandezze patrimoniali, economiche e finanziarie del bilancio della società che conferisce l'incarico, nonché ai profili di rischio connessi al processo di consolidamento dei dati;
  - ✓ alla preparazione tecnica e all'esperienza che il lavoro di revisione richiede;
  - ✓ alla necessità di assicurare, oltre all'esecuzione materiale delle verifiche, un'adeguata attività di supervisione e di indirizzo, nel rispetto dei principi di cui all'art. 11.

Le disposizioni sul corrispettivo sono da combinare con la previsione dell'art. 30 del decreto, che punisce il responsabile della revisione legale e i componenti dell'organo di amministrazione, i soci, e i dipendenti della società di revisione legale, che percepiscono, direttamente o indirettamente, dalla società assoggettata a revisione legale compensi in denaro o in altra forma, oltre quelli legittimamente pattuiti.

1.C Reati di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

art. 25-*septies* ***Reati di omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro***

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
Art 589 c.p.	***Omicidio colposo***	1. Chiunque cagiona per colpa la morte di una persona è punito con la reclusione da sei mesi a cinque anni. 2. Se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale o di quelle per la prevenzione degli infortuni sul lavoro la pena è della reclusione da due a sette anni. 3. Si applica la pena della reclusione da tre a dieci anni se il fatto è commesso con violazione delle norme sulla disciplina della circolazione stradale da: a) soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30 aprile 1992, n. 285, e successive modificazioni; b) soggetto sotto l'effetto di sostanze stupefacenti o psicotrope. 4. Nel caso di morte di più persone, ovvero di morte di una o più persone e di lesioni di una o più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo, ma la pena non può superare gli anni quindici.	L'art 25-septies del D.Lgs 231/2001 distingue l'applicabilità dell'art 589 c.p. nei casi in cui vi sia violazione dell'art 55, comma 2 del TU Sicurezza (comma 1 del'art 25-septies) (omicidio colposo aggravato), dai casi in cui tale articolo non sia applicabile (comma 2 dell'art 25-septies) (omicidio colposo). In quanto InnovaPuglia non rientra tra i seguenti casi: (i) stabilimenti in cui sono presenti sostanze pericolose; (ii) centrali termoelettriche; (iii) impianti ed installazioni operanti nel settore termonucleare; (iv) aziende per la fabbricazione e il deposito separato di esplosivi, polveri e munizioni; (v) industrie estrattive con oltre 50 lavoratori; (vi) aziende in cui si svolgono attività che espongono i lavoratori a rischi biologici di cui all'*articolo 268*, comma 1, lettere c) e d) del TU Sicurezza, da atmosfere esplosive, cancerogeni mutageni, e da attività di manutenzione, rimozione smaltimento e bonifica di amianto; (vii) attività svolte in cantieri temporanei o mobili, caratterizzate dalla compresenza di più imprese e la cui entità presunta di lavoro non sia inferiore a 200 uomini-giorno

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			il comma 1 dell'art 25-septies non è applicabile a Innova Puglia spa Nel reato in esame, l'evento dannoso può essere realizzato tramite un comportamento attivo (l'agente pone in essere una condotta con cui lede l'integrità di un altro individuo), ovvero mediante una condotta omissiva (l'agente semplicemente non interviene a impedire l'evento dannoso). Di norma, si ravvisa una condotta attiva nel dipendente che svolge direttamente mansioni operative e che materialmente danneggia altri, mentre la condotta omissiva è usualmente ravvisabile nel personale apicale che non ottempera agli obblighi di vigilanza e controllo e, in tal modo, non interviene ad impedire l'evento da altri causato.
Art. 590 c.p.	***Lesioni personali colpose**** *Rileva, ai fini 231, esclusivamente il comma 3.	Chiunque cagiona ad altri per colpa una lesione personale, è punito con la reclusione fino a tre mesi o con la multa fino a euro 309. Se la lesione è grave la pena è della reclusione da uno a sei mesi o della multa da euro 123 a euro 619, se è gravissima, della reclusione da tre mesi a due anni o della multa da euro 309 a euro 1.239. Se i fatti di cui al precedente capoverso sono commessi con **violazione delle norme** sulla disciplina della sicurezza stradale o di quella **per la prevenzione degli infortuni sul lavoro**, la pena per le lesioni gravi è della reclusione da tre mesi a un anno e della multa da euro 500 a euro 2.000 e la pena per le lesioni gravissime è della reclusione da uno a tre. Nei casi di violazione delle norme sulla circolazione stradale, se il fatto è commesso da soggetto in stato di ebbrezza alcolica ai sensi dell'articolo 186, comma 2, lettera c), del decreto legislativo 30aprile 1992, n. 285, e successive modificazioni, ovvero da soggetto sotto l'effetto di sostanze stupefacenti o psicotrope, la pena per le lesioni gravi è di è della reclusione da sei mesi a due anni e la pena per le lesioni gravissime è della reclusione da un anno e sei mesi a quattro anni. Nel caso di lesioni di più persone, si applica la pena che dovrebbe infliggersi per la più grave delle violazioni commesse aumentata fino al triplo; ma la pena della reclusione non può	La condotta criminosa può realizzarsi attraverso qualsiasi comportamento idoneo a cagionare la lesione (reato a forma libera). Da tale comportamento lesivo, che può essere anche di tipo morale (*e.g.* minacce) o non violento (*e.g.* contagio attraverso contatto), deve necessariamente scaturire una malattia fisica e/o mentale. Gli eventi contemplati dalla norma sono pertanto due: - il compimento di un atto che arreca una lesione e - l'insorgenza di una malattia conseguenza della lesione stessa, ove per malattia deve intendersi *qualsiasi alterazione anatomica o funzionale dell'organismo ancorché localizzata e non influente sulle condizioni organiche generali*. Tra le lesioni è possibile ricomprendere, ad esempio, le percosse, le alterazioni anatomiche di minima rilevanza, lo stress, la paura e l'angoscia. Nonostante la norma prescriva la procedibilità a querela della persona offesa, se la violazione è commessa con violazione delle norme per la prevenzione degli infortuni sul lavoro o abbia determinato una malattia professionale sussiste sempre la procedibilità d'ufficio. La natura del reato è **colposa** ovverosia manca nel soggetto attivo l'intenzionalità dell'evento lesivo che tuttavia si realizza a seguito della sua negligenza, imperizia, imprudenza (colpa generica) o per l'inosservanza di leggi e regolamenti (colpa specifica) La condotta negligente dell'ente che, omettendo di implementare le

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
		superare gli anni cinque. Il delitto e' punibile a querela della persona offesa, salvo nei casi previsti nel primo e secondo capoverso, limitatamente ai fatti commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro o relative all'igiene del lavoro o che abbiano determinato una malattia professionale.	norme poste a tutela della sicurezza del lavoratore (attraverso per esempio la mancata valutazione dei rischi aziendali e/o della nomina del responsabile interno per la sicurezza), abbia arrecato una lesione al soggetto passivo può costituire il presupposto per l'insorgere di responsabilità *ex* D.Lgs. 231/2001.

