

## ***Modello di Organizzazione, di Gestione e Controllo***

***di cui al Decreto Legislativo n. 231 dell'8 giugno 2001  
esteso nel proprio ambito di applicazione a tutte le  
ipotesi di reato considerate, nel lato attivo e passivo,  
della L. n. 190/2012, e definite in conformità con le  
disposizioni del Piano Nazionale Anticorruzione***

***- Parte Speciale -***

# INDICE

|  |    |
|--|----|
| 1.INTRODUZIONE.....  | 4  |
| 2. Parte “A” - REATI CONTRO LA PUBBLICA AMMINISTRAZIONE .....                    | 5  |
| 2.1.1. Le Fattispecie di Reato contro la Pubblica Amministrazione.....           | 5  |
| 2.1.2. Pubblica Amministrazione .....  | 9  |
| 2.1.3. Le Aree a Rischio ed i Reati .....  | 10 |
| 2.1.4. Fattispecie di Reato in tema di Corruzione e concussione.....             | 11 |
| 2.1.5.Fattispecie di Reato in tema di Erogazioni Pubbliche.....                  | 12 |
| 2.1.6.Destinatari parte speciale “A” .....                                       | 12 |
| 2.1.7.Regole di carattere generale .....   | 12 |
| 2.1.8.Protocolli specifici.....  | 13 |
| 2.1.9. Flussi Informativi e attività dell’Organismo di vigilanza.....            | 13 |
| 3. PARTE “B” - REATI SOCIETARI .....   | 14 |
| 3.1.1.Le Fattispecie di Reati Societari .....                                    | 14 |
| 3.1.2.Le aree a rischio ed i Reati .....   | 18 |
| 3.1.3. Destinatari parte speciale “B” .....                                      | 18 |
| 3.1.4 Regole di carattere generale .....   | 18 |
| 4. PARTE “C” - REATI IN MATERIA DI ANTIRICICLAGGIO.....                          | 20 |
| 4.1.1. Le Fattispecie di Reati sull’Antiriciclaggio.....                         | 20 |
| 4.1.2. Le aree a rischio ed i Reati.....   | 21 |
| 4.1.3..Fattispecie di Reato in Tema di Antiriciclaggio .....                     | 22 |
| 4.1.4.Destinatari parte speciale C.....  | 22 |
| 4.1.5.Regole di Carattere Generale.....  | 22 |
| 4.1.6.Protocolli Specifici.....  | 23 |
| 4.1.7.Flussi Informativi ed Attività dell’Organismo di vigilanza .....           | 23 |
| 5. PARTE “D” - REATI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO .....           | 24 |
| 5.1.1. Le Fattispecie di Reati in materia di salute e sicurezza sul lavoro ..... | 24 |
| 5.1.2. Le aree a rischio e i reati .....   | 25 |
| 5.1.3. Fattispecie di Reato in Tema di Salute e Sicurezza sul Lavoro.....        | 26 |
| 5.1.4. Responsabilità dei Protocolli/Controlli preventivi .....                  | 27 |
| 5.1.5. Destinatari della parte speciale “D”.....                                 | 27 |
| 5.1.6. Organizzazione Interna per la Prevenzione e Protezione.....               | 27 |
| 5.1.7. Individuazione delle funzioni aziendali corrispondenti .....              | 31 |
| 5.1.8. Misure Generali di Tutela.....  | 31 |
| 5.1.9.Protocolli specifici .....   | 32 |
| 5.1.10.Flussi Informativi e attività dell’Organismo di Vigilanza .....           | 32 |
| 5.1.11. Informazione e Formazione .....  | 33 |
| 6. PARTE “E” - REATI IN MATERIA DI CRIMINALITÀ INFORMATICA.....                  | 35 |
| 6.1.1. Le Fattispecie di Reati in materia di criminalità informatica.....        | 35 |

|  |    |
|--|----|
| 6.1.2. Le Aree a Rischio ed i Reati .....  | 37 |
| 6.1.3. Fattispecie di Reato in tema di delitti informatici riferibili alle risorse e sistemi interni aziendali ..... | 38 |
| 6.1.4. Responsabilità dei Protocolli/Controlli preventivi .....  | 38 |
| 6.1.5. Destinatari della parte speciale "E" .....  | 39 |
| 6.1.6. Regole di carattere generale .....  | 39 |
| 6.1.7. Protocolli Specifici.....   | 39 |
| 6.1.8. Flussi Informativi ed Attività dell'Organismo di Vigilanza.....   | 40 |
| 6.1.9. Formazione ed informazione. ....  | 40 |
| 7. Parte "F" - REATI AMBIENTALI.....   | 41 |
| 7.1.1. Le Fattispecie di Reati Ambientali .....  | 41 |
| 7.1.2. Destinatari della parte speciale "F" .....  | 43 |
| 7.1.3. Regole di carattere generale .....  | 44 |
| 7.1.4. Protocolli specifici .....  | 44 |
| 7.1.5. Flussi Informativi ed Attività dell'Organismo di vigilanza .....  | 44 |
| 8. Parte "G" - REATI di criminalità organizzata .....  | 46 |
| 8.1.1. Le Fattispecie di Criminalità Organizzata .....   | 46 |
| 8.1.2. Destinatari della parte speciale "G" .....  | 47 |
| 8.1.3. Regole di Carattere Generale .....  | 47 |
| 8.1.4. Protocolli Specifici.....   | 48 |
| 8.1.5. Flussi Informativi ed Attività l'Organismo di Vigilanza .....   | 48 |
| 9. ESCLUSIONI / NON APPLICABILITÀ.....   | 49 |
| 9.1.1. Le Fattispecie di Reato Previste dal Decreto ma non applicabili.....  | 49 |
| 9.1.2. FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO ED IN VALORI DI BOLLO (art. 25 bis del Decreto) .....         | 49 |
| 9.1.3. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO .....   | 49 |
| 9.1.4. REATI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO.....                                  | 50 |
| 9.1.5. PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI .....   | 50 |
| 9.1.6. DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE .....   | 51 |
| 9.1.7. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE.....   | 51 |
| 9.1.8. REATI TRANSNAZIONALI (LEGGE 16 MARZO 2006, N. 146, ARTT. 3 E 10).....   | 53 |
| 9.1.9. Impiego di lavoratori irregolari .....  | 53 |

# 1. INTRODUZIONE

La presente Parte Speciale costituisce parte integrante del Modello Organizzativo previsto dal Decreto, ed ha l'obiettivo di illustrare la tipologia dei reati contemplati dal Decreto e dalla L. n. 190/2012 ed in particolare di:

- individuare le fattispecie di reato potenzialmente applicabili al contesto aziendale di ATER;
- evidenziare alcune tipologie di reato potenzialmente applicabili ma a cui può associarsi un livello di rischio molto basso o remoto tenuto conto della specifica realtà aziendale;
- rappresentare le tipologie di reato che, pur previste dal Decreto, sono ritenute non applicabili nella fattispecie aziendale.

Dall'analisi dei reati di cui al catalogo 231 applicabili alle Aziende operanti nel settore dell'E.R.P. in estrema sintesi, risultano a maggior rischio le seguenti categorie di reato:

- 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.
- Art. 24-bis. Delitti informatici e trattamento illecito di dati.
- Art. 25. Concussione e corruzione, induzione indebita a dare o promettere utilità.

Con un livello di rischio inferiore, inoltre, risultano applicabili le seguenti categorie:

- Art. 24-ter. Delitti di criminalità organizzata.
- Art. 25-ter. Reati societari.
- Art. 25-sexies. Abusi di mercato.
- Art. 25-septies. Omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.
- Art. 25-octies. Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.
- Art. 25-novies. Delitti in materia di violazione del diritto d'autore.
- Art. 25-decies. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria.
- Art. 25-undecies. Reati ambientali.
- Art. 25-duodecies. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare art. 25.

Risultano, infine, in astratto non configurabili nelle società di E.R.P. le seguenti fattispecie di reato:

- Art. 25-bis. Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento.
- Art. 25-bis.1. Delitti contro l'industria e il commercio.
- Art. 25-quater. Delitti con finalità di terrorismo o di eversione dell'ordine democratico.
- Art. 25-quater. 1. Pratiche di mutilazione degli organi genitali femminili.
- Art. 25-quinquies. Delitti contro la personalità individuale.

La presente Parte Speciale si sviluppa nelle seguenti sezioni:

1. La tipologia dei reati contro la Pubblica Amministrazione (Parte A);
2. La tipologia dei reati societari (Parte B);
3. La tipologia dei reati in materia di antiriciclaggio (Parte C);
4. La tipologia dei reati in materia di salute e sicurezza sul luogo di lavoro (Parte D);
5. La tipologia dei reati informatici (Parte E);
6. La tipologia dei reati ambientali (Parte F);
7. La tipologia dei reati di criminalità organizzata (Parte G)

Nella parte denominata ESCLUSIONI / NON APPLICABILITÀ, ovvero, nella parte cosiddetta "residuale", vengono richiamati i reati non trattati in dettaglio in apposita sezione e che, per la specifica attività svolta da ATER, risultano non applicabili. Nelle singole sezioni della presente Parte Speciale per ciascuna delle fattispecie di reato si è provveduto ad associare:

- le principali tipologie di operazioni "a rischio" svolte nell'ambito aziendale (c.d. Attività sensibili);
- i Processi aziendali interessati;
- le responsabilità delle aree a rischio;
- le fattispecie di reato richiamate dal Decreto e dalla L. n. 190/2012 ai quali è associabile, per ATER un livello di rischio molto basso o remoto.

La suddetta impostazione rappresenta la premessa per esporre nella Mappatura dei Rischi di cui all'Allegato 3:

- i Protocolli/Controlli preventivi posti in essere;
- i livelli di responsabilità assegnati per l'applicazione costante dei controlli;
- il riferimento alle specifiche Policies/Documenti/Procedure aziendali di riferimento che dettano le regole di comportamento e di operatività.

## 2. PARTE “A” - REATI CONTRO LA PUBBLICA AMMINISTRAZIONE

### 2.1.1. Le Fattispecie di Reato contro la Pubblica Amministrazione

Le fattispecie di reato contemplate nella Parte A sono quelle relative agli artt. 24; 25; 25-decies del Decreto.

Si ricorda che l'art. 26 del Decreto configura per tali reati anche il caso del tentativo.

- I. Risultano a maggior rischio di reato la categoria contemplata **dall'Art. 24 del D.Lgs. 231/2001**. In particolare:
  - Malversazione a danno dello Stato o di altro ente pubblico (art. 316-bis c.p.).
  - Indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico o delle Comunità europee (art. 316-ter c.p.).
  - Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640, co. 2, n. 1, c.p.).
  - Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-bis c.p.).
  - Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-ter c.p.).

L'articolo 24 del D.Lgs. 231/2001 è stato rubricato “Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche o frode informatica in danno dello Stato o di un ente pubblico”.

#### Malversazione a danno dello Stato o dell'Unione Europea (art. 316-bis c.p.)

Tale ipotesi di reato si configura nel caso in cui, dopo avere ricevuto finanziamenti, sovvenzioni o contributi da parte dello Stato italiano, di altri enti Pubblici o dell'Unione Europea destinati alla realizzazione di opere o allo svolgimento di attività, non si proceda all'utilizzo o alla destinazione delle somme ottenute per gli scopi cui erano destinate (la condotta consiste nell'avere distratto, anche parzialmente, le attribuzioni di denaro, senza che rilevi che l'attività programmata si sia comunque svolta).

Il reato stesso può configurarsi anche con riferimento a finanziamenti già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

#### Indebita percezione di erogazioni in danno dello Stato o dell'Unione Europea (art. 316-ter c.p.)

Tale ipotesi di reato ha luogo qualora, mediante l'utilizzo o la presentazione di dichiarazioni o di documenti falsi o mediante l'omissione di informazioni dovute, si ottengano, senza averne diritto, contributi, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, da altri enti Pubblici o dalla Unione Europea.

In questa fattispecie il reato viene a realizzarsi nel momento dell'ottenimento dei finanziamenti.

Infine, va sottolineato che tale ipotesi di reato assume natura residuale rispetto alla fattispecie della truffa ai danni dello Stato, poiché si configura solamente nei casi in cui la condotta non integri gli estremi della truffa ai danni dello Stato.

#### Truffa in danno dello Stato, di altro ente Pubblico o dell'Unione Europea (art. 640, comma 2, n. 1, c.p.)

La fattispecie della truffa in danno dello Stato o di un altro ente pubblico (inclusi gli Stati membri dell'Unione e le istituzioni dell'Unione Europea) è posta a tutela del patrimonio di tali soggetti pubblici.

Tale reato si configura qualora, al fine di realizzare un ingiusto profitto, siano posti in essere artifici o raggiri tali da indurre in errore lo Stato o ad altro ente pubblico, con conseguente danno per lo stesso. Il comportamento attraverso il quale si realizza il reato di truffa consiste in qualsivoglia attività che possa trarre in errore l'ente che deve effettuare l'atto di disposizione patrimoniale.

A titolo esemplificativo tale reato può realizzarsi qualora, nella predisposizione di documenti o dati per la partecipazione a procedure di gara, si forniscano alla Pubblica Amministrazione informazioni non corrispondenti al vero (come, ad esempio, utilizzando documentazione artefatta che rappresenti anche la realtà in modo distorto), al fine di ottenere l'aggiudicazione della gara stessa.

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

Tale ipotesi di reato si configura nel caso in cui la truffa sia posta in essere per conseguire in modo indebito erogazioni pubbliche. L'elemento qualificante del reato è costituito dall'oggetto materiale della frode in quanto "per erogazione pubblica" va intesa "ogni attribuzione economica agevolata erogata da parte dello Stato, di enti Pubblici o dell'Unione Europea".

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

Questa fattispecie di reato è posta a tutela del patrimonio dei soggetti pubblici indicati nella norma, nonché l'interesse al regolare funzionamento dei sistemi informatici.

Detto reato si differenzia dal reato di truffa, in quanto l'attività fraudolenta riguarda il sistema informatico e non la persona e può concorrere con il reato di "accesso abusivo a un sistema informatico o telematico" previsto dall'art. 615-ter c.p.

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

**Configurabilità dei reati nel contesto ATER**

Tutti i reati compresi nell'art. 24 D.Lgs. 231/01 sembrano essere, in astratto, configurabili al contesto dell'E.R.P. e quindi dell'Azienda.

Tali reati, infatti, sono riconducibili alle attività svolte dalla Azienda per la richiesta di contributi/finanziamenti a soggetti pubblici (Regione Lazio, etc.) sia per attività rientranti nelle proprie competenze statutarie (progettazione e realizzazione di alloggi di E.R.P.), sia per attività collaterali relative ad es. alle consulenze specialistiche.

In particolare i reati di cui all'articolo 24 del D.Lgs. 231/2001, nel contesto specifico, possono comportare rischi significativi in quanto l'ATER si configura quale stazione appaltante di finanziamenti pubblici per le attività di nuova costruzione, recupero e manutenzione straordinaria ed opera quasi esclusivamente ricorrendo a finanziamenti pubblici.

La aree principalmente a rischio sono quella Tecnica (es. Direzione dei Lavori) e quella amministrativa (gestione finanziaria e rendicontazione).

- II. Risultano altresì a maggior rischio la categoria di reati contemplata **dall'Art. 25 D.Lgs. 231/2001**. Si ricorda che i reati elencati nell'articolo 25, rubricato, a seguito dell'entrata in vigore della Legge anticorruzione (L. 190/2012) "Concussione e corruzione, induzione indebita a dare o promettere utilità", appartengono alla categoria dei delitti dei pubblici ufficiali contro la pubblica amministrazione.

Soggetti attivi possono essere i pubblici ufficiali e gli incaricati di pubblico servizio, intesi come coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di questa ultima (deliberativi, autoritativi, certificativi), e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale (articolo 358 c.p.).

Anche in questo caso la norma accoglie una concezione oggettiva di pubblico servizio: ciò che rileva è solo il concreto esercizio di un pubblico servizio, a prescindere dal rapporto di impiego con lo Stato o altro ente pubblico o privato.

In particolare i reati contemplati **dall'Art. 25 D.Lgs. 231/2001** sono i seguenti:

- Corruzione per l'esercizio della funzione (art. 318 c.p.).
- Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.).
- Circostanze aggravanti (art. 319-bis c.p.).
- Corruzione in atti giudiziari (art. 319-ter c.p.).
- Induzione indebita a dare o promettere utilità (art. 319-quater c.p.).
- Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.).
- Pene per il corruttore (art. 321 c.p.).
- Istigazione alla corruzione (art. 322 c.p.).
- Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis).
- Concussione (art. 317 c.p.).

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

Tale ipotesi di reato, modificata con la L. 190/2012, si configura nel caso in cui il pubblico ufficiale, nell'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.