L'elemento soggettivo del reato (art 589) è la c.d. "colpa specifica", consistente nella violazione delle norme in materia di salute e sicurezza sul lavoro (intendendosi con tale locuzione tutte le norme che, direttamente e/o indirettamente, perseguono il fine di evitare incidenti sul lavoro o malattie professionali e che, in genere, tendono a garantire la sicurezza degli ambienti di lavoro).
Tale aspetto implica una significativa differenza rispetto ai criteri di imputazione soggettiva previsti per le altre figure delittuose richiamate dal D. Lgs. n. 231/01, tutte punite a titolo di dolo.
Per la configurazione del reato occorre che vi sia un nesso di causalità tra la colpa e l'evento dannoso.
Sussiste tale nesso di causalità anche nel caso in cui la verificazione dell'infortunio sia connessa ad un comportamento imprudente del lavoratore stesso, in quanto, in tale ipotesi, l'evento si presenta come la specifica realizzazione di uno dei rischi che la norma cautelare violata mira a prevenire.
In maniera analoga, le cautele antinfortunistiche sono finalizzate a prevenire eventi lesivi a carico non solo dei lavoratori, ma anche di terzi che vengono a trovarsi nei luoghi di lavoro: onde anche nell'ipotesi di infortunio occorso a soggetti estranei all'organizzazione dell'impresa, va affermato il nesso tra l'evento e la violazione della normativa antinfortunistica.
Conformemente ai principi generali in tema di colpa, la responsabilità di chi pure abbia posto in essere una violazione della normativa antinfortunistica vigente va esclusa allorché l'evento si sarebbe ugualmente verificato ove la condotta dell'imputato fosse stata esente da colpa.

Relativamente all'art 590, in maniera analoga al reato di cui all'art. 589 c.p. l'evento dannoso può essere realizzato tramite un comportamento attivo (l'agente pone in essere una condotta con cui lede l'integrità di un altro individuo), ovvero mediante una condotta omissiva (l'agente semplicemente non interviene a impedire l'evento dannoso).
Di norma, analogamente a quanto evidenziato con riferimento al reato di omicidio colposo, si ravvisa una condotta attiva nel dipendente che svolge direttamente mansioni operative e che materialmente danneggia altri, mentre la condotta omissiva è usualmente ravvisabile nel personale apicale che non ottempera agli obblighi di vigilanza e controllo e, in tal modo, non interviene ad impedire l'evento da altri causato.
Anche per la configurazione del reato in esame, analogamente a quanto chiarito con riferimento all'omicidio colposo, occorre che vi sia un nesso di causalità tra la colpa e l'evento dannoso. Al riguardo, valgono le medesime argomentazioni sopra svolte.

1.D Reati per delitti informatici e trattamento illecito dei dati ï Cyber crimes

art. 24-bis ***Delitti informatici e trattamento illecito dei dati*** (articolo aggiunto dalla L. 18 marzo 2008 n. 48, art. 7)

<table>
<tr><th>RIFERIM. NORMATIVO</th><th>REATO</th><th colspan="2">TESTO LEGGE DI RIFERIMENTO</th><th>NOTE</th></tr>
<tr><td rowspan="4">art 491 bis c.p.</td><td rowspan="4">Falsità in documenti informatici</td><td colspan="2">Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

[Si riportano di seguito gli articoli del Capo III del Titolo VII, Libro II cui l’art 491 bis fa riferimento]</td><td rowspan="4">Nei reati di falsità in atti è fondamentale la distinzione tra le falsità materiali e le falsità ideologiche:
o ricorre la <u>falsità materiale</u> quando vi sia divergenza tra l’autore apparente e l’autore reale del documento (es: mediante l’utilizzo di firma elettronica altrui), o quando questo sia stato alterato (anche da parte dell’autore originario) successivamente alla sua formazione;
o ricorre la <u>falsità ideologica</u> quando il documento contenga dichiarazioni non veritiere o non fedelmente riportate.

La condotta del pubblico ufficiale che, nell’esercizio delle sue funzioni e facendo uso di supporti tecnici di pertinenza della P.A., elabori un falso atto informatico destinato a rimanere nella memoria dell’elaboratore integra una falsità in atto pubblico materiale o ideologica (si veda in tal senso la sentenza della Cassazione, Sez. V, 3 settembre 2001, n. 32812 CP). Il medesimo reato (falsità materiale o ideologica) è integrato anche dal dipendente pubblico che, nella sua funzione di addetto alla gestione degli archivi informatici di una P.A., inserisce deliberatamente dati falsi negli elaborati elettronici dell’archivio o modifica quelli esistenti (sentenza della Cassazione, Sez. VI, 28 luglio 2003 n.31720).

Affinché la condotta criminosa possa essere punibile ai sensi del D.Lgs. 231/2001 occorre che il dipendente, un soggetto ad esso equiparato, o il soggetto in posizione apicale commetta anche uno solo dei reati presupposto riportati nella colonna adiacente.. L’ente deve inoltre trarne vantaggio o deve comunque essere portatore di un interesse nel compimento del reato stesso.</td></tr>
<tr><td>Art. 476 Falsità materiale commessa dal pubblico ufficiale
in atti pubblici.</td><td>Formazione di un atto falso o alterazione di un atto vero.</td></tr>
<tr><td>Art. 477 Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative.</td><td>Contraffazione o alterazione di certificati o autorizzazioni amministrative ovvero, mediante contraffazione o alterazione, simulazione dell’integrazione delle condizioni richieste per la loro validità.</td></tr>
<tr><td>Art. 478 Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti.</td><td>Simulazione e rilascio in forma legale di una copia di un atto pubblico o privato la cui esistenza è solo supposta.</td></tr>
</table>

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO		NOTE
		Art. 479 Falsità ideologica commessa dal pubblico ufficiale in atti pubblici	Falsa attestazione di dichiarazioni a lui non rese, omissione o alterazione di dichiarazioni ricevute, falsa attestazione di fatti dei quali l'atto è destinato a provare la verità.	Si rileva tuttavia che, ai sensi del Decreto, la commissione di tali reati è punibile solo qualora abbia ad oggetto documenti informatici
		Art. 480 Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative.	Falsa attestazione in certificati o in autorizzazioni amministrative di fatti dei quali l'atto è destinato a provare la verità.	
		Art. 481 Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità.	Falsa attestazione in certificati fatti dei quali l'atto è destinato a provare la verità.	
		Art. 482 Falsità materiale commessa dal privato.	Rif. articoli 476, 477, 478 c.p.	
		Art. 483 Falsità ideologica commessa dal privato in atto pubblico.	Attestazione falsa al pubblico ufficiale di fatti dei quali l'atto pubblico, da quest'ultimo redatto, è destinato a provare la verità.	
		Art. 484 Falsità in registri e notificazioni.	Produzione diretta o indiretta (sotto supervisione) di false indicazioni.	
		Art. 485 Falsità in scrittura privata.	Formazione, anche solo parziale, di una scrittura privata falsa o alterazione di una scrittura privata vera.	
		Art. 486 Falsità in foglio firmato in bianco. Atto privato.	Abuso di un foglio informatico in bianco detenuto in base ad un	

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO		NOTE
			titolo che comporti l'obbligo o la facoltà di riempirlo. L'abuso si realizza qualora il soggetto attiva scriva un atto diverso da quello a cui era autorizzato/obbligato.	
		Art. 487 Falsità in foglio firmato in bianco. Atto pubblico.	Abuso di un foglio informatico in bianco detenuto in ragione della specifica attività lavorativa (propria del pubblico ufficiale). L'abuso si realizza qualora il soggetto attivo scriva un atto diverso da quello a cui era autorizzato/obbligato.	
		Art. 490 Soppressione,distruzione e occultamento di atti veri.	Distruzione, soppressione e occultamento di un atto pubblico o di una scrittura privata.	
Art. 615 ter	***Accesso abusivo ad un sistema informatico o telematico****;*	Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento		Le condotte di reato si articolano: (i) nell'accesso abusivo in un sistema informatico o telematico protetto da misure di sicurezza; e (ii) nella permanenza in un sistema informatico o telematico contro la volontà espressa o tacita del titolare. Relativamente al punto (i), si deve evidenziare che per accesso non deve intendersi il mero collegamento fisico con il sistema bensì un vero e proprio collegamento logico attraverso il quale i due terminali coinvolti (quello su cui risiede il supporto informatico e quello del soggetto che perpetra il reato) possono istaurare un "dialogo" che consenta l'eventuale lettura, eliminazione, copiatura o modificazione di dati. L'accesso abusivo è perseguibile solo se la condotta potenzialmente criminosa è posta in essere contravvenendo alla volontà del titolare anche qualora non venga causata alcuna effettiva lesione della

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
		del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.	riservatezza dei dati contenuti nel sistema informatico. In tal senso si deve rilevare come la norma tuteli il diritto alla riservatezza e, di conseguenza, la protezione del "domicilio informatico" quale estensione del domicilio materiale. Pertanto, l'esistenza di misure di sicurezza a tutela del sistema informatico (sistema di protezione) costituisce, oltre che la chiara manifestazione della volontà del titolare di limitare e/o impedire l'accesso a terzi, anche il presupposto per la punibilità della condotta illecita. Come precisato da alcune pronunce giurisprudenziali, un sistema di protezione dovrebbe articolarsi nell'azione combinata di protezioni logiche (*e.g.* introduzione di *password*, limitazione del numero di utenti che possono accedere al sistema) e/o fisico-organizzative (*e.g.* segregazione delle sale *server*, o dei luoghi in cui i dati e/o i supporti elettronici sono archiviati, meccanismo di selezione dei soggetti abilitati all'accesso fisico o all'utilizzo di specifici terminali). Pertanto il reato non sussiste se tali misure di protezione non sono attivate al momento dell'ingresso. Per quanto concerne il punto (ii), gli estremi della fattispecie sono integrati anche qualora il soggetto, pur avendo validamente ottenuto l'autorizzazione all'accesso, rimanga nel sistema informatico, contravvenendo alla nuova e contraria volontà del titolare sopraggiunta solo successivamente al primo ingresso nel sistema, oppure qualora l'agente operi oltre i limiti dell'autorizzazione concessa, perseguendo fini diversi da quelli concordati. Appare evidente come la facilità di accesso, da parte di dipendenti, di soggetti ad essi equiparati, e/o di soggetti in posizione apicale, a terminali potenzialmente in grado di instaurare un "dialogo" con sistemi informatici di terzi soggetti, al fine di violarne la segretezza, possa rappresentare un'area a rischio *ex* D.Lgs. 231/2001 qualora tali dati siano utilizzati a vantaggio o nell'interesse, anche residuale, dell'ente. La violazione o anche la semplice visione dei dati contenuti in sistemi o archivi di terzi soggetti (*e.g. database* anagrafica clienti) potrebbe determinare non solo l'insorgere di responsabilità (penale e/o amministrativa) individuale del singolo dipendente o soggetto in posizione apicale che abbia commesso l'illecito, ma dell'ente stesso, ai sensi del D.Lgs. 231/2001, qualora ricorrano i presupposti dell'articolo