Non sono considerati rientranti nella fattispecie gli omaggi di cortesia solo se assumono caratteri di valorizzazione contenuta in modesta entità.

Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.)

Il reato si configura nel caso in cui il pubblico ufficiale, dietro corresponsione di denaro o altra utilità, compia un atto non dovuto anche se apparentemente e formalmente regolare e quindi contrario ai principi di buon andamento e imparzialità della Pubblica Amministrazione. Detto atto non dovuto può ricondursi ad atto illegittimo o illecito o ad atto posto in essere contrariamente all'osservanza dei doveri che competono al pubblico ufficiale.

Circostanze aggravanti (art. 319 bis c.p.)

La pena è aumentata se il fatto di cui all'articolo 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.

Corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.)

Le disposizioni degli articoli 318 e 319 si applicano anche all'incaricato di un pubblico servizio. In ogni caso, le pene sono ridotte in misura non superiore ad un terzo (art. modificato dalla Legge Anticorruzione del Novembre 2012).

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

Tale ipotesi di reato si configura nel caso in cui, in presenza di un comportamento finalizzato alla corruzione, il pubblico ufficiale rifiuti l'offerta illecitamente avanzatagli. Ai fini della configurabilità dell'ipotesi criminosa è sufficiente la semplice promessa di denaro seguita dal rifiuto del pubblico ufficiale.

Corruzione in atti giudiziari (art. 319-ter)

Il reato (che costituisce una fattispecie autonoma) assume la sua connotazione nel caso in cui la azienda sia parte di un procedimento giudiziario e, al fine di ottenere un vantaggio nel procedimento stesso (processo civile, penale o amministrativo), corrompa un pubblico ufficiale (non solo un magistrato, ma anche un cancelliere od altro funzionario).

Tale reato non sanziona penalmente soltanto le condotte di chi esercita funzioni giudiziarie, ma ha una portata ben più ampia che, come precisato dalla corte di Cassazione (sentenza n. 15208 del 25/02/2010), rende configurabile il reato in questione anche in presenza di un qualsiasi atto funzionale ad un procedimento giudiziario, indipendentemente dal soggetto che lo pone in essere (nel caso specifico la testimonianza resa in un procedimento penale).

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

La norma prevede che "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 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 da o promette denaro o altra utilità, è punito con la reclusione fino a tre anni.

Concussione (art. 317 c.p.)

Tale ipotesi di reato è stata modificata con la cosiddetta Legge "anticorruzione", la Legge 6 novembre 2012, n. 190; in particolare ora soggetto attivo del delitto può essere solo il pubblico ufficiale e non più l'incaricato di un pubblico servizio, come previsto nel testo precedente.

Il reato si configura quindi nel caso in cui un pubblico ufficiale, abusando della sua posizione, costringa taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli. Questo reato, peraltro, è suscettibile di un'applicazione meramente residuale nell'ambito delle fattispecie considerate dal D.Lgs. n. 231/2001; in particolare, tale forma di reato potrebbe ipotizzarsi, sempre ai fini del citato decreto, qualora un soggetto aziendale, concorra nel reato del pubblico ufficiale che, approfittando di tale qualificazione,

richiede a soggetti terzi prestazioni non dovute, nella considerazione che, da tale comportamento, derivi in qualche modo un vantaggio o interesse per la società e non solo a titolo personale o di terzi.

Nel reato di concussione la condotta assume i caratteri dell'abuso e della prevaricazione, essendo diretta a strumentalizzare l'ufficio pubblico per coartare la volontà altrui al fine di ottenere, indebitamente, la dazione o promessa di denaro o altra utilità. Il soggetto pubblico, pertanto, si giova dello stato di paura o timore creato nel soggetto passivo.

Ai fini della contestazione della responsabilità dell'ente ex D.Lgs. 231/01, costituendo la concussione un reato proprio di soggetti qualificati, è necessario che:

- il dipendente/apicale sia un Pubblico Ufficiale;
- vi sia il concorso del dipendente/apicale dell'ente nel reato commesso dal Pubblico Ufficiale (ad es. il dipendente compie atti che favoriscono la realizzazione della condotta delittuosa);
- concorso del dipendente/apicale con il Pubblico Ufficiale a danno di un terzo.

*Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri (art. 322 bis)*

L'art. 322 bis c.p. rappresenta il punto di riferimento per la disciplina della corruzione internazionale, introdotto dall'art. 3 della L. 29 settembre 2000 n. 300 che ha autorizzato la ratifica e dato esecuzione alla Convenzione di Bruxelles 26 luglio 1995 sulla tutela degli interessi finanziari delle Comunità europee (con i protocolli di Dublino del 27 settembre 1996 e di Bruxelles del 26 maggio 1997) e alla Convenzione OCSE di Parigi del 17 dicembre 1997 sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali.

Tale articolo punisce, al pari della corruzione dei pubblici ufficiali italiani, la corruzione "delle 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 internazionali".

#### **Configurabilità dei reati nel contesto ATER**

L'Azienda svolge un'attività di interesse pubblico per la quale propri dipendenti possono assumere il ruolo di pubblico ufficiale e di incaricato di pubblico servizio.

La caratterizzazione del soggetto che riveste la qualifica di pubblico ufficiale e di incaricato di pubblico servizio può dipendere dalla natura giuridica dell'ente (Ente Pubblico, ente pubblico economico, società di capitali a partecipazione pubblica) ed inoltre anche in funzione della presenza o meno di specifici ruoli all'interno dell'Azienda.

All'interno dell'Azienda rivestono la qualifica di Pubblico Ufficiale il Direttore dei Lavori, il Collaudatore, nonché i componenti delle commissioni di gara d'appalto, per le opere realizzate in veste di stazione appaltante.

Possono inoltre essere presenti con la qualifica di pubblico ufficiale l'ufficiale rogante e l'ufficiale che esegue gli sfratti.

L'Azienda agisce inoltre nella veste di "incaricata di pubblico servizio": il reato di cui all'art. 319 quater c.p. si può manifestare in tutti gli ambiti aziendali, con particolare riferimento a quelli in cui l'Azienda si interfaccia con gli assegnatari (beneficiari dell'attività svolta dall'ente); tuttavia sarà da valutare di volta in volta come l'eventuale commissione del reato possa fare sorgere anche un interesse o un vantaggio per l'ATER, presupposto per l'applicazione del D.Lgs. 231/01.

Complessivamente, in relazione ai reati di cui all'art.25 del decreto, appare in astratto plausibile l'ipotesi che soggetti apicali, o loro sottoposti, possano commettere atti di corruzione nell'interesse della Azienda promettendo o attribuendo qualche utilità a pubblici ufficiali o incaricati di pubblico servizio, detentori del potere di assumere decisioni o di svolgere attività rilevanti per l'azienda (es. autorizzazioni, concessione di finanziamenti, verifiche, controlli, ispezioni, etc.).

Allo stesso tempo il dipendente dell'Azienda con qualifica di pubblico ufficiale o incaricato di pubblico servizio può essere soggetto attivo dei reati previsti ad es. inducendo taluno a dare o promettere per sé o ad un terzo indebitamente denaro o altre utilità (art. 319-quater c.p.) o costringendo taluno a procurare a sé o ad altri denaro o altre utilità non dovutegli (art. 317 c.p.).



- III. Possono essere ricompresi nell'ambito della Parte A i reati contemplati dall'**art. 25-decies** – induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria che presentano tuttavia un livello di rischio inferiore.

Le fattispecie di reato di cui all'Art. 25-decies D.Lgs. 231/2001 sono le seguenti:

- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377 bis cp).

La previsione di cui all'art. 377-bis c.p. intende sanzionare ogni comportamento diretto ad influenzare la persona chiamata dinanzi all'Autorità Giudiziaria a rendere dichiarazioni utilizzabili in un procedimento penale o in altri procedimenti connessi. Tale influenza può avere ad oggetto l'induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci, al fine di celare elementi "compromettenti" a carico di una determinata società, con evidente interesse della medesima. La norma mira a tutelare il corretto svolgimento dell'attività processuale contro ogni forma di indebita interferenza.

### **Configurabilità dei reati nel contesto ATER**

Si tratta di un reato riconducibile alle fattispecie di coinvolgimento dell'Azienda in un procedimento penale, all'interno del quale si possa manifestare un rischio di condotta di personale dell'Azienda che consiste nell'uso della violenza o della minaccia oppure nella promessa del denaro od altra utilità, al fine di indurre il soggetto testimone a rendere dichiarazione non vere o distorte all'Autorità giudiziaria, procurando così un interesse o un vantaggio a favore della Società stessa.

E' vietato espressamente a tutti i soggetti dell'Azienda tenere comportamenti che possano influenzare il soggetto chiamato dinanzi l'Autorità Giudiziaria (es. attraverso la promessa di denaro o altra utilità) o che lo inducano (anche attraverso forme di coartazione) a dichiarare il falso.

### **2.1.2. Pubblica Amministrazione**

Dunque agli effetti della legge penale, viene comunemente considerata come "**pubblica amministrazione**" in senso oggettivo l'intera attività funzionale dello Stato e degli altri enti pubblici e, sotto il profilo soggettivo, qualsiasi soggetto giuridico che abbia in cura interessi pubblici, predeterminati in sede di indirizzo politico e che svolga attività legislativa, giurisdizionale, di governo o amministrativa, anche mediante atti di natura privatistica, in forza di norme di diritto pubblico e di atti autoritativi.

A titolo esemplificativo e non esaustivo possono indicarsi quali soggetti della P.A. i seguenti enti o categorie di enti:

- Istituzioni pubbliche comunitarie (Commissione delle Comunità europee, del Parlamento europeo, della Corte di Giustizia e della Corte dei Conti delle Comunità europee);
- Amministrazioni centrali e periferiche, Agenzie dello Stato (i.e. Ministeri, Dipartimenti, Camera, Senato, Presidenza del Consiglio dei Ministri, Agenzie delle Entrate, etc.);
- Authorities (Autorità Nazionale Anticorruzione A.N.AC., AVCP, Autorità per le garanzie nelle comunicazioni, Autorità per l'energia elettrica e il gas, Autorità garante per la protezione dei dati personali, Banca d'Italia, etc.);
- Regioni, Province, Comuni, Comunità montane, Autorità portuali;
- Aziende Sanitarie Locali, Aziende Ospedaliere, policlinici, istituti di ricovero;
- Università ed istituti di istruzione universitaria pubblici;
- Camere di Commercio, Industria, Artigianato e Agricoltura e loro associazioni;
- Enti pubblici non economici;
- Enti nazionali di previdenza e assistenza sociale (es. INPS, INAIL, INARCASSA, ENPAM, ENPAF, etc.);
- Enti produttori di servizi economici (es. ANAS, Gruppo Equitalia, ENAC);
- Enti produttori di servizi assistenziali, ricreativi e culturali (es. CONI, CRI);
- Enti di ricerca (es. ISTAT, ASI, CNR).

L'elenco delle Amministrazioni pubbliche viene annualmente pubblicato dall'ISTAT, in applicazione di quanto stabilito dall'articolo 1, comma 2, della legge 31 dicembre 2009, n. 196.

Qualora nello svolgimento della propria attività, dovessero sorgere problematiche interpretative sulla qualifica (pubblica o privata) dell'interlocutore, ciascuno dei Soggetti destinatari dovrà rivolgersi all'Organismo di vigilanza per i chiarimenti opportuni.

### **2.1.3. Le Aree a Rischio ed i Reati**

I reati considerati al paragrafo di cui sopra, trovano come presupposto l'instaurazione di rapporti con la Pubblica Amministrazione.

L'analisi delle Aree aziendali ha individuato i principali Processi ed Attività aziendali interessate da potenziali tipologie di reato.

Nell'ambito di questa analisi sono state identificate le fasi/attività critiche, i soggetti e/o le Funzioni aziendali interessati, realizzando una completa Mappatura dei Rischi tra: i reati previsti dal Decreto, le Funzioni aziendali interessate, i Processi/Attività aziendali correlati, i Protocolli/Controlli preventivi/le regole da adottare, il livello di rischio previsto.

L'elencazione dei Processi/Funzioni aziendali a rischio reato (v. Mappatura dei Rischi) devono considerarsi non in senso esaustivo o chiuso, essendo possibile che in futuro e/o in occasione di modifiche organizzative interne, tale Mappatura dei Rischi venga opportunamente adattata o modificata.

Di seguito si riportano comunque per completezza di trattazione, i principali riferimenti stralciati dal documento della Mappatura dei Rischi.

**2.1.4. Fattispecie di Reato in tema di Corruzione e concussione**

| FATTISPECIE DI REATO   | CORRELATE ATTIVITÀ AZIENDALI A RISCHIO  | FUNZIONI AZIENDALI COINVOLTE NELLE SUDETTE ATTIVITÀ AZIENDALI   |
|--|---|---|
| <ul style="list-style-type: none"> <li>⇒ Corruzione per un atto d'ufficio</li> <li>⇒ Corruzione per un atto contrario ai doveri d'ufficio</li> <li>⇒ Corruzione di persona incaricata di un pubblico servizio</li> <li>⇒ Istigazione alla corruzione</li> <li>⇒ Concussione</li> </ul> | <ul style="list-style-type: none"> <li>⇒ Accertamenti della P.A.</li> <li>⇒ Verifiche/ispezioni da parte di Enti, Organi di Vigilanza, Gestione Rapporti con la P.A.</li> <li>⇒ Acquisti di beni e servizi</li> <li>⇒ Valutazione delle forniture</li> <li>⇒ Qualificazione imprese</li> <li>⇒ Rimborsi spese</li> <li>⇒ Assunzione di personale</li> <li>⇒ Benefits &amp; Compensation</li> <li>⇒ Contabilità Fornitori</li> <li>⇒ Uscite finanziarie</li> </ul> | <ul style="list-style-type: none"> <li>⇒ Servizio Rapporti Istituzionali e Organizzazione</li> <li>⇒ Servizio Amministrazione, Controllo e Tesoreria</li> <li>⇒ Servizio Avvocatura</li> <li>⇒ Servizio Gestione Immobili</li> <li>⇒ Servizio Patrimonio</li> <li>⇒ Servizio Tecnico</li> </ul> |

### **2.1.5. Fattispecie di Reato in tema di Erogazioni Pubbliche**

| <b>FATTISPECIE DI REATO</b>   | <b>CORRELATE ATTIVITÀ AZIENDALI A RISCHIO</b>                      | <b>FUNZIONI AZIENDALI COINVOLTE NELLE SUDETTE ATTIVITÀ AZIENDALI:</b>  |
|---|--|--|
| <p>⇒ Truffa aggravata per il conseguimento di erogazioni pubbliche.</p> <p>⇒ Indebita percezione di erogazioni a danno dello Stato.</p> | <p>⇒ Gestione Finanziamenti, Contributi e/o Benefici pubblici.</p> | <p>⇒ Servizio Rapporti Istituzionali e Organizzazione</p> <p>⇒ Servizio Amministrazione, Controllo e Tesoreria</p> <p>⇒ Servizio Avvocatura</p> <p>⇒ Servizio Gestione Immobili</p> <p>⇒ Servizio Patrimonio</p> <p>⇒ Servizio Tecnico</p> |

### **2.1.6. Destinatari parte speciale "A"**

Saranno potenzialmente a rischio a titolo esemplificativo e non esaustivo:

- il Presidente del Consiglio di Amministrazione
- il Consiglio di Amministrazione
- il Direttore Generale
- RUP
- I Direttori dei Lavori – I responsabili dell'esecuzione dei contratti
- Il Responsabile dell'Ufficio Gestione Risorse Umane e Formazione
- il Responsabile dell'Ufficio Tesoreria;
- i dirigenti, quadri e funzionari che, in relazione alle competenze loro attribuite, possono venire in contatto con i pubblici ufficiali o gli esercenti un pubblico servizio;
- i dirigenti, quadri e funzionari coinvolti nell'esecuzione delle attività finanziate

### **2.1.7. Regole di carattere generale**

Tutte le attività dell'Azienda nelle Operazioni a Rischio sono svolte nel rispetto delle leggi vigenti, delle norme del Codice Etico e di tutti i regolamenti aziendali vigenti.

L'Azienda impronta il proprio Modello organizzativo a requisiti di formalizzazione, chiarezza, separazione e adeguata comunicazione delle responsabilità, dei ruoli e delle competenze.

Le procedure aziendali sono caratterizzate dalla separazione dei ruoli di impulso decisionale, di esecuzione, di realizzazione e di controllo. Le stesse devono essere volte a formalizzare e documentare le fasi principali del processo.

L'Azienda conforma la propria politica retributiva e di carriera alla rigorosa applicazione dei contratti collettivi nazionali di lavoro applicabili e delle norme, anche di natura amministrativa, alle quali è soggetta in quanto ente pubblico economico.