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			5 del citato decreto (interesso o vantaggio proprio dell'ente). Al fine di prevenire il compimento di tali atti illeciti, la società è chiamata ad implementare misure organizzative precauzionali nel rispetto di quanto disposto dalla normativa sulla *privacy*; tali misure includono, ad esempio: ▪ l'introduzione di specifici filtri che prevengano l'accesso a determinate categorie di siti considerati non correlati con l'attività lavorativa; ▪ l'associazione di univoci codici di accesso a ciascun utente (username e password) che consenta di identificare il "profilo utente" e di verificare le attività, anche in rete, riconducibile a ciascun utente, indipendentemente dal terminale utilizzato; ▪ l'adozione di sistemi che consentano la tracciabilità in rete degli utenti che si avvalgono degli strumenti informatici dell'ente. Per tracciabilità dell'attività in rete dei dipendenti (e della corrispondenza elettronica) si deve intendere la sola acquisizione di tali dati e non anche il loro controllo nel continuo. In ragione delle mansioni svolte, gli utenti dovrebbero essere abilitati, e debitamente autorizzati da livelli gerarchici superiori, ad accedere a specifiche funzionalità dei sistemi informatici della società (*entitlement reviews*). Le autorizzazioni dovrebbero essere periodicamente riviste e controllate. Inoltre, si consiglia di vietare l'utilizzo di qualsiasi *hardware* e/o *software* diversi da quelli aziendali forniti direttamente dalla società; qualora sia invece consentito l'utilizzo di *laptop* o *software* non forniti dall'intermediario l'attività in rete e non, effettuata attraverso tali ultimi supporti, dovrà essere adeguatamente tracciabile nel rispetto di quanto premesso *supra*. Al fine di sensibilizzare il personale in relazione ai presidi informatici implementati, si consiglia di somministrare *training* focalizzati sulla *'information security* e sulle metodologie più frequentemente utilizzate per carpire *password* e codici di accesso (e.g. *phishing*) nonché di effettuare specifici controlli volti a testare la sicurezza dei sistemi informatici e la correttezza di utilizzo. Il reato presupposto introdotto da questo articolo ricalca la figura di reato preesistente quale violazione di domicilio (ex art 614 c.p.)

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			Non è richiesto che il reato sia commesso a fini di lucro o di danneggiamento del sistema; può pertanto realizzarsi anche qualora lo scopo sia quello di dimostrare la propria abilità e la vulnerabilità dei sistemi altrui, anche se più frequentemente l'accesso abusivo avviene al fine di danneggiamento o è propedeutico alla commissione di frodi o di altri reati informatici. Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali: verificarsi della distruzione o del danneggiamento dei dati, dei programmi o del sistema, o dell'interruzione totale o parziale del suo funzionamento; o quando si tratti di sistemi di interesse pubblico o di fatti compiuti con abuso della qualità di operatore del sistema. Nel contesto aziendale il reato può essere commesso anche da un dipendente che, pur possedendo le credenziali di accesso al sistema, acceda a parti di esso a lui precluse, oppure acceda, senza esserne legittimato, a banche dati della Società (o anche di terzi concesse in licenza alla Società), mediante l'utilizzo delle credenziali di altri colleghi abilitati.
Art. 615 quater	***Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici***	Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente riproduce, si procura,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, è punito con la reclusione sino ad un anno e con la multa sino a 5164 euro. La pena è della reclusione da uno a due anni e della multa da 5163 euro a 10329 euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 quater.	La norma costituisce il naturale completamento dell'articolo 615-*ter* (**Accesso abusivo ad un sistema informatico o telematico**) in quanto delinea il presupposto logico per la commissione del reato di "**accesso abusivo**" ovvero l'illecita acquisizione e diffusione di codici che consentono l'accesso a sistemi informatici o telematici protetti da misure di sicurezza.. Il reato in commento si configura, pertanto, come presupposto logico a quello di abusivo accesso ad un sistema informatico o telematico. Le condotte criminose, punibili se poste in essere fine di procurare all'agente o ad altri un profitto o di arrecare ad altri un danno, sono così raggruppabili: (i) detenzione, diffusione e/o riproduzione di codici di accesso, parole chiave e ogni altro mezzo idoneo allo scopo; (ii) fornitura a terzi di indicazioni o istruzioni idonee al compimento dell'accesso abusivo nel sistema informatico o telematico. Per quanto riguarda la condotta al punto (i), si deve rilevare che l'atto del comunicare, e/o del consegnare e/o del diffondere codici, parole

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			chiave o altri mezzi idonei all'accesso ad un sistema informatico, deve essere necessariamente successivo a quello del "detenere". Al contrario, per quanto riguarda l'attività di riproduzione, essa prescinde (non necessita) dalla detenzione stessa e anzi deve essere intesa come una riproduzione non autorizzata di un qualsiasi mezzo di accesso. In relazione alla condotta *sub* (ii), si tratta della fornitura di tutte le informazioni tecniche necessarie per ricostruire i codici di accesso o le parole chiave in modo tale da poter aggirare o superare le misure di protezione poste a presidio del sistema informatico o telematico. Ai fini del compimento del reato, è irrilevante che i codici siano stati procurati abusivamente o mediante autonoma elaborazione degli stessi. In linea generale, l'oggetto di tutela è costituito da qualsiasi mezzo che permetta di superare la protezione di un sistema informatico o telematico, indipendentemente dalla natura del mezzo stesso. Più nello specifico, l'oggetto in danno del quale la condotta criminosa è perpetrata è costituito da codici di accesso, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico, adeguatamente protetti da misure di sicurezza. Per altri mezzi idonei devono intendersi sia i mezzi fisici di accesso (*e.g.* tesserini di riconoscimento), attribuiti dal gestore del sistema al legittimo utilizzatore, sia quelli elettronici, memorizzati dall'utente stesso (*e.g. password*, codice alfanumerici). La norma punisce con maggior severità la condotta criminosa qualora sia perpetrata in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da un'impresa esercente servizi pubblici o di pubblica necessità. La norma punisce con maggior severità la condotta criminosa qualora essa sia perpetrata da un pubblico ufficiale, un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da un operatore del sistema. Le condotte punite se realizzate abusivamente dall'art. 615-quater c.p. sono molteplici: ✓ l'utilizzo non autorizzato di codici d'accesso; ✓ la diffusione che si manifesta nel rendere disponibili tali