Qualsiasi rapporto con funzionari pubblici deve essere corretto, formale, documentabile ed attento alle molteplici implicazioni che da esso possono derivare.

L'assunzione di personale dipendente avviene secondo criteri oggettivi di individuazione delle necessità aziendali e delle corrispondenti capacità e titoli individuali, con processo condiviso da più funzioni aziendali che contribuiscono alla scelta dei candidati nel rispetto dei predetti criteri. La dotazione organica dell'Azienda, compresi i mutamenti di livello e la variazione quantitativa, è un ambito soggetto alla vigilanza e al controllo dell'Organismo di vigilanza.

L'opportunità di accesso a finanziamenti e contributi pubblici deve essere individuata sulla base dell'effettiva presenza di tutti i requisiti legali richiesti; una volta ottenuto il beneficio, lo stesso deve essere utilizzato esclusivamente nell'ambito e per le finalità individuati dal provvedimento di erogazione, nel rispetto di tutte le modalità attuative previste, fornendo alla P.A. competente una rendicontazione trasparente, completa e veritiera delle attività finanziate svolte.

#### **2.1.8. Protocolli specifici**

L'attuazione della volontà dell'Azienda in termini di soggetti collegiali o individuali, apicali o subordinati, che dispongono dei poteri decisionali e di rappresentanza dell'Ente è definita dalla Legge Regionale n. 30/2002, dallo Statuto, nonché dei regolamenti interni vigenti.

In linea con le disposizioni normative generali e speciali sopra evidenziate, l'Azienda si è dotata ed ha debitamente formalizzato e divulgato al proprio interno i seguenti documenti aziendali:

- codice etico e di comportamento;
- regolamento di organizzazione aziendale
- Regole per le assunzioni definite dai CCNL (contratti collettivi nazionali lavoro) applicati (FEDERCASA e CISPEL Federmanager);
- Documento Programmatico per la sicurezza dei dati (DPS)
- Regolamento aziendale per l'utilizzo del sistema informatico
- Carta dei Servizi per l'erogazione dei servizi di edilizia residenziale pubblica
- Regolamento di Contabilità
- Regolamento per l'acquisizione di lavori, servizi e forniture in economia

#### **2.1.9. Flussi Informativi e attività dell'Organismo di vigilanza**

L'organismo di vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche a campione o a seguito di segnalazione, delle fasi di ciascuna Operazione a Rischio, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione per prevenire e, se del caso, reprimere, ogni comportamento che sia in contrasto con le regole aziendali.

### 3. PARTE “B” - REATI SOCIETARI

#### 3.1.1. Le Fattispecie di Reati Societari

- I. Si riporta di seguito una breve descrizione dei reati contemplati **nell’art. 25-ter del Decreto**, relativo ai reati societari.

L’art. 26 del Decreto configura per tali reati anche il caso del tentativo.

Le fattispecie di reato di cui **all’Art. 25-ter** D.Lgs. 231/2001 sono le seguenti:

- False comunicazioni sociali (art. 2621 c.c.).
- False comunicazioni sociali in danno dei soci o dei creditori (art. 2622, co. 1 e 3, c.c.).
- Falso in prospetto (art. 2623, co. 2, c. c.)<sup>1</sup>.
- Falsità nelle relazioni o nelle comunicazioni delle società di revisione<sup>2</sup> (art. 2624, c. 1 e 2, c.c.).
- Impedito controllo (art. 2625, co. 2, c.c.).
- Indebita restituzione di conferimenti (art. 2626 c.c.).
- Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.).
- Illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.).
- Operazioni in pregiudizio dei creditori (art. 2629 c.c.).
- Omessa comunicazione del conflitto d’interessi (art. 2629-bis c.c.).
- Formazione fittizia del capitale (art. 2632 c.c.).
- Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.).
- Illecita influenza sull’assemblea (art. 2636 c.c.).
- Aggiotaggio (art. 2637 c.c.).
- Ostacolo all’esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, c. 1 e 2, .c.).
- Corruzione tra privati (art. 2635 co. 3 c.c.)

Il decreto 11 aprile 2002, n. 61 ha previsto l’inserimento nel decreto legislativo 8 giugno 2001, n. 231, dell’art. 25-ter (Reati societari), che prevede specifiche sanzioni a carico dell’ente *“in relazione a reati in materia societaria previsti dal codice civile, se commessi nell’interesse della società da amministratori, direttori generali, liquidatori o da persone sottoposte alla loro vigilanza, qualora il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica”*.

Caratteristica principale dei reati societari è la loro natura di reati propri, ossia di reati che possono essere commessi solo da soggetti che hanno una particolare qualifica soggettiva. Più precisamente, a seconda della disposizione presa in considerazione, soggetti attivi dei reati societari possono essere: gli amministratori, i direttori generali, i sindaci, i liquidatori, i soci conferenti, i responsabili della revisione e, per effetto della legge 262/2005, i dirigenti delle società con azioni quotate preposti alla redazione dei documenti contabili societari.

- I reati per semplicità possono essere classificati in:

- Le falsità:

Artt. da 2621 a 2624 c.c. Il reato si perfeziona allorché gli amministratori, i direttori generali, (i dirigenti preposti alla redazione dei documenti contabili societari, i sindaci,) o i liquidatori espongono nei bilanci, nelle relazioni o nelle altre comunicazioni sociali previste dalla legge, dirette ai soci o al pubblico 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, nonché informazioni riguardanti beni posseduti dalla società per conto di terzi, in modo idoneo ad indurre in errore i destinatari sulla predetta situazione, con l’intenzione di ingannare i soci o il pubblico e al fine di conseguire per sé o per altri un ingiusto profitto, cagionando un danno patrimoniale ai soci o ai creditori.

---

<sup>1</sup> L’articolo 2623 del codice civile, che disciplinava il falso in prospetto, è stato abrogato dall’art. 34, Legge 28 dicembre 2005, n. 262 (Legge di riforma del Risparmio). La corrispondente fattispecie delittuosa è stata trasferita nel TUF (art. 173 -bis), ma non è richiamata nel presente art. 25-ter, D.Lgs. 231/2001.

<sup>2</sup> L’articolo 2624 del codice civile, che disciplinava le falsità nelle relazioni o nelle comunicazioni della società di revisione, è stato abrogato dall’art. 37, co. 34, d. lgs.27 gennaio 2010, n. 39 (Testo unico della revisione legale dei conti). La corrispondente fattispecie di reato è stata trasferita nell’art. 27 del citato decreto, ma non è richiamata nel presente art. 25 - ter, D.Lgs. 231/2001. Secondo autorevole dottrina ciò comporta la fuoriuscita di entrambi i reati dalla sfera dei fatti di reato rilevanti ai sensi del D.Lgs. 231/2001.

- La tutela penale del capitale sociale e del patrimonio:
  - Indebita restituzione di conferimenti, Art. 2626. La fattispecie in esame punisce la condotta degli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, restituiscano anche simultaneamente i conferimenti ai soci o li liberino dall'obbligo di effettuarli. Si noti che trattasi di reato proprio degli amministratori.
  - Illegale ripartizione degli utili e delle riserve, Art. 2627. La fattispecie in esame punisce la condotta degli amministratori che, fuori dei casi di legittima riduzione del capitale sociale, ripartiscono utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva, ovvero ripartiscono 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. Il reato si perfeziona con l'acquisto o la sottoscrizione di azioni o quote sociali, ivi comprese quelle della società controllante, tali da cagionare una lesione all'integrità del capitale sociale o delle riserve non distribuibili per legge.
  - Operazioni in pregiudizio dei creditori, Art. 2629. 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, tali da cagionare un danno ai creditori. Si fa presente che il risarcimento del danno ai creditori prima del giudizio estingue il reato.
  - Omessa comunicazione del conflitto d'interessi, Art. 2629 bis. La norma in esame riguarda le società con titoli quotati nei mercati regolamentati italiani o di un altro Stato dell'UE o diffusi tra il pubblico in misura rilevante, ovvero di soggetti sottoposti a vigilanza ai sensi del T.U.B. o del T.U.F., ovvero del Codice delle Assicurazioni Private. La condotta consiste nella violazione degli obblighi di cui all'art. 2391 c. 1 c.c.
  - Formazione fittizia del capitale, Art. 2632. Il reato punisce la condotta degli amministratori e dei soci conferenti che, anche in parte, formano o aumentano fittiziamente il capitale della società mediante attribuzione di azioni o quote sociali per somma inferiore al loro valore nominale; sottoscrivono reciprocamente azioni o quote; sopravvalutano in modo rilevante i conferimenti dei beni in natura o i crediti ovvero il patrimonio della società, nel caso di trasformazione.
  - Indebita ripartizione dei beni sociali da parte dei liquidatori, Art. 2633. Il reato si perfeziona con la ripartizione di beni sociali tra i soci prima del pagamento dei creditori sociali o dell'accantonamento delle somme necessarie a soddisfarli, che cagioni un danno ai creditori. Si tratta di un reato proprio dei liquidatori.
- Altri illeciti:
  - Impedito controllo, Art. 2625. È un illecito sanzionato penalmente nel solo caso del danno ai soci, che è proprio degli amministratori e consiste nell'impedire od ostacolare, mediante occultamento di documenti od altri idonei artifici, lo svolgimento delle attività di controllo legalmente attribuite ai soci, ad altri organi sociali o alle società di revisione.
  - Illecita influenza sull'assemblea, Art. 2636. 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. Soggetti attivi non sono soltanto gli amministratori, trattandosi di reato comune, ma nella sostanza si può ipotizzare che soltanto i soci (evidentemente di relativo peso) possano essere ulteriori soggetti attivi del reato.
  - Aggiotaggio, Art. 2637. Il reato di aggio presuppone operazioni distorsive di strumenti finanziari di società non quotate. La realizzazione della fattispecie prevede che si diffondano notizie false ovvero si pongano in essere operazioni simulate o altri artifici, concretamente idonei a cagionare una sensibile alterazione del prezzo di strumenti finanziari non quotati, ovvero ad incidere in modo significativo sull'affidamento del pubblico nella stabilità patrimoniale di banche o gruppi bancari.
  - Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, Art. 2638. Il reato si consuma allorché amministratori, direttori generali, (dirigenti preposti alla redazione dei documenti contabili societari, sindaci), liquidatori o altre persone sottoposte alla loro vigilanza, soggetti al potere di controllo di autorità pubbliche di vigilanza, con comunicazioni alle autorità medesime espongono, al fine di ostacolare la vigilanza stessa, falsità sulla situazione patrimoniale, economica o finanziaria dei sottoposti alla vigilanza, o occultano, con altri mezzi fraudolenti, fatti che avrebbero dovuto obbligatoriamente comunicare, ovvero omettono le

comunicazioni dovute. Viene così completata secondo il legislatore la tutela penale dell'informazione societaria, in questo caso nella sua destinazione alle autorità di vigilanza settoriali (non solo Consob, Banca d'Italia, Isvap, COVIP, ma anche Autorità garante della concorrenza e del mercato, Garante della privacy, Autorità per le Garanzie nelle Comunicazioni, Autorità per la Vigilanza sui Contratti Pubblici di Lavori, Servizi e Forniture etc.).

- Corruzione tra privati (art. 2635 co. 3 c.c.): la norma prevede che, 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. Si prevede invece 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 di tali soggetti. Peraltro, chi dà o promette denaro o altra utilità alle persone indicate è punito con le pene ivi previste. Tale reato può comportare responsabilità per l'ente solo nei casi di condotte attive, non essendo compatibili i fatti di corruzione passiva con l'interesse e vantaggio per l'ente. Ad es. si possono ipotizzare forme di corruzione attiva di personale dell'ente verso funzionari di istituti bancari o assicurativi, ispettori di enti di certificazione, responsabili di altre società ed imprese appaltatrici nei casi di contenziosi in atto, etc. Di conseguenza il Codice Etico e/o i protocolli comportamentali dovranno disciplinare i rapporti con tali soggetti, così come il Codice Sanzionatorio prevedere espressa sanzioni in caso di violazioni di tali precetti.

### **Configurabilità dei reati nel contesto ATER**

Tutti i reati sopra esposti sembrano trovare applicazione nel contesto dell'E.R.P., con le dovute necessarie contestualizzazioni relative alla natura giuridica dell'Azienda. Non si applicano all'ATER i reati esclusivamente applicabili a società quotate (Art. 2629 bis c.c.) o a società, anche non quotate, che emettono strumenti finanziari (art. 2637).

Complessivamente il bilancio, per sua natura, contiene numerose stime e valutazioni che, seppur tecnicamente esplicitate dalla funzione amministrativa, derivano in realtà da processi di determinazione che coinvolgono le diverse funzioni aziendali: di conseguenza gli ambiti in cui si possono realizzare le fattispecie di reato in questione attraversano trasversalmente l'intera organizzazione aziendale.

Da sottolineare anche gli obblighi di comunicazione verso l'ANAC<sup>3</sup> (ex AVCP), che gravano sull'Azienda e che possono generare responsabilità ai sensi dell'art. 2638 c.p.

#### **II. Nella Parte B trattati sono trattati altresì i reati di cui all'art. 25-sexies "Reati di abusi di mercato".**

Le fattispecie di reato di cui all'Art. 25-sexies D.Lgs. 231/2001 sono le seguenti:

- Abuso di informazioni privilegiate (D.Lgs. 24.2.1998, n. 58, art. 184 TUF).
- Manipolazione del mercato (D.Lgs. 24.2.1998, n. 58, art. 185 TUF).

L'art. 25-sexies fa riferimento alle fattispecie di "Abuso di informazioni privilegiate" e di "Manipolazione del mercato", previste dal D.Lgs. 24.2.1998, n. 58, "Testo unico delle disposizioni in materia di intermediazione finanziaria".

Occorre inoltre fare espresso richiamo agli artt. 187 bis e 187 ter del D.Lgs. 58/98 i quali, benché relativi a fattispecie sanzionate non penalmente ma solo amministrativamente, non rientranti nelle previsioni dell'art. 25-sexies del D.Lgs. 231/01, presentano elementi di stretta contiguità o, addirittura, di vera e propria coincidenza.

Sulla base della normativa in esame, l'Azienda può quindi essere chiamato a rispondere sia degli illeciti penali che degli illeciti amministrativi commessi, nell'interesse e/o a vantaggio dell'Azienda medesima, da persone che rivestano funzioni di rappresentanza, amministrazione o di direzione ovvero da persone sottoposte alla direzione o alla vigilanza di questi ultimi.

Per quanto riguarda il sistema sanzionatorio previsto dal TUF vige il cosiddetto "doppio binario" (artt. 187 duodecies e 187 terdecies), dove si prevede rispettivamente per i reati di abuso informazioni privilegiate e manipolazione del mercato specifiche sanzioni in capo sia alla persona fisica che alla persona giuridica.

### **Gli abusi di informazione privilegiata**

<sup>3</sup> Si ricorda che il decreto-legge 24 giugno 2014, n. 90 (Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari) ha previsto la soppressione della AVCP



L'abuso di informazione privilegiata è un reato (o anche un illecito amministrativo) proprio di persone fisiche legate all'emittente che possono essere distinti in:

- insider primari (ad es. membri del CdA dell'emittente, partecipanti al capitale dell'emittente, etc.);
- insider secondari (ad es. soggetti in possesso di informazione privilegiata, che ne conoscono o che ne potrebbero conoscere in base a l'ordinaria diligenza il carattere privilegiato). L'insider può essere chiunque, in possesso di informazioni privilegiate, conosca o possa conoscere in base ad ordinaria diligenza il carattere privilegiato dell'informazione medesima: quindi, può esserlo una persona facente parte, a qualsiasi livello, dell'organico della società, oppure un elemento esterno che, al fine di assolvere specifici compiti o incarichi (sindaci, liquidatori, funzionari pubblici, consulenti), venga a conoscenza di informazioni idonee a far trarre illecito profitto al soggetto medesimo. Per l'insider secondario tuttavia, oggi, potrà essere ascritta soltanto una responsabilità di tipo amministrativo.

La tipologia delle notizie utilizzate a tal fine è vasta; possono riguardare imminenti iniziative dell'ente, oppure decisioni strategiche da parte del Consiglio di Amministrazione (ad es. particolari investimenti o disinvestimenti in certi settori), il lancio di offerte pubbliche di acquisto o di vendita.

### Manipolazione del mercato

La manipolazione del mercato è un reato (o un illecito amministrativo) in cui chiunque (non solo con dolo, ma anche con colpa) può operare una manipolazione sia informativa sia operativa. Per la configurazione dell'illecito amministrativo è sufficiente la colpa.

Le manipolazioni del mercato possono essere di due tipologie:

1. Manipolazione informativa: è sanzionata la condotta di chi tramite mezzi di informazione, compreso internet o ogni altro mezzo diffonde informazioni, voci o notizie in merito agli strumenti finanziari:

- false o fuorvianti;
- che forniscano o siano suscettibili di fornire indicazioni false o fuorvianti in merito a strumenti finanziari.

2. Manipolazione operativa: condotte di chi pone in essere operazioni od ordini di compravendita:

- a) che forniscano o siano idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari;
- b) che consentano, tramite l'azione di una o di più persone che agiscono di concerto, di fissare il prezzo di mercato di uno o più strumenti finanziari ad un livello anomalo o artificiale;
- c) che utilizzino artifici od ogni altro tipo di inganno o di espediente;
- d) ovvero altri artifici idonei a fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di strumenti finanziari.

### Configurabilità dei reati nel contesto ATER

Premesso che l'Azienda non è, per sua natura, società non è possibile escludere a priori la potenziale configurabilità dei reati di cui all'art. 25 sexies del D.Lgs. 231/01, o di illeciti amministrativi di cui agli artt. 187 bis e 187 ter del D.Lgs. 58/98, in capo alle stesse per le motivazioni di seguito esposte.

A titolo meramente esemplificativo, per quel che concerne l'abuso di informazioni privilegiate ed in particolare la fattispecie di insider trading, tra i comportamenti altamente a rischio nell'Azienda, si può individuare la comunicazione a terzi di informazioni privilegiate ottenute da rappresentanti della società/ente in ragione della propria posizione, al fine di far conseguire un interesse/vantaggio alla società/ente stessa.

Tra le informazioni "privilegiate" che riguardano l'Ente si indicano a titolo esemplificativo le seguenti:

- Variazioni nel management;
- Ristrutturazioni e riorganizzazioni aziendali che hanno un effetto sulle attività, sulle passività, sulle posizioni finanziarie dell'Ente e sul conto economico;
- Cause legale rilevanti;
- Tesoreria;
- Insolvenza da parte di debitori rilevanti;
- Riduzione nel valore degli immobili;
- Comunicazioni di risultati aziendali, sia positivi, sia negativi.

In riferimento alla manipolazione di mercato, in sede di risk assessment, si ricordano alcune condotte che possono determinare una manipolazione operativa.

Il processo della tesoreria, che risulta quello esposto a maggiore rischio in relazione sia ai reati di cui all'art. 25 sexies del Decreto che agli illeciti amministrativi di cui agli artt. 187 bis e 187 ter del D.Lgs. 58/98, dovrà essere presidiato adeguatamente, al fine di ridurre al massimo il rischio che condotte improprie possano influenzare il prezzo di eventuali strumenti finanziari.

### **3.1.2. Le aree a rischio ed i Reati**

L'analisi delle Aree aziendali ha individuato i principali Processi ed Attività aziendali interessate da potenziali tipologie di reato.

Le Attività aziendali considerate più specificamente a rischio in relazione ai reati societari sono le seguenti:

- tutti i Processi/Attività aziendali di gestione di dati che contribuiscono alla formazione del bilancio preventivo e del bilancio consuntivo;
- la redazione del bilancio, della relazione sulla gestione;
- i flussi di comunicazione tra gli organi istituzionali;
- le attività di Controllo interno, comprendendo anche le Attività aziendali di registrazione contabile e/o di gestione contabile in generale.

Nell'ambito di questa analisi, sono state identificate le fasi/Attività aziendali critiche, i soggetti e/o le Funzioni aziendali interessati, realizzando una completa Mappatura dei Rischi tra: i reati previsti dal Decreto, le Funzioni aziendali interessate, i Processi/Attività aziendali correlati, i Protocolli/ Controlli preventivi/le regole da adottare, il livello di rischio previsto.

Per quanto attiene alle finalità del Decreto le Attività aziendali di ATER sono considerate in ottica di Processo, al fine di facilitare l'individuazione delle Attività aziendali critiche, a rischio e/o che possono avere un impatto diretto o indiretto nella possibile commissione dei reati rilevanti di cui al Decreto.

L'elencazione dei Processi/Funzioni aziendali a rischio reato (v. Mappatura dei Rischi),devono considerarsi non in senso esaustivo o chiuso, essendo possibile che in futuro e/o in occasione di modifiche organizzative interne tale Mappatura dei Rischi venga opportunamente adattata o modificata.

### **3.1.3. Destinatari parte speciale "B"**

Saranno potenzialmente a rischio a titolo esemplificativo e non esaustivo:

- il Presidente del Consiglio di Amministrazione
- il Consiglio di Amministrazione
- il Direttore Generale
- il Responsabile Ufficio Tesoreria
- il Ufficio Budget Pianificazione e Controllo di gestione;
- i dirigenti, quadri e funzionari ai quali è affidato il compito di tenere le scritture contabili e redigere tutti i prospetti contabili;

### **3.1.4. Regole di carattere generale**

Coloro ai quali è affidato il compito di tenere le scritture contabili devono effettuare ogni registrazione in modo accurato, completo, veritiero e trasparente ed a consentire eventuali verifiche da parte di soggetti, anche esterni, a ciò preposti.

Essi devono assicurare che ogni scrittura consenta di ricostruire la relativa operazione e sia accompagnata da una adeguata documentazione che faciliti anche le successive attività di controllo e vigilanza. Anche il passaggio di informazioni e dei dati da ciascuna funzione aziendale a quella amministrativa dovrà essere regolamentato anche ai fini di una responsabilizzazione circa la veridicità e completezza delle informazioni trasmesse (es. tramite sottoscrizione di apposite dichiarazioni / attestazioni da parte dei responsabili aziendali).

Per quanto attiene agli amministratori, direttori, sindaci e liquidatori sono vietati tutti quei comportamenti che possono configurare ipotesi di reato relativi alle falsità, alla tutela del patrimonio ed agli altri illeciti previsti dall'art. 25-ter del D.Lgs. 231/01.

Saranno inoltre definiti adeguati percorsi formativi per tutti i responsabili che partecipano ai processi amministrativi per assicurare una comprensione dei principi di governance, di quelli contabili generali, delle norme e delle relative sanzioni. Naturalmente, per il personale delle funzioni amministrative responsabili dei processi in oggetto, dovranno essere previsti percorsi formativi più ampi che assicurino un puntuale aggiornamento rispetto alle novità legislative in materia.

L'Organismo di Vigilanza, nell'ambito delle proprie attività, dovrà confrontarsi con adeguata periodicità con le funzioni responsabili della tenuta delle scritture contabili, della formazione del bilancio e delle comunicazioni societarie, compresi i soggetti esterni (es. revisori dei conti), ed essere informato prontamente di ogni situazione di anomalia o criticità che possa generare profili di rischio anche solo potenziali.

Tutti i dipendenti devono assicurare all'organismo di vigilanza massima collaborazione, completezza e chiarezza delle informazioni fornite, trasparenza ed accuratezza dei dati e delle elaborazioni, segnalazione di conflitti di interesse, etc.

## 4. PARTE “C” - REATI IN MATERIA DI ANTIRICICLAGGIO

### 4.1.1. Le Fattispecie di Reati sull'Antiriciclaggio

Il Decreto Legislativo 21 novembre 2007, n. 231 ha dato attuazione alla direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (c.d. III direttiva antiriciclaggio), e alla direttiva 2006/70/CE che ne reca misure di esecuzione. Di conseguenza si è avuta una riorganizzazione della legislazione in materia di antiriciclaggio.

Per quanto concerne la responsabilità amministrativa dipendente da reato il terzo comma dell'art. 63 del D.Lgs. 231/2007 ha introdotto nel Decreto l'art. 25 octies, che estende la responsabilità amministrativa degli enti ai reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita (artt. 648, 648 bis e 648 ter del c.p.).

Si riporta di seguito una breve descrizione dei reati contemplati **nell'art. 25 octies del Decreto**.

L'art. 26 configura per tali reati anche il caso del tentativo.

Le fattispecie di reato di cui all'Art. 25-octies D.Lgs. 231/2001 sono le seguenti:

- Ricettazione (art. 648 cp);
- Riciclaggio (art. 648 bis cp);
- Impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter cp).

Trattasi di reati generalmente indirizzati ad enti soggetti alla disciplina antiriciclaggio (D.Lgs. 231/2007 come le banche, le Poste, altri intermediari finanziari).

Tale disciplina, agli articoli dal 10 al 14, esplicita i destinatari della normativa antiriciclaggio, tra i quali sono compresi, tra l'altro, i professionisti (commercialisti, consulenti del lavoro, notai, avvocati), gli uffici della pubblica amministrazione ed altri operatori qualificati.

Le norme di cui sopra mirano ad impedire che dal denaro o cose in qualche modo collegati ad un delitto, si possa trarre un vantaggio con conseguente protrarsi e stabilizzazione del pregiudizio economico subito dalla persona offesa o del vantaggio derivante dalla commissione del delitto medesimo. Esse tutelano altresì l'interesse dell'ordinamento all'individuazione e punizione degli autori del delitto presupposto e ad impedire che vengano messi in circolazione nel mercato legale capitali o beni illegittimamente acquisiti.

La ricettazione consiste nell'acquisto, ricezione, occultamento di denaro o cose provenienti da delitto, al fine di procurare a sé o ad altri un profitto, mediazione nelle predette attività.

L'applicazione di tale ipotesi di reato ha luogo soltanto se l'autore del delitto di ricettazione non sia concorrente nel delitto presupposto (cosiddetta auto-ricettazione).

Il delitto di riciclaggio, invece, si realizza con la sostituzione, trasferimento di denaro, beni o altre utilità provenienti da delitto non colposo, ovvero qualsiasi operazione sui predetti, tale da ostacolare l'identificazione della loro provenienza delittuosa.

La differenza tra riciclaggio e ricettazione risiede proprio nel fatto che, nella seconda ipotesi, vi è sostituzione (cioè scambio) di denaro, beni o altra utilità di provenienza delittuosa con altri “puliti”, ovvero un loro trasferimento da un soggetto ad un altro con qualsiasi forma negoziale, tali da ostacolare l'identificazione della provenienza illecita degli stessi.

In ogni caso integra il reato in esame qualsiasi operazione tale da ostacolare la predetta identificazione.

La terza fattispecie, impiego di denaro, beni o utilità di provenienza illecita, affine a quelle di ricettazione e riciclaggio, si realizza, fuori dei casi di concorso in questi due reati, mediante una particolare modalità: l'investimento o l'utilizzo strumentale in attività economiche o finanziarie di denaro, beni o altre utilità provenienti da delitto.

La commissione del fatto di cui all'art. 648 ter c.p. nell'esercizio di attività professionale costituisce circostanza aggravante.

#### **Configurabilità dei reati nel contesto ATER**

Trattasi di reati generalmente indirizzati ad enti soggetti alla disciplina antiriciclaggio (D.Lgs. 231/2007 come le banche, le Poste, altri intermediari finanziari), non direttamente associabili al contesto di attività svolte in ambito E.R.P. e quindi dell'Azienda.

Complessivamente le attività svolte nel settore dell'Edilizia Residenziale Pubblica ed i relativi rapporti contrattuali instaurati con i terzi esterni, specie nell'ambito delle procedure di appalto e delle commesse pubbliche, sono potenzialmente esposte al rischio di riciclaggio.

Si rinvia quindi esplicitamente al decreto antiriciclaggio di cui al D.Lgs. 231/2007 ed in particolare ai principi generali di conoscenza della clientela e di tracciabilità delle operazioni.

Comunque, si ritiene necessario evidenziare come l'Azienda, per quanto riguarda il settore degli appalti, risponde alla normativa pubblicistica ex D.Lgs. 163/2006, e del relativo regolamento di attuazione, che contiene disposizioni cautelative come anche alle disposizioni in tema **di tracciabilità dei flussi finanziari ex L. 136/2010, art. 3, s.m.i.**

In particolare il D.Lgs. 163/06 prevede una serie di verifiche svolte dalla stazione appaltante a carico delle imprese partecipanti alle procedure di gara, volte ad acquisire evidenza del possesso dei requisiti (di ordine generale, di idoneità professionale, di capacità economico e finanziaria e tecnico-professionale).

La L. 136/2010 e s.m.i. all'art. 3 stabilisce che *"per assicurare la tracciabilità dei flussi finanziari finalizzata a prevenire infiltrazioni criminali, gli appaltatori, i subappaltatori e i subcontraenti della filiera delle imprese nonché i concessionari di finanziamenti pubblici anche europei a qualsiasi titolo interessati ai lavori, ai servizi e alle forniture pubblici devono utilizzare uno o più conti correnti bancari o postali (...) dedicati"*.

Nella gestione degli appalti di lavori pubblici, servizi e forniture, dunque, occorre sottolineare l'importanza delle attività di tracciabilità dei flussi finanziari, come disciplinate dalla normativa suddetta e come specificato successivamente dall'AVCP (determinazione n. 4/2011), le quali richiedono ulteriori presidi di controllo da parte delle figure interne preposte.

In particolare l'Azienda nei contratti sottoscritti con gli appaltatori relativi ai lavori, ai servizi e alle forniture, il committente:

- ha inserito, a pena di nullità assoluta, un'apposita clausola con la quale essi assumono gli obblighi di tracciabilità dei flussi finanziari (art. 3 c. 8 primo capoverso della L. 136/2010);
- verifica che nei contratti sottoscritti con i subappaltatori e i subcontraenti della filiera delle imprese a qualsiasi titolo interessate ai lavori, ai servizi e alle forniture sia inserita, a pena di nullità assoluta, un'apposita clausola con la quale ciascuno di essi assume gli obblighi di tracciabilità dei flussi finanziari (art. 3 c. 9 della L. 136/2010).

Ulteriori controlli, in capo all'Azienda (in qualità di Stazione Appaltante), dovranno essere svolti in fase di stato avanzamento lavori finalizzati alla verifica dell'avvenuta trasmissione delle fatture quietanzate relative ai pagamenti corrisposti dagli affidatari al subappaltatori o cottimisti (art. 118 del D.Lgs. 163/2006).

Circa il rispetto degli oneri di tracciabilità tra appaltatore, subappaltatori e subcontraenti (previsti all'art. 3 c. 5 L. 136/2010) sembra esistere, in capo alla Azienda/stazione appaltante, più che un obbligo normativo, un dovere etico-morale in tal senso da realizzarsi concretamente secondo procedure e protocolli interni che ne dovranno stabilire le modalità, la frequenza di controllo e le conseguenze nel caso in cui i controlli diano esito negativo.

Ulteriori rischi potenziali si possono rilevare in riferimento ad alcuni processi aziendali:

- gestione degli incassi in contanti e gestione della cassa, per quanto attiene al rispetto della normativa per il contrasto al riciclaggio ed all'uso del denaro contante, per la quali si ricordano le limitazioni all'uso del contante e dei titoli al portatore previste dal D.Lgs. 231/2007 all'art. 49 e s.m.i.;
- vendita di alloggi di E.R.P., sebbene le società di E.R.P. non rientrino nel novero delle agenzie di affari in mediazione immobiliare, laddove le stesse potrebbero comunque risultare destinatarie degli obblighi generali previsti dal D.Lgs. 231/2007, in particolare per quanto attiene gli obblighi di verifica della clientela.

#### **4.1.2. Le aree a rischio ed i Reati**

L'analisi delle Aree aziendali ha consentito di individuare alcune Attività aziendali per le quali potrebbero sussistere rischi di commissione dei reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita.

Nell'ambito della suddetta analisi sono state identificate le fasi/Attività aziendali critiche, i soggetti e/o le Funzioni aziendali interessati, realizzando una completa Mappatura dei Rischi tra i reati previsti dal Decreto, le Funzioni aziendali interessate, i Processi/Attività aziendali correlati, i Protocolli/ Controlli preventivi /le regole da adottare, il livello di rischio previsto.

Per gli scopi del presente paragrafo vengono definite aree a rischio tutte quelle Aree aziendali, Funzioni aziendali, Uffici a e/o Processi, etc. che hanno parte nei processi e nelle attività individuate nella Mappatura dei Rischi.

Per quanto attiene alle finalità del Decreto le Attività aziendali di ATER sono considerate in ottica di Processo, al fine di facilitare l'individuazione delle Attività aziendali critiche, a rischio e/o che possono avere un impatto diretto o indiretto nella possibile commissione dei reati rilevanti di cui al Decreto.

L'elencazione dei Processi/Funzioni aziendali a rischio reato (v. Mappatura dei Rischi) devono considerarsi non in senso esaustivo o chiuso, essendo possibile che in futuro e/o in occasione di modifiche organizzative interne, tale Mappatura dei Rischi venga opportunamente adattata o modificata.

All'interno della Mappatura dei Rischi sono richiamati i Protocolli/Controlli preventivi ritenuti rilevanti per contrastare validamente le possibilità di commissione di reato. La descrizione di tali Protocolli/Controlli preventivi è contenuta in massima parte all'interno di tutte le Policies, le Procedure e le disposizioni di ATER con particolare riferimento ai reati in materia di antiriciclaggio, da seguire (e far seguire) nei vari Processi aziendali.