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			codici ad un numero indeterminato di soggetti; ✓ la comunicazione che consiste nel rendere disponibili tali codici ad un numero limitato di soggetti; ✓ la consegna che riguarda cose materiali come può essere un token di accesso ad un servizio di home banking; ✓ la comunicazione o diffusione di istruzioni che permettono di eludere le protezioni di un sistema.
Art. 615 quinquies	***Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;***	Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, e` punito con la reclusione fino a due anni e con la multa sino a euro 10.329.	Le condotte di reato sono costituite da: (i) danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso riconducibili, tramite la diffusione, la comunicazione o la consegna di un programma informatico, apparecchiature o dispositivi di propria o altrui creazione; (ii) interruzione, totale o anche solo parziale, o alterazione del funzionamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso riconducibili, tramite la diffusione, la comunicazione o la consegna di un programma informatico, apparecchiature o dispositivi di propria o altrui creazione. La norma va pertanto a punire tutti quei comportamenti prodromici al danneggiamento, all'interruzione o all'alterazione di un sistema informatico (reato contemplato all'art. 635-*bis* c.p.) posti in essere attraverso l'utilizzo di *virus*, *maleware*, o specifiche apparecchiature *hardware*. La diffusione di programmi che possono danneggiare il contenuto o alterare il corretto funzionamento di sistemi informatici può essere intesa come una vera e propria attività di *hacking* eventualmente posta in essere dal dipendente, da un soggetto ad esso equiparato, o da un soggetto in posizione apicale. Va osservato come, da un punto di vista tecnico, gli artt. 615quater e 615 quinquies possono essere considerati accessori agli artt. 615ter, 635bis, 635ter e 635quater: la detenzione o dissezione di codici di accesso o la detenzione o diffusione di programmi o dispositivi diretti a danneggiare o interrompere un sistema telematico, di per sé non compiono alcun danneggiamento, se non utilizzati per un accesso abusivo ad un sistema o nella gestione di un'intercettazione di

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			informazioni.
Art. 617 quater	***Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche***	Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato.	Le fattispecie criminose individuate dall'art. 617-*quater*, commi 1 e 2, riconducibili ad un diverso fondamento logico, sono accomunate dal bene oggetto di tutela: le informazioni che risiedono su di un sistema informatico/telematico o che sono scambiate tra più sistemi. Il primo comma della norma sancisce la punibilità della condotta di un soggetto che, con mezzi fraudolenti ovvero senza esserne legittimato, intercetta, impedisce e/o interrompe le comunicazioni relative ad un sistema informatico o telematico o le comunicazioni che si svolgono tra più sistemi. Integra gli estremi del reato in commento anche la condotta di un soggetto che si avvale di mezzi volti ad eluderei meccanismi di sicurezza preordinati ad impedire l'accesso di estranei alle comunicazioni Il secondo comma ricostruisce invece la condotta criminosa di quel soggetto che rivela al pubblico, anche solo parzialmente e tramite un qualunque mezzo di informazione, il contenuto delle comunicazioni intercettate. L'abusiva intercettazione delle informazioni di un sistema informatico può essere prodromico allo svolgimento del reato di diffusione delle stesse anche se, ai fini della perseguibilità, la norma non richiede che tali condotte criminose debbano necessariamente presentarsi congiuntamente in capo al medesimo soggetto agente. Al contrario, in forza dell'autonomia loro conferita, possono essere poste in essere da soggetti diversi, in momenti anche temporali diversi. Tali condotte sono punibili ai sensi dell'art. 617-*quater* esclusivamente a querela della persona offesa salvo i casi in cui siano state poste in essere in danno di un sistema informatico o telematico dello Stato o di altro ente pubblico o da un'impresa esercente servizi pubblici o di pubblica necessità; in tali casi la condotta delittuosa è perseguibile d'ufficio e la pena, più severa, è commisurata alla rilevanza e all' utilità pubblica del sistema danneggiato. Per quanto concerne gli specifici presidi, si rinvia a quanto detto in sede di commento dell'art. 615-*ter* (aspetti procedurali).

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
Art. 617 quinquies	***Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche***	Chiunque, 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, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.	L'art. 617-*quinquies* va a completare il quadro dei reati che hanno a oggetto l'intercettazione e la manipolazione delle informazioni relative ad un sistema informatico e/o telematico ovvero intercorrenti tra più sistemi (si rimanda al commento dell'articolo 617-*quater*). La norma sancisce la punibilità dell'installazione di apparecchiature che abbiano il fine di intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico (e/o telematico) o intercorrenti tra più sistemi. L'intercettazione può avvenire sia mediante dispositivi tecnici, sia con l'utilizzo di software (c.d. *spyware*). L'impedimento od interruzione delle comunicazioni (c.d. "*Denial of service*") può anche consistere in un rallentamento delle comunicazioni e può realizzarsi non solo mediante impiego di virus informatici, ma anche ad esempio sovraccaricando il sistema con l'immissione di numerosissime comunicazioni fasulle Come sottolineato da una recente giurisprudenza, all'atto dell'intercettare è possibile equiparare quello del "copiare" i codici di accesso degli utenti di un sistema informatico tramite apparecchiature utilizzate a tal fine. Per gli aspetti procedurali si rinvia a quanto precedentemente evidenziato per l'art. 615-*ter* (aspetti procedurali) Il reato è perseguibile a querela della persona offesa, salvo che sussistano le circostanze aggravanti previste dalla norma, tra le quali rientrano le condotte commesse in danno di un sistema utilizzato dallo Stato o da altro ente pubblico o da imprese esercenti servizi pubblici o di pubblica necessità o con abuso della qualità di operatore di sistema. Nell'ambito aziendale l'impedimento o l'interruzione potrebbero essere ad esempio causati dall'installazione non autorizzata di un software da parte di un dipendente. L'art. 617-quinquies punisce il solo fatto della installazione, fuori dai casi consentiti dalla legge, di apparecchiature atte a intercettare, impedire o interrompere le comunicazioni, indipendentemente dal verificarsi di tali eventi. Il delitto è perseguibile d'ufficio.