Di seguito si riportano comunque per completezza di trattazione, i principali riferimenti stralciati dalla Mappatura dei Rischi.

#### **4.1.3. Fattispecie di Reato in Tema di Antiriciclaggio**

| <b>FATTISPECIE DI REATO</b>  | <b>CORRELATE ATTIVITÀ AZIENDALI A RISCHIO</b>   | <b>FUNZIONI AZIENDALI COINVOLTE NELLE SUDETTE ATTIVITÀ AZIENDALI</b>  |
|--|---|---|
| ⇒ Ricettazione<br>⇒ Riciclaggio<br>⇒ Impiego di denaro, beni o utilità di provenienza illecita | ⇒ Qualificazione dei fornitori<br>⇒ Acquisti di beni e servizi<br>⇒ Valutazione delle forniture<br>⇒ Uscite finanziarie<br>⇒ Incassi<br>⇒ Fatturazione attiva | ⇒ Servizio Rapporti Istituzionali e Organizzazione<br>⇒ Servizio Amministrazione, Controllo e Tesoreria<br>⇒ Servizio Avvocatura<br>⇒ Servizio Gestione Immobili<br>⇒ Servizio Patrimonio<br>⇒ Servizio Tecnico |

#### **4.1.4. Destinatari parte speciale C**

Sono tutti i soggetti che intrattengono per conto dell'Azienda rapporti con soggetti terzi, in particolare coloro i quali curano i processi amministrativo-finanziari.

#### **4.1.5. Regole di Carattere Generale**

Gli organi di A.T.E.R. e i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti hanno l'obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate.

In particolare le procedure aziendali sono caratterizzate dalla separazione dei ruoli di impulso decisionale, di esecuzione e realizzazione, nonché di controllo, con adeguata formalizzazione e documentabilità delle fasi principali del processo.

Tutti i destinatari, in coerenza con il Codice Etico e le procedure aziendali esistenti, hanno l'obbligo di:

- porre in essere correttamente e legalmente, in modo trasparente e collaborativo, tutte le attività di gestione delle risorse finanziarie;
- monitorare e tener traccia della provenienza e dell'impiego dei flussi finanziari, dei beni e delle altre risorse aziendali, nonché delle operazioni compiute in relazione ad essi;

#### **4.1.6. Protocolli Specifici**

Oltre alle regole generali citate in precedenza anche con riferimento ad altre fattispecie di rischio, che qui si intendono per richiamate, l'Azienda ha già predisposto ed adottato:

- Codice Etico;
- Regolamento di Contabilità.

L'Azienda ha adottato dei protocolli per la "tracciabilità dei flussi finanziari ai sensi della L. 136/2010 e della L. 217/2010", da applicare obbligatoriamente per tutti i pagamenti relativi ad una commessa pubblica di lavori, servizi e/o forniture tra i quali si ricorda l'inserimento di una clausola risolutiva espressa in tutti i contratti ex art. 3 L. n. 136/2010.

#### **4.1.7. Flussi Informativi ed Attività dell'Organismo di vigilanza**

L'Organismo di vigilanza potrà discrezionalmente attivarsi con verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, delle fasi di ciascuna Operazione a Rischio, evitando per quanto possibile di interferire con i processi decisionali aziendali,

L'organismo di vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione e repressione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello.

## 5. PARTE “D” - REATI IN MATERIA DI SALUTE E SICUREZZA SUL LAVORO

### 5.1.1. Le Fattispecie di Reati in materia di salute e sicurezza sul lavoro

Le Fattispecie di Reati in Materia di Salute e Sicurezza sul Lavoro sono contemplate dall'Art. 25-septies D.Lgs. 231/2001. In particolare si tratta:

- Omicidio colposo (art. 589 c.p.).
- Lesioni personali colpose (art. 590, c. 3, c.p.).

La legge 3 agosto 2007 n. 123, “Misure in tema di tutela della salute e della sicurezza sul lavoro e delega al Governo per il riassetto e la riforma della normativa in materia”, ha introdotto l'articolo 25-septies nel decreto legislativo 231/2001, per estendere la responsabilità amministrativa degli enti ai delitti di cui agli articoli 589 e 590 3° comma del codice penale, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro. Successivamente, il decreto legislativo 9 aprile 2008 n. 81 (cosiddetto Testo Unico Sicurezza) ha modificato i profili sanzionatori della responsabilità dell'ente ed introdotto nuove disposizioni in tema di modelli organizzativi idonei a prevenire i reati in esame.

Le norme in esame tutelano la vita e l'incolumità dei lavoratori. In particolare, viene sanzionata penalmente l'inosservanza di precetti cautelari contenuti nelle norme in materia di prevenzione di infortuni sul lavoro e malattie professionali, a seguito della quale si verificano la morte o lesioni gravissime o gravi del lavoratore. L'attività lavorativa presenta dei rischi che l'ordinamento mira ad evitare, prescrivendo delle cautele idonee a contenere il pericolo insito nell'attività lavorativa stessa. L'obbligo di osservare le regole cautelari ricade su determinati soggetti, anche terzi, che assumono la c.d. “posizione di garanzia”.

Secondo la giurisprudenza prevalente, i soggetti passivi dei reati in esame sono, non solo i lavoratori, ma anche i terzi che si trovino in un luogo di lavoro in cui si richiede di conformarsi alle regole di cautela predisposte per prevenire ed evitare infortuni sul lavoro.

I soggetti attivi dei reati in esame sono i destinatari delle norme antinfortunistiche, titolari degli obblighi di sicurezza, previsti dal D.Lgs. 81/2008 (Datore di lavoro, dirigenti, preposti, responsabile del servizio di protezione e prevenzione, addetti squadre primo soccorso ed antincendio, etc.) chiamati a rispondere penalmente delle loro inosservanze, in quanto assumono una posizione di garanzia rispetto al bene giuridico tutelato, ossia una posizione di controllo sulle fonti di rischio.

L'articolo 25 septies del decreto ricollega il sorgere della responsabilità amministrativa degli enti non a tutte le ipotesi di omicidio colposo previste dall'art. 589 c.p., ma soltanto a quelle violazioni (art. 589 c. 2 c.p.) commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Anche per quanto attiene alle lesioni personali colpose, l'art. 25 septies del decreto ricollega il sorgere della responsabilità a carico dell'ente, per la sola ipotesi di delitto di lesioni gravi o gravissime commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

L'art. 583 c.p. definisce gravi le lesioni se dal fatto deriva una malattia che metta in pericolo di vita la persona offesa, ovvero una malattia o un'incapacità di attendere alle ordinarie occupazioni per un tempo superiore ai quaranta giorni, nonché se il fatto produce l'indebolimento permanente di un senso o di un organo.

La lesione personale è gravissima, invece, 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, perdita della capacità di procreare, ovvero una permanente e grave difficoltà della favella, la deformazione, ovvero lo sfregio permanente del viso.

#### **Configurabilità dei reati nel contesto ATER**

I reati in oggetto risultano di fatto applicabili a qualsivoglia società e di conseguenza a tale logica non sfuggono le aziende operanti nell'E.R.P. Le ipotesi di reato di cui all'art. 25-septies, infatti, nel contesto dell'Azienda possono presentarsi in due diversi ambiti:

- Il primo relativo alle **sedi aziendali**: tale ipotesi si presenta configurabile, anche se con una probabilità di accadimento abbastanza bassa, tenendo conto delle specifiche attività di natura prettamente amministrativa svolte e dall'assenza di specifiche fonti di rischio (es. macchinari, attrezzature).
- Il secondo relativo ai **cantieri esterni** nei quali operano dipendenti dell'Azienda in veste di stazione appaltante (es. Direttore Lavori, coordinatori in fase di esecuzione, ecc.). In questo ambito, che vede tra l'altro il sovrapporsi della normativa relativa agli appalti pubblici (D.Lgs.



163/2003), con il testo unico sulla sicurezza (D.Lgs. 81/2008), la probabilità di accadimento risulta in astratto maggiore.

Il tema della sicurezza nei luoghi di lavoro riveste oggi un ruolo centrale rispetto alle tematiche di sostenibilità delle organizzazioni e richiede un atteggiamento di diffusa consapevolezza a tutti i livelli dell'organizzazione, di collaborazione e di cooperazione di tutto il personale con gli uffici interni addetti al servizio di protezione, così come con le ditte appaltatrici, in una logica ed in una cultura di prevenzione che richiede costanza nella formazione e nell'applicazione delle regole e dei principi.

### **5.1.2. Le aree a rischio e i reati**

Per quanto attiene alla specifica fattispecie di reati e alla loro rilevanza ai fini delle responsabilità previste dal Decreto, ATER ha considerato i fattori di rischio valutando la tipologia di attività che prevede un lavoro sostanzialmente d'ufficio escludendosi attività di produzione industriale di norma più esposte ai rischi di incidenti sul lavoro e di salute.

La valutazione riguardo l'idoneità del sistema aziendale organizzato e predisposto da ATER a esimere la Azienda dalla responsabilità di cui al Decreto per i reati d'interesse, è stata effettuata tenendo conto degli obblighi richiamati dall'art. 30 del D.Lgs. n. 81/2008 per quanto applicabili nella fattispecie e che riguardano:

- il rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- le attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- le attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- le attività di sorveglianza sanitaria;
- le attività di informazione e formazione dei lavoratori;
- le attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- l'acquisizione di documentazioni e certificazioni obbligatorie di legge;
- le periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate;
- la previsione di idonei sistemi di registrazione dell'avvenuta effettuazione delle attività sopra specificate;
- l'articolazione di funzioni che assicurino le competenze tecniche e i poteri necessari per la verifica, valutazione, gestione e controllo del rischio;
- la previsione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello Organizzativo;
- la previsione di un idoneo sistema di controllo sull'attuazione del Modello Organizzativo 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.

Della necessità di rispettare i citati obblighi si è tenuto conto nel Documento di valutazione dei rischi aziendali.

Per gli scopi del presente paragrafo vengono definite aree a rischio tutte quelle Aree aziendali, Funzioni aziendali, Uffici e/o Processi, etc. che hanno parte nei processi e nelle attività individuate in Mappatura dei Rischi.

Per quanto attiene alle finalità del Decreto le attività di ATER sono considerate in ottica di Processo, al fine di facilitare l'individuazione delle attività critiche, a rischio e/o che possono avere un impatto diretto o indiretto nella possibile commissione dei reati rilevanti di cui al Decreto.

L'elencazione dei Processi/Funzioni aziendali a rischio reato (Mappatura dei Rischi) devono considerarsi non in senso esaustivo o chiuso, essendo possibile che in futuro e/o in occasione di modifiche organizzative interne, tale Mappatura dei Rischi venga opportunamente adattata o modificata.

All'interno della Mappatura dei Rischi sono richiamati i Protocolli/Controlli preventivi ritenuti rilevanti per contrastare validamente le possibilità di commissione di reato. La descrizione di tali Protocolli/Controlli preventivi è contenuta in massima parte all'interno di tutte le Policies, le Procedure e le disposizioni di ATER attinenti la salute e la sicurezza sul lavoro, da seguire (e far seguire) nei vari Processi aziendali.

Di seguito si riportano comunque per completezza di trattazione, i principali riferimenti stralciati dalla Mappatura dei Rischi.

### 5.1.3. Fattispecie di Reato in Tema di Salute e Sicurezza sul Lavoro

| FATTISPECIE DI REATO   | CORRELATE ATTIVITÀ AZIENDALI A RISCHIO  | FUNZIONI AZIENDALI COINVOLTE NELLE SUDETTE ATTIVITÀ AZIENDALI:               |
|--|---|--|
| <p>⇒ Omicidio colposo,</p> <p>⇒ Lesioni colpose gravi o gravissime,</p> <p><i>Entrambi i reati sono commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro.</i></p> | <ol style="list-style-type: none"> <li>1. Emissione ed aggiornamento delle politiche aziendali in materia.</li> <li>2. Monitoraggio leggi, regolamenti e variazioni.</li> <li>3. Nomina delle figure professionali previste dal D.Lgs. n. 81/2008</li> <li>4. Formalizzazione ed aggiornamento periodico del "Documento di valutazione dei rischi aziendali" di cui agli artt. 17 e 28 del TU.</li> <li>5. Attività formativa obbligatoria.</li> <li>6. Sistema di Prevenzioni Incendi.</li> <li>7. Procedure per la conformità alle norme contenute nel d.lgs. 9 aprile 2008 n. 81.</li> <li>8. Procedure di monitoraggio e controllo sulla gestione dei rischi.</li> <li>9. Fornitura di informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività.</li> <li>10. Procedure di pronto soccorso.</li> <li>11. Monitoraggio dell'attività svolta dal medico competente.</li> <li>12. Tenuta della lista dei fornitori esterni che operano per le attività di sicurezza.</li> <li>13. Formazione del budget per la spesa annuale della sicurezza.</li> <li>14. Adempimenti da parte delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori da affidare in appalto o mediante contratto d'opera o di somministrazione.</li> </ol> | <p>⇒ Datore di lavoro</p> <p>⇒ RSPP</p> <p>⇒ Dirigenti</p> <p>⇒ Preposti</p> |

#### **5.1.4. Responsabilità dei Protocolli/Controlli preventivi**

Alla luce delle normative applicabili e delle indicazioni fornite nelle Linee Guida dell'Associazione di categoria, appare evidente che l'area di rischio generale dell'Azienda, con riferimento a questi reati, consiste in ogni attività che comporti l'obbligo di osservanza delle prescrizioni generali e specifiche in materia di sicurezza ed igiene del lavoro, ovvero l'art. 2087 c.c. ed il D.Lgs. n. 81/2008, nonché altre norme e disposizioni ad essi correlati: ciò si realizza per ogni attività aziendale che prevede l'impiego di anche solo un lavoratore, secondo la ampia definizione che ne viene data dall'art. 2 del D.Lgs. n. 81/2008, nonché per le attività aziendali, comportanti obblighi e responsabilità specifiche, quali quelle di fabbricazione, vendita, noleggio o concessione in uso di attrezzature di lavoro, dispositivi di protezione individuale ed impianti<sup>4</sup>, quelle di installazione e montaggio di impianti, attrezzature di lavoro ed altri mezzi tecnici<sup>5</sup>, quelle connesse a contratti di appalto, d'opera o di somministrazione.

#### **5.1.5. Destinatari della parte speciale "D"**

Destinatari del presente capitolo sono:

- il **Datore di Lavoro** ex art. 2 c. 1 lett. b) D.Lgs. 81/2008 che da Statuto e da regolamento di organizzazione è il Direttore Generale;
- i **Dirigenti** che in ragione delle competenze professionali e dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferito, attuano le direttive del datore di lavoro organizzando l'attività lavorativa e vigilando su di essa (art. 2, comma 1, lettera d, D.Lgs 81/2008);
- i **Preposti** che in ragione delle competenze professionali e nei limiti dei poteri gerarchici e funzionali adeguati alla natura dell'incarico conferito, sovrintendono all'attività lavorativa e garantiscono l'attuazione delle direttive ricevute, controllando la corretta esecuzione da parte dei lavoratori ed esercitando un funzionale potere di iniziativa (art. 2, comma 1, lettera e, D.Lgs. 81/2008);
- il **Responsabile del Servizio di Prevenzione e Protezione ("RSPP")** dell'Azienda al quale sono demandate specifiche responsabilità in materia, ai sensi del T.U. in materia di Sicurezza (D.Lgs. 81/2008);
- il **Medico competente**, nominato ai sensi e per gli effetti degli artt. 38, 39, 40 e 41 del T.U. in materia di Sicurezza (D.Lgs. 81/2008);
- il **Rappresentante dei Lavoratori per la Sicurezza**, di cui agli artt. 47 e 50 del T.U. in materia di Sicurezza (D.Lgs. 81/2008);
- i **Lavoratori**, come definiti dall'art. 2 del D.Lgs. n. 81/2008.

#### **5.1.6. Organizzazione Interna per la Prevenzione e Protezione**

Con riguardo alla predisposizione del **Servizio di Prevenzione e Protezione**, così come previsto dalla legge, l'Azienda, ai sensi dell'articolo 17, lettera b, comma 4 del D.Lgs. n. 81/2008, ha nominato l'Ing. Giancarlo Mongelli quale Responsabile del Servizio di Prevenzione e Protezione (RSPP) per la sicurezza dei lavoratori, in possesso dei requisiti di professionalità, esperienza e formazione previsti e 2 addetti del Servizio di Prevenzione e Protezione ossia l'Ing. Mirko Gentile e il Geom. Carlo Serafi.

Le competenze ed attribuzioni specifiche dell'RSPP, a cui risponde e del cui servizio il Datore di Lavoro si avvale, consistono nel coordinamento del Servizio di Prevenzione e Protezione dai Rischi, i cui compiti in particolare si estrinsecano nel:

- individuare i fattori di rischio, valutare i rischi e individuare le misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
- elaborare, per quanto di competenza, le misure preventive e protettive conseguenti alla valutazione dei rischi (DVR), ed i sistemi di controllo di tali misure;

- elaborare le procedure di sicurezza per le varie attività aziendali;
- proporre i programmi di formazione ed informazione dei lavoratori;
- partecipare alle consultazioni in materia di tutela della salute e sicurezza del lavoro, nonché alle riunioni periodiche annuali sulla sicurezza;
- fornire ai lavoratori le informazioni: sui rischi per la salute e sicurezza sul lavoro connessi all'attività dell'impresa in generale; sulle procedure di primo soccorso, lotta antincendio ed evacuazione; i nominativi dei lavoratori addetti al primo soccorso e prevenzione incendi e del medico competente.

L'RSPP è tenuto al segreto in ordine ai processi lavorativi di cui venga a conoscenza nell'esercizio delle funzioni attribuite.

I **Dirigenti**, come definiti dall'art. 2, comma 1, lett. d) del D.Lgs. n. 81/2008, ovvero coloro che attuano le direttive del Datore di Lavoro, organizzando l'attività lavorativa e vigilando su di essa, sono obbligati ai sensi dell'art. 18 del D.Lgs. n. 81/2008, in concorso con il Datore di Lavoro e secondo le attribuzioni e competenze ad essi conferite a:

- a) nominare il medico competente per l'effettuazione della sorveglianza sanitaria nei casi previsti dal presente decreto legislativo;
- b) designare preventivamente i lavoratori incaricati dell'attuazione delle misure di prevenzione incendi e lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato, di salvataggio, di primo soccorso e, comunque, di gestione dell'emergenza;
- c) nell'affidare i compiti ai lavoratori, tenere conto delle capacità e delle condizioni degli stessi in rapporto alla loro salute e alla sicurezza;
- d) fornire ai lavoratori i necessari e idonei dispositivi di protezione individuale, sentito il responsabile del servizio di prevenzione e protezione e il medico competente, ove presente;
- e) prendere le misure appropriate affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni e specifico addestramento accedano alle zone che li espongono ad un rischio grave e specifico;
- f) richiedere l'osservanza da parte dei singoli lavoratori delle norme vigenti, nonché delle disposizioni aziendali in materia di sicurezza e di igiene del lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuali messi a loro disposizione;
- g) inviare i lavoratori alla visita medica entro le scadenze previste dal programma di sorveglianza sanitaria e richiedere al medico competente l'osservanza degli obblighi previsti a suo carico nel presente decreto;
- g-bis) nei casi di sorveglianza sanitaria di cui all'articolo 41 D.Lgs. n. 81/2008, comunicare tempestivamente al medico competente la cessazione del rapporto di lavoro;
- h) adottare le misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato ed inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- i) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- l) adempiere agli obblighi di informazione, formazione e addestramento di cui agli articoli 36 e 37 D.Lgs. n. 81/2008;
- m) astenersi, salvo eccezione debitamente motivata da esigenze di tutela della salute e sicurezza, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave e immediato;
- n) consentire ai lavoratori di verificare, mediante il rappresentante dei lavoratori per la sicurezza, l'applicazione delle misure di sicurezza e di protezione della salute;

o) consegnare tempestivamente al rappresentante dei lavoratori per la sicurezza, su richiesta di questi e per l'espletamento della sua funzione, copia del documento di cui all'articolo 17, comma 1, lettera a) D.Lgs. n. 81/2008, anche su supporto informatico come previsto dall'articolo 53, comma 5 D.Lgs. n. 81/2008, nonché consentire al medesimo rappresentante di accedere ai dati di cui alla lettera r); il documento è consultato esclusivamente in azienda;

p) elaborare il documento di cui all'articolo 26, comma 3 D.Lgs. n. 81/2008, anche su supporto informatico come previsto dall'articolo 53, comma 5, e, su richiesta di questi e per l'espletamento della sua funzione, consegnarne tempestivamente copia ai rappresentanti dei lavoratori per la sicurezza; il documento è consultato esclusivamente in azienda;

q) prendere appropriati provvedimenti per evitare che le misure tecniche adottate possano causare rischi per la salute della popolazione o deteriorare l'ambiente esterno verificando periodicamente la perdurante assenza di rischio;

r) comunicare in via telematica all'INAIL e all'IPSEMA, nonché per loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, entro 48 ore dalla ricezione del certificato medico, a fini statistici e informativi, i dati e le informazioni relativi agli infortuni sul lavoro che comportino l'assenza dal lavoro di almeno un giorno, escluso quello dell'evento e, a fini assicurativi, quelli relativi agli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni; l'obbligo di comunicazione degli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni si considera comunque assolto per mezzo della denuncia di cui all'articolo 53 del testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali, di cui al d.P.R. 30 giugno 1965, n. 1124;

s) consultare il rappresentante dei lavoratori per la sicurezza nelle ipotesi di cui all'articolo 50 D.Lgs. n. 81/2008;

t) adottare le misure necessarie ai fini della prevenzione incendi e dell'evacuazione dei luoghi di lavoro, nonché per il caso di pericolo grave e immediato, secondo le disposizioni di cui all'articolo 43 D.Lgs. n. 81/2008. Tali misure devono essere adeguate alla natura dell'attività, alle dimensioni dell'azienda o dell'unità produttiva, e al numero delle persone presenti;

u) nell'ambito dello svolgimento di attività in regime di appalto e di subappalto, munire i lavoratori di apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro;

v) nelle unità produttive con più di 15 lavoratori, convocare la riunione periodica di cui all'articolo 35 D.Lgs. n. 81/2008;

z) aggiornare le misure di prevenzione in relazione ai mutamenti organizzativi e produttivi che hanno rilevanza ai fini della salute e sicurezza del lavoro, o in relazione al grado di evoluzione della tecnica della prevenzione e della protezione;

aa) comunicare in via telematica all'INAIL e all'IPSEMA, nonché per loro tramite, al sistema informativo nazionale per la prevenzione nei luoghi di lavoro di cui all'articolo 8, in caso di nuova elezione o designazione, i nominativi dei rappresentanti dei lavoratori per la sicurezza; in fase di prima applicazione l'obbligo di cui alla presente lettera riguarda i nominativi dei rappresentanti dei lavoratori già eletti o designati;

bb) vigilare affinché i lavoratori per i quali vige l'obbligo di sorveglianza sanitaria non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità.

**I Preposti** (art. 2 comma 1 lett. e), ovvero coloro che sovrintendono all'attività lavorativa e garantiscono l'attuazione delle direttive ricevute, controllandone la corretta esecuzione da parte dei dipendenti ed esercitando un funzionale potere di iniziativa, sono obbligati ai sensi dell'art. 19 del D.Lgs. n. 81/2008, secondo le loro attribuzioni e competenze a:

a) sovrintendere e vigilare sulla osservanza da parte dei singoli lavoratori dei loro obblighi di legge, nonché delle disposizioni aziendali in materia di salute e sicurezza sul lavoro e di uso dei mezzi di protezione collettivi e dei dispositivi di protezione individuale messi a loro disposizione e, in caso di persistenza della inosservanza, informare i loro superiori diretti;

- b) verificare affinché soltanto i lavoratori che hanno ricevuto adeguate istruzioni accedano alle zone che li espongono ad un rischio grave e specifico;
- c) richiedere l'osservanza delle misure per il controllo delle situazioni di rischio in caso di emergenza e dare istruzioni affinché i lavoratori, in caso di pericolo grave, immediato e inevitabile, abbandonino il posto di lavoro o la zona pericolosa;
- d) informare il più presto possibile i lavoratori esposti al rischio di un pericolo grave e immediato circa il rischio stesso e le disposizioni prese o da prendere in materia di protezione;
- e) astenersi, salvo eccezioni debitamente motivate, dal richiedere ai lavoratori di riprendere la loro attività in una situazione di lavoro in cui persiste un pericolo grave ed immediato;
- f) segnalare tempestivamente al datore di lavoro o al dirigente sia le deficienze dei mezzi e delle attrezzature di lavoro e dei dispositivi di protezione individuale, sia ogni altra condizione di pericolo che si verifichi durante il lavoro, delle quali venga a conoscenza sulla base della formazione ricevuta;
- g) frequentare appositi corsi di formazione secondo quanto previsto dall'articolo 37 del D.Lgs. n. 81/2008.

I **Dipendenti**, ovvero coloro che il D.lgs. n. 81/2008 definisce quali "**Lavoratori**", sono obbligati a prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro.

Essi devono, in particolare:

- a) contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;
- b) osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale;
- c) utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto e, nonché i dispositivi di sicurezza;
- d) utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;
- e) segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d), nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla successiva lettera
- f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;
- g) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
- h) 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;
- i) partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;
- j) sottoporsi ai controlli sanitari previsti dal presente decreto legislativo o comunque disposti dal medico competente.

Al **Medico Competente** sono attribuite le responsabilità ed i compiti di cui agli articoli 38, 39, 40 e 41 del D.Lgs. n. 81/2008

Inoltre, qualora l'Azienda affidi lavori ad una o più imprese appaltatrici od a lavoratori autonomi, il Datore di Lavoro assume gli obblighi previsti dall'articolo 26 del D.Lgs. n. 81/2008 relativo ai **contratti di appalto o d'opera o di somministrazione**, ed in particolare gli obblighi collegati:

- alla verifica della idoneità tecnico professionale delle imprese appaltatrici o dei lavoratori autonomi in relazione ai lavori, ai servizi e alle forniture da affidare in appalto o mediante contratto d'opera o di somministrazione;
- al fornire dettagliate informazioni sui rischi specifici esistenti nell'ambiente nel quale i predetti soggetti sono destinati ad operare e sulle misure di prevenzione ed emergenza adottate in relazione alla propria attività;
- al cooperare nell'attuazione delle misure di protezione e prevenzione dei rischi incidenti sull'attività lavorativa oggetto dell'appalto;
- al coordinare gli interventi di protezione e prevenzione cui sono esposti i lavoratori, informandosi reciprocamente anche al fine di eliminare i rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva;
- al predisporre il Documento Unico di Valutazione dei Rischi da Interferenza (DUVRI);

Laddove i lavori oggetto di appalto consistessero in lavori edili o di ingegneria civile riportati nell'allegato X del D.Lgs. n. 81/2008, al Datore di Lavoro, in qualità di committente, si applicano inoltre le disposizioni sui cantieri temporanei e mobili previste dagli artt. 88 e seguenti del D.Lgs. n. 81/2008

#### **5.1.7. Individuazione delle funzioni aziendali corrispondenti**

Nell'ambito dell'organizzazione della Sicurezza aziendale, ferme restando le nomine formalizzate del RSPP, del Medico Competente, dei componenti le Squadre di Primo Soccorso ed Anti-Incendio, le altre posizioni che rilevano ai fini della normativa applicabile (D.Lgs. 81/2008), e ciò a prescindere dalla individuazione civilistica della qualifica, sono i seguenti:

1. DATORE DI LAVORO: risulta ricoprire tale funzione, in forza dei poteri attribuiti dalla legge istitutiva dell'Azienda dallo Statuto e dal regolamento di Organizzazione, il Direttore Generale;
2. DIRIGENTI: risultano ricoprire tale funzione, in base a provvedimento di determina del Direttore Generale, tutti i dirigenti presenti in Azienda ossia il dott. Luigi Bussi dirigente del servizio Rapporti Istituzionali e Organizzazione, l'Avv. Franco Bartolomei dirigente del Servizio Avvocatura, il dott. Lino Gaspare Barcaroli dirigente del Servizio Gestione Immobili, l'Ing. Giancarlo Mongelli Dirigente del servizio Tecnico;
3. PREPOSTI: risultano ricoprire tale funzione, in base a provvedimento di determina del Direttore, tutti i quadri presenti in Azienda

#### **5.1.8. Misure Generali di Tutela**

Oltre alla predisposizione ed aggiornamento periodico del Documento di Valutazione dei Rischi, l'Azienda pone in essere le seguenti misure generali di tutela:

- a) programmazione e destinazione di adeguate risorse economiche, umane ed organizzative per il rispetto delle misure di prevenzione e sicurezza, per la verifica della loro attuazione e per la vigilanza sull'osservanza degli adempimenti prescritti;
- b) programmazione dei processi produttivi in modo da ridurre al minimo l'esposizione a rischio dei lavoratori, in relazione ai rischi individuati nel DVR;

- c) rispetto dei principi ergonomici nell'organizzazione del lavoro, nella concezione dei posti di lavoro, nella scelta delle attrezzature e nella definizione dei metodi di lavoro e produzione;
- d) riduzione dei rischi alla fonte; sostituzione di ciò che è pericoloso con ciò che non lo è o lo è meno; limitazione al minimo del numero dei lavoratori che sono, o che possono essere, esposti al rischio;
- e) utilizzo limitato degli agenti chimici, fisici e biologici sui luoghi di lavoro;
- f) priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale;
- g) controllo sanitario dei lavoratori;
- h) allontanamento del lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e l'adibizione, ove possibile, ad altra mansione;
- i) informazione e formazione adeguate per i lavoratori;
- j) informazione e formazione adeguate per dirigenti e i preposti;
- k) informazione e formazione adeguate per i rappresentanti dei lavoratori per la sicurezza;
- l) istruzioni adeguate ai lavoratori;
- m) partecipazione e consultazione dei lavoratori;
- n) partecipazione e consultazione dei rappresentanti dei lavoratori per la sicurezza;
- o) programmazione delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, anche attraverso l'adozione di codici di condotta e di buone prassi;
- p) misure di emergenza da attuare in caso di primo soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato;
- q) uso di segnali di avvertimento e di sicurezza;
- r) regolare manutenzione di ambienti, attrezzature, impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti;
- s) rispetto delle disposizioni aziendali in materia di sicurezza e l'utilizzo dei DPI sono costantemente monitorati da parte dei dirigenti e/o preposti, che ne esigono l'osservanza, segnalando al datore di lavoro o suo delegato per gli opportuni provvedimenti, anche disciplinari, le ipotesi di violazione.

#### **5.1.9. Protocolli specifici**

L'art. 30 D.Lgs. 81/08 stabilisce i criteri che devono essere posseduti dal Modello organizzativo in materia di sicurezza sul lavoro, affinché l'adozione di quest'ultimo abbia efficacia esimente ai sensi del D.Lgs. n. 231/01, prevedendo che *"i modelli di organizzazione aziendale definiti conformemente alle Linee Guida UNI INAIL per un sistema di gestione della salute e sicurezza sul lavoro (SGSL) [...] si presumono conformi, per le parti corrispondenti"*.

#### **5.1.10. Flussi Informativi e attività dell'Organismo di Vigilanza**

Al fine di consentire all'Organismo di vigilanza di monitorare efficacemente le misure di prevenzione e protezione poste in atto dall'Azienda allo scopo di prevenire gli infortuni sul lavoro, evitando al contempo



inutili sovrapposizioni con l'attività di controllo già delegata alle strutture aziendali competenti, si prevede che pervengano all'Organismo di vigilanza, con le scadenze predefinite e per la parte di competenza in relazione alle attività svolte dall'Azienda, i seguenti documenti e relazioni:

- relazione scritta periodica del R.S.P.P. al Datore di Lavoro, contenente la descrizione della situazione delle aree operative per quanto riguarda l'igiene e sicurezza sul lavoro (stato del sistema di prevenzione e protezione implementato in Azienda) e la prevenzione incendi.
- notifica tempestiva degli infortuni e incidenti, con particolare riguardo a quelli con prognosi maggiore o uguale a 20 gg. L'organismo in tali casi potrà acquisire dal Datore di lavoro o suo delegato, dall'R.S.P.P. e dal R.S.L.:
  - ✓ le informazioni necessarie per verificare le cause dell'infortunio stesso
  - ✓ le ragioni per le quali le misure di prevenzione e sicurezza non hanno, in tutto o in parte, funzionato
  - ✓ le indicazioni circa le misure correttive che si intendono adottare per evitare la ripetizione delle condizioni che hanno consentito l'infortunio
  - ✓ i successivi riscontri circa la effettiva adozione delle misure correttive;
- messa a disposizione del documento di valutazione del rischio di cui all'articolo 28 del T.U. in materia di Sicurezza (D.Lgs. 81/08), ivi compreso l'elenco delle sostanze pericolose e nocive ai sensi della normativa vigente;
- segnalazione tempestiva delle situazioni anomale riscontrate dal Medico Competente nell'ambito delle visite periodiche o programmate. Tali segnalazioni, nel rispetto delle norme sulla privacy, saranno riferite al tipo di mansione, alle sostanze utilizzate ed alla lavorazione che il medico competente ritiene possa avere incidenza sulla salute del lavoratore;
- segnalazione, da parte del RSPP, della effettuazione degli interventi di modifica del DVR formativi in materia di sicurezza, prevenzione ed igiene del lavoro, ovvero segnalazione della mancata effettuazione di quelli programmati, indicandone le ragioni. L'Organismo di vigilanza, inoltre, assistere alle riunioni annuali sulla sicurezza.