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
Art. 635 bis	***Danneggiamento di informazioni, dati e programmi informatici***	Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.	Le condotte di reato si articolano: (i) nella distruzione, cancellazione e soppressione di informazioni, dati e programmi informatici; e/o (ii) nel deterioramento [l'alterazione in negativo di un bene in modo da diminuirne il valore] e/o alterazione di informazioni, dati e programmi informatici Il danneggiamento, l'alterazione o il deterioramento, fino alla inutilizzabilità di un programma informatico, di dati e o di informazioni possono configurarsi come una vera e propria attività di *hacking* La norma punisce con maggior severità la condotta qualora essa sia posta in essere da un operatore di sistema, con abuso della sua qualifica. Il legislatore ha inteso, in tal modo, punire la violazione del rapporto di fiducia che si instaura tra l'utilizzatore del sistema e il soggetto che lo fornisce/gestisce che, in virtù di tale ruolo, si trova in una posizione privilegiata nel perpetrare il reato in questione.
Art. 635 ter	***Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità***	Salvo che il atto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena e` della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto e` commesso con abuso della qualità di operatore del sistema, la pena e` aumentata.	La norma reca una specificazione dell'articolo 635-*bis* in quanto tratteggia il reato di danneggiamento avente però ad oggetto informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o che siano, comunque, di pubblica utilità. Il legislatore ha inteso sanzionare in modo specifico le condotte criminose di: (i) distruzione, cancellazione e soppressione; e/o (ii) deterioramento e/o alterazione quando esse abbiano ad oggetto informazioni, dati o programmi utilizzati nel pubblico interesse dallo Stato o da altro ente pubblico
Art. 635 quater	***Danneggiamento di sistemi informatici o telematici***	Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici	La norma punisce le condotte già individuate dall'art. 635-*bis*, quali l'introduzione e la trasmissione di dati, informazioni o programmi che abbiano però la conseguenza di rendere inservibili, anche solo parzialmente, sistemi informatici o telematici di terzi o di ostacolarne gravemente il funzionamento.

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
		altrui o ne ostacola gravemente il funzionamento e` punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.	
Art. 635 quinquies	***Danneggiamento di sistemi informatici o telematici di pubblica utilità***	Se il fatto di cui all'articolo 635- quater e` 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 pena e` della reclusione da uno a quattro anni. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo e` reso, in tutto o in parte, inservibile, la pena e` della reclusione da tre a otto anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto e` commesso con abuso della qualità di operatore del sistema, la pena e` aumentata	La norma punisce condotte già individuate dall'art. 635-*bis*, quali l'introduzione e la trasmissione di dati, informazioni o programmi che abbiano però la conseguenza di rendere inservibili, anche solo parzialmente, sistemi informatici o telematici di pubblica utilità o di ostacolarne gravemente il funzionamento.
art 640 quinquies	***Frode informatica del certificatore di firma elettronica***	Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti alla legge per il rilascio di un certificato qualificato, e` punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro	La fattispecie delittuosa delineata dall'articolo in commento identifica la condotta penalmente rilevante del certificatore di firma elettronica che rilascia un certificato qualificato pur in assenza dei requisiti richiesti dalla legge. Il rilascio del certificato qualificato incrementa la sicurezza e l'integrità del documento su cui la firma è apposta. In altri termini, in presenza di certificazione, la firma elettronica si trasforma in firma qualificata. Più nello specifico, la condotta del soggetto che induce i terzi a ritenere che vi sia ragionevole certezza dell'integrità dei dati contenuti nel documento e dell'autenticità dello stesso risulta perseguibile se messa in atto al fine di procurare a sé o ad altri un ingiusto profitto e arrecare danno a terzi.

1.E Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci allôautoritaôgiudiziaria

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
Art. 377-bis c.p.	***Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci allôautorità giudiziaria***	Salvo che il fatto costituisca più grave reato, chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere, è punito con la reclusione da due a sei anni.	Le condotte illecite possono radicare la responsabilità dell'ente qualora siano poste in essere a vantaggio e/o nell'interesse, seppur non esclusivi, dell'ente stesso.

1.F Delitti in materia di violazione del diritto dôautore

RIFERIM. NORMATIVO **(Legge 22 aprile 1941, n. 633)**	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
art 171		Salvo quanto previsto dall'art. 171-bis e dall'art. 171-ter, è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma: a) omissis a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa; (omissis) La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.	La norma punisce la messa a disposizione del pubblico, mediante immissione in un sistema di reti telematiche e/o con connessioni di qualunque genere, di un'opera dell'ingegno392 protetta393 o anche solo una parte di essa. Ai sensi del comma 2 dell'articolo 171, il reato previsto alla lettera a-*bis* è estinto con il pagamento, prima dell'apertura del dibattimento o prima dell'emissione del decreto penale di condanna, di una somma pari alla metà del massimo della pena stabilita al comma 1 (multa da euro 51 a euro 2.065); tale previsione, che sarebbe comunque inapplicabile, ai sensi del comma 3, nel caso in cui la violazione della lettera a-*bis* fosse commessa in danno di un'opera inedita o con usurpazione della paternità, non modifica la rilevanza dell'illecito commesso ai fini della responsabilità amministrativa dell'ente in quanto essa continua a sussistere ogniqualvolta il reato si estingua per una causa diversa dall'amnistia (si veda l'art. 8, comma 1, lett. b) del D.Lgs. 231/2001). Ai fini dell'analisi della rischiosità occorre precisare che potrebbe potenzialmente rilevare la pubblicazione, in un sistema di reti telematiche e/o con connessioni di qualunque genere, di una qualunque opera dell'ingegno prodotta da terzi, quali ad esempio un ricerca finanziaria, uno studio, una raccomandazione, un articolo, una banca dati, una generica pubblicazione, sulla quale la Società non vanta alcun diritto. Posto che anche la pubblicazione parziale dell'opera dell'ingegno integra gli estremi del reato, la diffusione di un estratto equivale

RIFERIM. NORMATIVO **(Legge 22 aprile 1941, n. 633)**	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			all'integrale pubblicazione dell'opera stessa.
art. 171-bis		1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità. 2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.	Le condotte alternative di reato si realizzano nei casi di: (i) duplicazione abusiva di **programmi per elaborare** contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (S.I.A.E.); o (ii) importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale, concessione in locazione di programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (S.I.A.E.); o (iii) rimozione arbitraria o elusione di dispositivi applicati a protezione di un programma; o (iv) trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca di dati; o (v) esecuzione dell'estrazione o del reimpiego della banca di dati; o (vi) distribuzione, vendita o concessione in locazione di una banca di dati. La condotta ***sub* (i)** (**duplicazione abusiva**) può essere posta in essere sia dai legittimi utilizzatori dei programmi per elaborare (*i.e. software*), qualora violino specifiche condizioni contrattuali, sia da terzi. L'oggetto materiale della condotta è costituito da "programmi per elaborare" che costituiscono una creazione intellettuale dell'autore e sono pertanto tutelati ai sensi dell'art. 2, n. 8 della Legge 633/1941 (ovvero i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso). Nel concetto di duplicazione rientrano la copia identica del programma originale, o con minime modifiche, e la copia parziale, purché sufficientemente organica e autonoma. Non si ritiene invece che copie di *back*-up, necessarie per l'utilizzo del programma e non stabilmente trasferite nel sistema informatico