L'Organismo di vigilanza potrà, infine, sulla base delle informazioni pervenutegli, chiedere al RSPP o agli altri Destinatari della presente Parte Speciale gli ulteriori approfondimenti che riterrà opportuni.

In ogni caso, delle verifiche svolte a seguito delle segnalazioni, notifiche e comunicazioni di cui sopra, l'Organismo di Vigilanza provvederà a dare riscontro scritto nel verbale di sua competenza e nell'informativa al Consiglio di Amministrazione, indicando anche le eventuali ulteriori segnalazioni ai fini di prevenzione che ritenesse di annotare.

Nell'ambito delle proprie competenze, l'Organismo di Vigilanza potrà effettuare verifiche a campione, periodiche od occasionali, in merito al rispetto delle norme in materia di prevenzione infortuni, sicurezza ed igiene del lavoro, dandone atto nel verbale di propria competenza e nella relazione periodica al Consiglio di Amministrazione.

Ove riscontri inadempienze, ne darà tempestiva segnalazione al RSPP e al Consiglio di Amministrazione per i necessari interventi correttivi e sanzionatori.

#### **5.1.11. Informazione e Formazione**

In base al sistema di prevenzione e protezione adottato dall'Azienda e ai sensi di quanto previsto dagli articoli 36 e 37 del D.Lgs. n. 81/2008 tra i compiti del Datore di Lavoro e dei Dirigenti rientrano anche i seguenti:

- provvedere affinché tutti i lavoratori, che prestano servizio subordinato o ausiliario o autonomo, ricevano un'adeguata informazione sui rischi per la sicurezza e la salute connessi all'attività dell'unità locale in generale e sui rischi specifici cui gli stessi lavoratori siano esposti in relazione all'attività svolta nei rispettivi posti di lavoro, nonché circa le misure e le attività di protezione e prevenzione aziendali adottate, rendendo note le norme essenziali di prevenzione, sicurezza ed igiene mediante affissione, negli ambienti di lavoro, di estratti delle stesse o comunque con ogni altro mezzo idoneo a renderne più utile ed immediata la conoscenza, secondo le regole di cui all'articolo 36 del T.U. in materia di sicurezza (D.Lgs. 81/08), anche mediante appositi corsi di formazione in aula; ove l'informazione riguardi lavoratori stranieri, va fatta verifica preliminare della comprensione della lingua utilizzata per il percorso formativo;
- provvedere affinché tutti i lavoratori, che prestino servizio subordinato o ausiliario o autonomo, ricevano una formazione sufficiente e adeguata in materia di sicurezza e di salute, con particolare riferimento al proprio posto di lavoro ed alle proprie mansioni, secondo le regole di cui all'articolo 37 del del T.U. in materia di sicurezza (D.Lgs. 81/08);
- disporre, controllare ed esigere, anche in applicazione di norme disciplinari, che i lavoratori tutti osservino le norme di legge e le disposizioni interne in materia di sicurezza e igiene del lavoro, prevenzione incendi e tutela dell'ambiente, in particolare utilizzando i mezzi di protezione collettivi messi a loro disposizione e i dispositivi di protezione individuali da fornire loro, sentito il Responsabile del Servizio di Prevenzione e Protezione.

Tutta la formazione erogata viene regolarmente rendicontata mediante redazione di verbale da inserire in ciascuna cartella personale ed in una raccolta, preferibilmente informatica, a cura del R.S.P.P.

Per quanto concerne l'informazione e la formazione relativa al presente Modello Organizzativo, l'Organismo di vigilanza organizzerà sessioni formative dirette ai Destinatari. Tale formazione sarà riproposta con cadenza triennale, e comunque nel caso in cui si renda necessario e/o opportuno aggiornare i Destinatari in merito ad eventuali modifiche normative e/o organizzative dell'Azienda ovvero nel caso risulti modificato il novero dei Destinatari.

## 6. PARTE “E” - REATI IN MATERIA DI CRIMINALITÀ INFORMATICA

### 6.1.1. Le Fattispecie di Reati in materia di criminalità informatica

L'Art. 24-bis del D.Lgs. 231/2001 contempla i delitti informatici e trattamento illecito dei dati. In particolare:

- Falsità in un documento informatico pubblico o privato avente efficacia probatoria (art. 491 -bis c.p.).
- Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.).
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.).
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.).
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.).
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.).
- Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.).
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.).
- Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.).
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.).
- Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.).

Falsità in un documento informatico pubblico o privato avente efficacia probatoria (art. 491-bis c.p.)

Le prime fattispecie (dall'art.476 c.p all'art.493 c.p.) richiamate in modo esplicito dall'art. 491 bis c.p. riguardano i reati di falso nei documenti informatici. In particolare, il bene giuridico tutelato, dalle fattispecie di reato di cui al capo III del titolo VII del codice penale, è la fede pubblica documentale ; si tratta di quella particolare fiducia che la collettività ripone sulla veridicità o autenticità di un documento.

Per documento informatico si intende qualsiasi 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.

I reati di falso possono avere ad oggetto un atto pubblico oppure una scrittura privata.

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.

Le nozioni di pubblico ufficiale, incaricato di pubblico servizio ed esercente di un servizio di pubblica necessità sono contenute rispettivamente negli artt. 357, 358 e 359 c.p.

Accesso abusivo ad un sistema informatico o telematico (art.615-ter c.p.)

Il reato consistente nella condotta di chi 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 reato previsto è consistente nella condotta di chi, al fine di procurare a sè o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

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

Il reato consiste nella condotta di chi, 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 reato consiste nella condotta di chi fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe.

Salvo che il fatto costituisca più grave reato, detto reato si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle predette comunicazioni.

*Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)*

Il reato è consistente nella condotta di chi, 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 reato consiste nella condotta di chi, salvo che il fatto costituisca più grave reato, distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

*Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità, (art.635-ter c.p.)*

Il reato consiste nella condotta di chi, salvo che il fatto costituisca più grave reato, 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.

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

Il reato consiste nella condotta di chi, salvo che il fatto costituisca più grave reato, 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 o telematici di pubblica utilità, (art. 635-quinquies c.p.)*

Il reato consiste nella condotta di chi, salvo che il fatto costituisca più grave reato, mediante le condotte di cui all'articolo 635-bis c.p., ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, 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.

*Frode informatica del soggetto che presta servizi di certificazione di firma elettronica, (art. 640-quinquies c.p.)*

Il reato consiste nella condotta del 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. Tale reato si configura quindi come un reato proprio, cioè che può essere commesso solo da chi possiede la qualifica del fornitore dei servizi di certificazione di firma elettronica.

**Configurabilità dei reati nell'Azienda**

In generale gli enti operanti nell'E.R.P. gestiscono un sistema informativo di interesse pubblico e le loro attività sono pressoché integralmente gestite da procedure informatiche. In linea di principio quindi i reati in questione attraversano l'intera organizzazione aziendale.

L'Azienda si è dotata di regolamenti, protocolli specifici, e idonei meccanismi di controllo volti a impedire alterazioni del sistema informativo aziendale.

È da considerarsi, inoltre, che nell'espletamento delle proprie funzioni, una parte del personale dell'Azienda, dispone di credenziali per l'accesso a banche dati esterne di proprietà di soggetti pubblici, tra le quali si segnalano:

- Agenzia delle Entrate;
- Catasto;

- Anagrafe reddituale.

Il reato Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.), non sembra configurabile all'interno del contesto aziendale, mancando la qualifica soggettiva presupposto del reato, in quanto le società di E.R.P. non svolgono il servizio di certificazione di firma elettronica.

#### **6.1.2. Le Aree a Rischio ed i Reati**

L'analisi delle Aree aziendali ha consentito di individuare alcune Attività aziendali per le quali potrebbero sussistere rischi di commissione dei reati in materia di crimini informatici.

Nell'ambito della suddetta analisi sono state identificate le fasi/Attività aziendali critiche, i soggetti e/o le Funzioni aziendali interessate, realizzando una completa Mappatura dei Rischi tra i reati previsti dal Decreto, le Funzioni aziendali interessate, i Processi/Attività aziendali correlati, i Protocolli/ Controlli preventivi/le regole da adottare, il livello di rischio previsto.

Per quanto attiene alle finalità del Decreto le Attività di ATER sono considerate in ottica di Processo, al fine di facilitare l'individuazione delle Attività aziendali critiche, a rischio e/o che possono avere un impatto diretto o indiretto nella possibile commissione dei reati rilevanti di cui al Decreto.

L'elencazione dei Processi/Funzioni aziendali a rischio reato (v. Mappatura dei Rischi) devono considerarsi non in senso esaustivo o chiuso, essendo possibile che in futuro e/o in occasione di modifiche organizzative interne, tale Mappatura dei Rischi venga opportunamente adattata o modificata.

All'interno della Mappatura dei Rischi sono richiamati i Protocolli/Controlli preventivi ritenuti rilevanti per contrastare validamente le possibilità di commissione di reato. La descrizione di tali Protocolli/Controlli preventivi è contenuta all'interno di tutte le Policies, le Procedure e le disposizioni di ATER da seguire (e far seguire) nei vari Processi aziendali.

Per quanto attiene a ATER le possibili violazioni al sistema informatico interno con finalità di commissione dei reati trattati nel presente capitolo e che possono avere quindi un impatto diretto o indiretto su quanto previsto dal Decreto, sono considerate nelle Policies formalizzate sui controlli d'accesso fisico e logico dei sistemi, delle reti telematiche e degli archivi informatici come richiamate nella Mappatura dei Rischi.

Di seguito si riportano comunque per completezza di trattazione, i principali riferimenti stralciati dalla Mappatura dei Rischi.

**6.1.3. Fattispecie di Reato in tema di delitti informatici riferibili alle risorse e sistemi interni aziendali**

| FATTISPECIE DI REATO  | CORRELATE ATTIVITÀ AZIENDALI A RISCHIO  | FUNZIONI AZIENDALI COINVOLTE NELLE SUDETTE ATTIVITÀ AZIENDALI  |
|---|---|--|
| <p>Falsità di documenti informatici (art. 491 bis)</p> <p>Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)</p> <p>Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater)</p> <p>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o danneggiamento di informazioni, dati e programmi informatici (art.635 bis)</p> <p>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater)</p> <p>Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies)</p> <p>Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis)</p> <p>Danneggiamento di sistemi informatici o telematici (art. 635 quater)</p> | <p>⇒ Accesso ai sistemi, PC e risorse contenenti dati aziendali</p> <p>⇒ Utilizzo dei mezzi di comunicazione elettronica (internet, posta elettronica, etc.)</p> <p>⇒ Accesso alle reti ed ai sistemi</p> <p>⇒ Manutenzione di software di sistema ed applicativi interni</p> <p>⇒ Utilizzo di supporti esterni elettronici (CD rom, "pen drive", etc.)</p> <p>⇒ Gestione delle autorizzazione d'accesso (Password, etc.)</p> | <p>⇒ Servizio Rapporti Istituzionali e Organizzazione</p> <p>⇒ Servizio Amministrazione, Controllo e Tesoreria</p> <p>⇒ Servizio Avvocatura</p> <p>⇒ Servizio Gestione Immobili</p> <p>⇒ Servizio Patrimonio</p> <p>⇒ Servizio Tecnico</p> |

**6.1.4. Responsabilità dei Protocolli/Controlli preventivi**

Si rinvia alla Mappatura dei Rischi per il dettaglio dei diversi livelli di responsabilità all'interno della Società di primo livello e dei livelli successivi in riferimento ad ogni Attività aziendale a rischio reato.

In particolare, la responsabilità di primo livello del rispetto dei Protocolli/Controlli preventivi della Azienda è attribuita ai dirigenti mentre per la responsabilità di secondo livello è attribuita ai quadri.

#### **6.1.5. Destinatari della parte speciale "E"**

Destinatari della presente parte speciale sono tutti i soggetti che svolgono attività implicanti l'utilizzo di strumenti informatici, trattandosi di reati comuni. Particolarmente delicato risulta essere il ruolo dell'Ufficio Sistemi Informativi .

#### **6.1.6. Regole di Carattere Generale**

Gli organi di A.T.E.R. ed i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti hanno l'obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate.

In coerenza con il Codice Etico e le procedure aziendali, i medesimi hanno l'obbligo di:

- a) porre in essere correttamente e legalmente, in modo trasparente e collaborativo, tutte le attività di gestione delle risorse informatiche;
- b) rispettare le disposizioni di legge e le regole aziendali, ponendo la massima attenzione, professionalità ed accuratezza, nell'utilizzo dei sistemi informatici;
- c) monitorare e tener traccia dell'utilizzo del sistema informatico, dei programmi delle licenze e delle password personali e di sistema.

#### **6.1.7. Protocolli Specifici**

Oltre ai protocolli esistenti in Azienda e già citati in precedenza con riferimento ad altre fattispecie di rischio, che qui si intendono per richiamati, l'Azienda ha già predisposto ed adottato:

- ✓ Codice Etico e di comportamento;
- ✓ Documento Programmatico sulla Sicurezza: anche se di fatto l'obbligo della stesura ed aggiornamento annuale del D.P.S. è venuto meno con il decreto semplificazioni (DL 5/2012), resta la validità concettuale del documento come previsto dalla prima stesura del D.Lgs. 196/03 (Allegato B) e delle relative misure minime di sicurezza.
- ✓ Regolamento per l'utilizzo del sistema informatico (Ordine di servizio n. 2 del 17.02.2009);
- ✓ Sistemi di autenticazione informatica: l'accesso ai sistemi informatici è consentito solo attraverso password personali che permettono di verificare in modo puntuale la condotta degli utenti nella corretta esecuzione delle funzioni informatiche e possono servire per circoscrivere i responsabili di ipotesi delittuose.
- ✓ Sistemi di autorizzazione: è stata impostata la profilazione dei singoli utenti (o gruppi di utenti) nell'utilizzo delle risorse informatiche (compresi programmi gestionali e contabili), con la funzione di limitare l'accesso ai soli dati di propria competenza, in base alle regole organizzative dell'Azienda.

A.T.E.R. sta inoltre sviluppando i seguenti protocolli:

- ✓ una procedura per formalizzare e documentare gli interventi di gestione effettuati da soggetti esterni all'azienda;

- ✓ una procedura preordinata a regolare l'acquisto di nuovi software e a monitorare le scadenze delle licenze aziendali:
- ✓ una clausola risolutiva espressa nei contratti con i terzi, al fine di regolare l'eventuale violazione del Codice Etico e del Modello.

Naturalmente si sottolinea come la rapida evoluzione dal lato tecnologico debba imporre frequenti aggiornamenti ed adeguamenti dei protocolli vigenti, per accrescerne la loro efficacia complessiva.

#### **6.1.8. Flussi Informativi ed Attività dell'Organismo di Vigilanza**

L'Organismo ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione e repressione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello.

Inoltre all'Organismo di vigilanza deve essere tempestivamente segnalata ogni notizia o evidenza relativa all'utilizzo dei sistemi informatici aziendali e di terzi effettuato in violazione delle norme aziendali o legali.

L'Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, delle fasi di ciascuna Operazione a Rischio, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione per prevenire e, se del caso, reprimere, ogni comportamento che sia in contrasto con le regole aziendali.

Inoltre, tutti i membri dell'Azienda saranno tenuti a segnalare all'Organismo di vigilanza ogni notizia o evidenza riguardante l'utilizzo dei sistemi informatici effettuato in violazione delle norme aziendali o legali nonché riguardanti la violazione di diritti di proprietà industriale di terzi.

Si ricorda infine che qualsivoglia sistema di controllo e/o di monitoraggio dell'attività dei dipendenti, spesso utilizzato come primo presidio a fronte dei rischi -reato in materia informatica, dovrà essere conforme allo statuto dei lavoratori (legge 300/1970) ed alle disposizioni emesse dal garante della Privacy (leggasi le linee guida del Garante per posta elettronica e internet pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007).

#### **6.1.9. Formazione ed informazione.**

E' necessario porre molta enfasi alla sensibilizzazione di soggetti apicali, sottoposti nonché di consulenti e collaboratori esterni, a riguardo della corretta utilizzazione dei sistemi e degli strumenti informatici.