RIFERIM. NORMATIVO **(Legge 22 aprile 1941, n. 633)**	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			dell'utente, e quelle di riserva, effettuate per evitare la perdita del programma, abbiano rilevanza penale ai fini della norma in commento. Alla medesima conclusione si deve giungere anche in relazione all'utilizzo di un unico *software*, in assenza di una licenza multipla, attraverso un struttura organizzata in rete (LAN – *Local Area Network*) che consente di collegare tra loro varie postazioni di lavoro informatiche in modo da favorirne l'interazione. La configurabilità penale è infatti esclusa in quanto la condotta di duplicazione penalmente sanzionata richiede la creazione di una nuova copia del *software* che risieda su altri supporti In merito alle condotte di cui al **punto (ii)** (importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale, concessione in locazione di programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori) sono accomunate dall'elemento (attività) dell'intermediazione tra il produttore della copia abusiva e l'utilizzatore finale. In merito alla **distribuzione** occorre precisare che essa ha ad oggetto la messa in commercio o in circolazione, o comunque a disposizione del pubblico, con qualsiasi mezzo e a qualsiasi titolo, dell'originale dell'opera o di esemplari della stessa. La **detenzione** si caratterizza invece per il perseguimento di uno scopo commerciale o imprenditoriale; ai fini della punibilità risultano pertanto rilevanti, oltre ai casi in cui la detenzione sia finalizzata alla vendita delle copie non autorizzate, anche quei casi in cui la detenzione del *software* sia destinata a svolgere una qualsiasi funzione interna nello svolgimento dell'attività imprenditoriale del detentore. Per **concessione in locazione** infine si deve intendere la cessione in uso degli originali, di copie o di supporti di opere tutelate dal diritto d'autore, fatta per un periodo limitato di tempo e al fine del conseguimento di un beneficio economico e/o commerciale diretto o indiretto. L'oggetto materiale delle condotte è costituito dai programmi contenuti su supporti non contrassegnati dalla Società italiana degli autori ed editori (S.I.A.E.); la prova dell'illecita detenzione del

RIFERIM. NORMATIVO **(Legge 22 aprile 1941, n. 633)**	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			programma non può essere desunta dal possesso di un CD privo dei contrassegni SIAE o di etichette originali essendo invece necessario risalire alla fonte del programma, stabilire chi lo abbia abusivamente messo in circolazione e seguirne il percorso fino ad ottenere la prova dell'acquisizione illecita. In assenza di una simile ricostruzione manca la prova che il programma sia una copia illegale o, quantomeno, che il detentore fosse a conoscenza di tale illegalità. In merito alle condotte di cui al punto ***sub* (iii)**, gli strumenti che possono essere impiegati per la **rimozione** e/o **l'elusione** dei dispositivi applicati a protezione di un programma per elaborare non sono tassativamente indicati; è possibile pertanto ricomprendervi qualunque strumento o condotta idonei allo scopo. Le condotte di cui ai **punti (iv), (v) e (vi)** sono accomunate dall'identico oggetto tutelato ovverosia le **banche dati**, considerate come opere dell'ingegno a tutti gli effetti e definite come "*raccolte di opere, dati o altri elementi indipendenti, sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo*". La **riproduzione** su supporti non contrassegnati S.I.A.E., il t**rasferimento** su altro supporto, la **distribuzione**, la **comunicazione**, la presentazione o dimostrazione in pubblico del contenuto di una banca dati sono punibili se commessi in violazione delle disposizioni di cui agli artt. 64-*quinquies* e 64-*sexies*, L.633/1941 che disciplinano, rispettivamente, i diritti esclusivi dell'autore della banca dati e le eccezioni a tali diritti. **L'estrazione** o il **reimpiego** dei dati contenuti in una banca dati invece sono penalmente rilevanti se compiuti in violazione degli artt. 102-*bis* e 102-*ter*, L.633/1941, concernenti i diritti del costruttore e i diritti e gli obblighi dell'utente stesso della banca dati. A tutte le condotte sopra delineate si applica un'aggravante specifica nei casi di rilevante gravità che sembra doversi valutare in base a criteri quantitativi e qualitativi, potendo essere considerate rilevanti anche, ad esempio, singole duplicazioni di programmi dal valore

RIFERIM. NORMATIVO **(Legge 22 aprile 1941, n. 633)**	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
			patrimoniale e tecnico apprezzabili.
art. 171-ter		1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro: a) omissis b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati; …..omissis h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse. 2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque: a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;	L'oggetto materiale della condotta è costituito da opere dell'ingegno destinate al circuito televisivo, cinematografico della vendita e del noleggio e dai dischi, dai nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento. Le condotte che possono in astratto radicarne la responsabilità sono: a) l'utilizzo di *software* e *hardware* aziendali per scaricare, copiare, riprodurre opere dell'ingegno protette dal diritto d'autore (in ogni caso tali condotte difficilmente possono essere compiute a vantaggio o nell'interesse dell'ente); b) l'utilizzo di materiali didattico-scientifici (*e.g.* materiali resi disponibili su piattaforme di *e-learning*) creati per la formazione del personale e/o dei clienti coperti dal diritto d'autore.
art. 171-septies		1. La pena di cui all'articolo 171-ter, comma 1, si applica anche: a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non	

RIFERIM. NORMATIVO **(Legge 22 aprile 1941, n. 633)**	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
		comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi; b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.	
art. 171-octies		1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio. 2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.	

1.G Reati ambientali

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
art. 727-*bis* c.p.	***Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette***	.	NON APPLICABILE A INNOVAPUGLIA
art. 733-*bis* c.p.	***Distruzione o deterioramento di habitat all'interno di un sito protetto***		NON APPLICABILE A INNOVAPUGLIA
D.Lgs. 3 aprile 2006, n. 152, artt. 137,	***(norme su acque reflue industriali)***	Chiunque apra o comunque effettui nuovi scarichi di acque reflue industriali contenenti le sostanze pericolose …(omissis), ovvero superando i valori limite fissati nella tabella… (omissis), senza autorizzazione, oppure continui ad effettuare o mantenere detti scarichi dopo che l'autorizzazione sia stata sospesa o revocata, ovvero non osservando i divieti di scarico previsti dagli articoli …(omissis) è punito con …(omissis)	L'art. 137 punisce le condotte poste in essere in violazione della normativa specifica inerente le acque reflue industriali, consistenti sostanzialmente nel: i) gestire scarichi senza una valida autorizzazione; ii) effettuare scarichi che comportano la violazione dei limiti tabellari imposti dalla legge; iii) effettuare scarichi vietati dalla legge, ad esempio sul suolo o nel sottosuolo; iv) scaricare illecitamente in mare. Sono tutte ipotesi di reati di pericolo, sussistenti a prescindere dalla realizzazione di un effettivo danno ambientale.
D.Lgs. 3 aprile 2006, artt. 256, 257, 258, 259, 260, 260-*bis*, 279	***(norme su gestione rifiuti :*** ***art 256 - Attività di gestione dei rifiuti non***	1. Chiunque effettua una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione di cui ……(omissis) è punito: a) con la pena dell'arresto da tre mesi a un anno o con l'ammenda da duemilaseicento euro a ventiseimila	Comportamenti potenzialmente a rischio possono essere collegati alla gestione da parte di soggetti terzi dei rifiuti prodotti negli uffici.

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
	autorizzata	euro se si tratta di rifiuti non pericolosi; b) con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro se si tratta di rifiuti pericolosi. 3. Chiunque realizza o gestisce una discarica non autorizzata è punito con la pena dell'arresto da sei mesi a due anni e con l'ammenda da duemilaseicento euro a ventiseimila euro. Si applica la pena dell'arresto da uno a tre anni e dell'ammenda da euro cinquemiladuecento a euro cinquantaduemila se la discarica è destinata, anche in parte, allo smaltimento di rifiuti pericolosi 5. Chiunque, in violazione del divieto di cui all'articolo 187, effettua attività non consentite di miscelazione di rifiuti, è punito con la pena di cui al comma 1, lettera b;	
	art 257 - Bonifica dei siti		La condotta criminosa può essere suddivisa in due fasi: la prima fase consiste nell'inquinamento del suolo, del sottosuolo o delle acque, con qualsiasi tipo di condotta (omissiva o attiva); la seconda fase è costituita dall'omessa bonifica. Si tratta, quindi, di un reato di danno, in cui l'evento è costituito dall'inquinamento di un sito, che si realizza qualora le concentrazioni di inquinanti nella matrice ambientale superino dei livelli soglia di rischio (CSC, Concentrazioni soglia di rischio), stabilite dal legislatore. L'omessa bonifica o l'omessa comunicazione di un inquinamento agli enti preposti, è considerata una condizione di punibilità:
	Art.259 - Traffico illecito di rifiuti		La condotta criminosa riguarda esclusivamente le spedizioni transfrontaliere di rifiuti. Il traffico illecito di rifiuti è costituito da qualsiasi spedizione di rifiuti in violazione degli obblighi imposti dalla normativa comunitaria (si tratta in particolari di obblighi diretti a garantire tracciabilità dei rifiuti e la loro gestione in modo corretto, ad esempio la destinazione ad impianti autorizzati, la previsioni di controlli per motivi ambientali e sanitari e così via)

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
	Art.260 - Attività organizzate per il traffico illecito di rifiuti		per integrare questo delitto è necessaria la realizzazione di una pluralità di operazioni espressione dell'allestimento di mezzi e di attività continuative organizzate, poste in essere al fine di conseguire un ingiusto profitto. Le operazioni possono riguardare la cessione, ricezione, trasporto, esportazione e importazione di rifiuti, nonché la più generica gestione abusiva (quindi in assenza della necessaria autorizzazione) di un quantitativo ingente di rifiuti La natura abusiva della gestione posta in essere può derivare non solo dalla totale mancanza di un provvedimento autorizzazione, ma anche da una gestione sulla base di un titolo autorizzativo scaduto o per tipologie di rifiuti diverse da quelle oggetto di una valida autorizzazione.
	Art.260-bis - Sistema informatico di controllo della tracciabilità dei rifiuti		La condotta criminosa è connessa alla gestione del sistema di controllo della tracciabilità dei rifiuti (c.d. Sistri), che prevede una serie di procedure dirette a garantire il tracciamento digitale dei rifiuti, dal momento della loro produzione al momento del loro smaltimento o recupero finale. La norma punisce le condotte idonee a inficiare il sistema di tracciabilità. In particolare: i) la falsificazione di un certificato di analisi dei rifiuti e la sua utilizzazione nell'ambito del Sistri; ii) l'inserimento di un certificato falso nei dati da fornire al sistema informatico del Sistri; iii) il trasporto di rifiuti pericolosi non accompagnato dalla copia cartacea della scheda Sistri e, ove necessario, dalla copia del certificato analitico che identifica le caratteristiche dei rifiuti trasportati; iv) il trasporto di rifiuti, pericolosi o non pericolosi, accompagnato da una scheda Sistri che sia stata fraudolentemente alterata. Si noti che la normativa che prevede l'entrata in vigore del sistema SISTRI ha subito diverse sospensioni e rinvii tanto che il sistema non è ancora attivo.
Legge 7 febbraio 1992, n. 150, artt. 1 e 3-*bis*	***Commercio internazionale di specie animali e vegetali minacciate di estinzione***		NON APPLICABILE A INNOVAPUGLIA

RIFERIM. NORMATIVO	REATO	TESTO LEGGE DI RIFERIMENTO	NOTE
Legge 28 dicembre 1993, n. 549, art. 3	***(Misure a tutela dell'ozono stratosferico e dell'ambiente)***		NON APPLICABILE A INNOVAPUGLIA
D.Lgs. 6 novembre 2007, n. 202, artt. 8 e 9	***(inquinamento provocato dalle navi)***		NON APPLICABILE A INNOVAPUGLIA

ALLEGATO 2: IDENTIFICAZIONE DEI RISCHI

OMISSIS