Occorre consapevolezza generale che alcuni comportamenti possono generare un rischio per l'Azienda e di conseguenza consapevolezza sulle corrette procedure, controlli e sistemi di prevenzione adottati. L'informazione e la formazione hanno, dunque, in ciò una parte di grande rilievo.



## 7. PARTE “F” - REATI AMBIENTALI

### 7.1.1. Le Fattispecie di Reati Ambientali

Le fattispecie di reato di cui all'Art. 25-undecies D.Lgs. 231/2001 sono le seguenti:

- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.).
- Distruzione o deterioramento di habitat all'interno di un sito protetto (art. 733-bis c.p.).
- Inquinamento idrico (art. 137)
- Gestione di rifiuti non autorizzata (art. 256):
  - raccolta, trasporto, recupero, smaltimento, commercio e intermediazione di rifiuti, non pericolosi e pericolosi, in mancanza della prescritta autorizzazione, iscrizione o comunicazione (art. 256, co. 1, lett. a) e b).
  - realizzazione o gestione di una discarica non autorizzata (art. 256, co. 3, primo periodo).
  - realizzazione o gestione di discarica non autorizzata destinata, anche in parte, allo smaltimento di rifiuti pericolosi (art. 256, co. 3, secondo periodo).
  - attività non consentite di miscelazione di rifiuti (art. 256, co. 5).
  - deposito temporaneo presso il luogo di produzione di rifiuti sanitari pericolosi (art. 256, co. 6).
- Bonifica dei siti (art. 257):
  - inquinamento del suolo, del sottosuolo, delle acque superficiali e delle acque sotterranee con il superamento delle concentrazioni soglia di rischio (sempre che non si provveda a bonifica, in conformità al progetto approvato dall'autorità competente) e omissione della relativa comunicazione agli enti competenti (co. 1 e 2). La condotta di inquinamento di cui al co. 2 è aggravata dall'utilizzo di sostanze pericolose.
- Falsificazioni e utilizzo di certificati di analisi di rifiuti falsi (artt. 258 e 260-bis):
  - predisposizione di un certificato di analisi dei rifiuti falso (per quanto riguarda le informazioni relative a natura, composizione e caratteristiche chimico-fisiche dei rifiuti) e uso di un certificato falso durante il trasporto (art. 258, co. 4, secondo periodo).
  - predisposizione di un certificato di analisi di rifiuti falso, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti - SISTRI; inserimento di un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti (art. 260-bis, co. 6).
  - trasporto di rifiuti pericolosi senza copia cartacea della scheda SISTRI –Area movimentazione o del certificato analitico dei rifiuti, nonché uso di un certificato di analisi contenente false indicazioni circa i rifiuti trasportati in ambito SISTRI (art. 260-bis, co. 6 e 7, secondo e terzo periodo).
  - trasporto di rifiuti con copia cartacea della scheda SISTRI – Area movimentazione fraudolentemente alterata (art. 260-bis, co. 8, primo e secondo periodo). La condotta di cui al co. 8, secondo periodo, è aggravata se riguarda rifiuti pericolosi.
- Traffico illecito di rifiuti (artt. 259 e 260):
  - spedizione di rifiuti costituente traffico illecito (art. 259, co. 1). La condotta è aggravata se riguarda rifiuti pericolosi attività organizzate, mediante più operazioni e allestimento di mezzi e attività continuative, per il traffico illecito di rifiuti (art. 260). Delitto, caratterizzato da dolo specifico di ingiusto profitto e pluralità di condotte rilevanti (cessione, ricezione, trasporto, esportazione, importazione o gestione abusiva di ingenti quantitativi di rifiuti). La pena è aggravata in caso di rifiuti ad alta radioattività (co. 2).
- Inquinamento atmosferico (art. 279):
- Reati previsti dalla Legge 7 febbraio 1992, n. 150 in materia di commercio internazionale di esemplari di flora e fauna in via di estinzione e detenzione animali pericolosi
- Reati previsti dalla Legge 28 dicembre 1993, n. 549, in materia di tutela dell'ozono stratosferico e dell'ambiente
- Reati previsti dal D.Lgs. 6 novembre 2007, n. 202, in materia di inquinamento dell'ambiente marino provocato da navi:

#### Inquinamento idrico (art. 137 D.Lgs. 152/2006)

Per quanto concerne gli scarichi industriali sono sanzionati gli scarichi di acque reflue industriali contenenti sostanze pericolose:

- senza la necessaria autorizzazione da parte delle autorità competenti;

- in violazione delle prescrizioni imposte dall'autorizzazione ottenuta o da autorità competenti;
- il superamento dei valori limite tabellari fissati;

ed infine è sanzionata la violazione del divieto di scarico sul suolo, nelle acque e nel sottosuolo.

*Inquinamento Atmosferico (art. 279 D.Lgs. 152/2006) e tutela dell'ozono (L. 549/93)*

Sono sanzionate le violazioni ai valori limite di emissione o alle prescrizioni stabilite dall'autorizzazione o dalla normativa, dall'autorità competente che determini il superamento dei valori limite di qualità dell'aria previsti. In tema di tutela dell'ozono stratosferico (L. 549/1993) sono invece punite la produzione, il consumo, l'importazione, l'esportazione, la commercializzazione e la detenzione delle sostanze lesive, secondo quanto previsto dal Regolamento CE n. 3093/94 (quest'ultimo abrogato e sostituito da ultimo dal Regolamento CE n. 1005/2009).

*Attività di gestione rifiuti (art. 256 c1 D.Lgs. 152/2006)*

In merito all'attività di gestione di rifiuti non autorizzata, viene perseguito chiunque effettui una attività di raccolta, trasporto, recupero, smaltimento, commercio ed intermediazione di rifiuti in mancanza della prescritta autorizzazione, iscrizione o comunicazione. In questo caso potrebbe configurarsi comunque una responsabilità del produttore dei rifiuti a titolo di concorso nel reato. Ciò, non solo in caso di conoscenza della natura illecita dell'attività di gestione dei rifiuti concessa in appalto, ma anche in caso di violazione di specifici obblighi di controllo sul soggetto incaricato alla raccolta e smaltimento dei rifiuti prodotti.

Viene altresì sanzionato chiunque realizzi o gestisca una discarica non autorizzata, così come chi svolga attività non consentite di miscelazione di rifiuti non pericolosi con rifiuti pericolosi (art. 256 c.5 D.Lgs. 152/2006).

*Falsificazioni e utilizzo di certificati di analisi di rifiuti falsi (art. 258 c.4 D.Lgs. 152/2006).*

In questa fattispecie viene colpito l'ente che, in violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari, fornisca false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti ovvero faccia uso di un certificato falso durante il trasporto dei rifiuti medesimi.

*Deposito di rifiuti sanitari (art. 256 c.6 D.Lgs. 152/2006).*

Si precisa che il reato può considerarsi integrato qualora sussistano le seguenti condizioni:

- si tratti di rifiuti sanitari pericolosi a rischio infettivo compresi nell'elenco esemplificativo previsto dall'Allegato 1 del D.P.R. 15 luglio 2003 n. 254 "Regolamento recante disciplina della gestione dei rifiuti sanitari a norma dell'articolo 24 della L. 31 14 luglio 2002, n. 179";
- siano violati i limiti temporali o quantitativi previsti dall'art. 8 del D.P.R. 254/2003.

*Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260 bis commi 6,7, e 8 D.Lgs. 152/06).*

L'articolo punisce colui che, nella predisposizione di un certificato di analisi di rifiuti, utilizzato nell'ambito del sistema di controllo della tracciabilità dei rifiuti, fornisca false indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti e che inserisca un certificato falso nei dati da fornire ai fini della tracciabilità dei rifiuti.

**Configurabilità dei reati nel contesto dell'Azienda**

Tenendo conto delle attività svolte dall'azienda sembrano essere non concretamente configurabili i reati seguenti:

- Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (Codice Penale art. 727-bis).
- Distruzione o deterioramento di habitat all'interno di un sito protetto (Art. 733-bis Codice Penale).
- Disciplina dei reati relativi all'applicazione in Italia della convenzione sul commercio internazionale delle specie animali e vegetali in via di estinzione, (Legge 7 Febbraio 1992, n. 150).
- "Misure a tutela dell'ozono stratosferico e dell'ambiente (Legge 28 dicembre 1993, n. 549, Art. 3 comma 6) e Superamento valori limite di emissione e di qualità dell'aria (D.Lgs. 152/06 art. 279 c. 5),
- Inquinamento delle acque (D.Lgs. 152/06, art. 137).
- Inquinamento colposo provocato da navi (Art. 8 co.1 e 2 e Art. 9 co. 1 e 2 D.Lgs. 6 novembre 2007, n. 202).
- Reati di cui al D.Lgs. 3 aprile 2006, n. 152: Discarica non autorizzata (art. 256, comma 3, primo periodo), Deposito di rifiuti sanitari (art. 256 comma 6), traffico illecito di rifiuti (art. 259, comma 1), attività organizzate per il traffico illecito di rifiuti (art. 260, comma 1), anche ad alta radioattività (art. 260, comma 2). Queste ultime fattispecie di illeciti, presupponendo lo svolgimento di un'attività imprenditoriale relativa alla gestione dei rifiuti e di ingente quantità, non trovano riscontro con l'attività svolta in ambito E.R.P.

Tra i reati configurabili al contesto delle Aziende che operano nel contesto dell'E.R.P. possono rientrare i seguenti:

- Attività di gestione rifiuti (art. 256 c1 D.Lgs. 152/2006).
- Bonifica dei siti (art. 257 D.Lgs. 152/2006).
- Falsificazioni e utilizzo di certificati di analisi di rifiuti falsi (art. 258 c.4 D.Lgs. 152/2006).
- Miscelazione rifiuti (art. 256 c.5 D.Lgs. 152/2006).
- Sistema informatico di controllo della tracciabilità dei rifiuti (art. 260 bis commi 6,7, e 8 D.Lgs. 152/06).

Tali reati possono riguardare sia le attività di gestione rifiuti prodotti presso le sedi dell'Azienda E.R.P., sia le attività che coinvolgono il personale della stessa nei ruoli di Direzione Lavori per gli interventi di manutenzione, recupero e costruzione di immobili di E.R.P., ai sensi della normativa sugli appalti pubblici.

Nel primo caso occorre sottolineare, in genere, le modeste quantità e la non pericolosità dei rifiuti prodotti da attività puramente amministrative.

Nel secondo caso, per quanto tali reati siano direttamente commessi da personale dell'impresa aggiudicataria dell'appalto, può emergere una colpa in organizzazione a carico dell'Azienda, in particolare in relazione alle attività di inquinamento dei suoli e di smaltimento dei rifiuti prodotti in cantiere.

Occorre dunque valutare in concreto il corretto adempimento degli obblighi imposti da normativa alle imprese che, se non correttamente assolti, potrebbero fare insorgere una responsabilità in seno alla Azienda stessa. Specifiche prescrizioni a carico delle ditte appaltatrici in materia di smaltimento dei rifiuti, comprese le precise responsabilità nella predisposizione dei formulari dei rifiuti, devono trovare apposita indicazione all'interno del Capitolato d'appalto.

Ulteriori considerazioni devono essere infine fatte in relazione ai reati di cui all'art. 257 D.Lgs. 152/2006 (Siti contaminati). Tale reato prevede una duplice fattispecie:

- da una parte punisce chiunque cagioni l'inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee con il superamento delle concentrazioni soglia di rischio (CSR) ovvero non provveda alla bonifica in conformità al progetto approvato dall'autorità competente;
- dall'altra punisce lo stesso soggetto (il responsabile dell'inquinamento) nel caso di mancata effettuazione della comunicazione alle autorità competenti di cui all'articolo 242 D.Lgs. 152/2006.

Nel contesto dell'Azienda è chiaro che, difficilmente, possa manifestarsi una diretta responsabilità nel cagionare l'inquinamento (il responsabile dell'inquinamento, piuttosto, potrebbe essere individuato nell'impresa appaltatrice), mentre sembra meno remota l'ipotesi di responsabilità derivante da una mancata comunicazione da parte del Direttore Lavori, in caso di eventi che possano contaminare il sito o eventi che evidenziano un inquinamento pregresso dello stesso.

Ciò anche se, da una prima analisi, sembra esclusa (ai fini 231) la responsabilità di omessa comunicazione da parte del proprietario o gestore dell'area che invece è prevista dall'art. 245 comma II D.Lgs. 152/2006.

In ogni caso in queste fattispecie si ritiene di non poter escludere tout-court un coinvolgimento dell'Azienda in un procedimento penale a carico della persona fisica, con un rischio generico derivante da una colpa in organizzazione.

#### **7.1.2. Destinatari della parte speciale "F"**

Destinatari della presente parte speciale sono (in quanto rappresentanti il vertice aziendale ovvero per i poteri e le responsabilità espressamente ad essi conferiti ovvero per i compiti ad essi spettanti):

- ✓ il Presidente del CdA;
- ✓ il Direttore Generale;
- ✓ tutti coloro che si occupano della gestione delle problematiche ambientali all'interno della Azienda.

### **7.1.3. Regole di carattere generale**

Il presente protocollo ha la finalità di assicurare che le attività relative agli adempimenti e alla gestione delle tematiche ambientali, siano debitamente regolamentate e gestite, avvengano nel rispetto dei principi di trasparenza e correttezza e siano documentate in maniera chiara, accurata e precisa.

Tutte le attività dell'Azienda nelle aree a rischio sono svolte nel rispetto delle leggi vigenti, delle norme del Codice Etico e di comportamento, seguendo i principi, le procedure ed i protocolli aziendali di cui al presente Modello.

L'Azienda ha impostato il proprio Modello organizzativo conformemente ai requisiti di formalizzazione e chiarezza. E' stata attuata una separazione delle funzioni debitamente comunicate anche alle responsabilità e alla ripartizione dei ruoli e delle competenze.

### **7.1.4. Protocolli specifici**

L'azienda si è dotata di un:

- ✓ Codice Etico e di comportamento.

Per indirizzare la gestione ambientale alla compliance e al rispetto della normativa in materia ambientale, A.T.E.R. sta provvedendo:

- ✓ a introdurre e formalizzare alcune procedure che garantiscano la tracciabilità e documentazione dell'attività svolta, per:
  - la gestione di eventi che potrebbero comportare una contaminazione ambientale;
  - la gestione dei rifiuti prodotti dall'azienda;
- ✓ a introdurre, nei capitolati d'appalto, una disposizione che qualifichi formalmente l'appaltatore come produttore dei rifiuti generati dalle attività oggetto di appalto e lo obblighi contrattualmente all'osservanza di quanto previsto dal d.lgs. 152/2006 e alle ulteriori disposizioni vigenti in materia ambientale ed escluda qualsiasi responsabilità di A.T.E.R. connessa ad una gestione non conforme alle disposizioni di legge;
- ✓ a prevedere espressamente, nei contratti di locazione commerciale, l'obbligo in capo al locatario di rispettare la normativa ambientale vigente, con particolare riferimento a quella riguardante la gestione dei rifiuti, escludendo qualsiasi responsabilità di A.T.E.R. connessa ad una gestione non conforme alle disposizioni di legge;
- ✓ a rafforzare la formazione e il coinvolgimento dei ruoli e delle funzioni sensibili rispetto ai rischi della possibile commissione di reati;
- ✓ ad inserire una clausola risolutiva espressa nei contratti con i terzi, al fine di regolare l'eventuale violazione del Codice Etico e del Modello.

### **7.1.5. Flussi Informativi ed Attività dell'Organismo di vigilanza**

L'organismo di vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione per prevenire e, se del caso, reprimere, ogni comportamento che sia in contrasto con le regole aziendali.

L'Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione e repressione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello, fermo restando il dovere di osservare il

divieto di comunicare e/o diffondere le informazioni e/o dati acquisiti, salvo il caso in cui la comunicazione e/o la diffusione siano richieste da forze di polizia, dall'autorità giudiziaria, da organismi di sicurezza o da altri soggetti pubblici per finalità di difesa o sicurezza dello stato o di prevenzione, accertamento o repressione di reato.

## 8. PARTE “G” - REATI DI CRIMINALITA' ORGANIZZATA

### 8.1.1. Le Fattispecie di Criminalità Organizzata

Le fattispecie di reato di cui all'Art. 24-ter D.Lgs. 231/2001 sono le seguenti:

- Associazione per delinquere (art. 416 c.p.).
- Associazione per delinquere finalizzata a commettere i delitti di riduzione o mantenimento in schiavitù o in servitù, tratta di persone, acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 D.Lgs. 286/1998 (art. 416, co. 6, c.p.).
- Associazione di tipo mafioso (art. 416-bis c.p.).
- Delitti commessi avvalendosi delle condizioni previste dall'articolo 416-bis c.p. per le associazioni di tipo mafioso ovvero al fine di agevolare l'attività di tali associazioni.
- Scambio elettorale politico-mafioso (art. 416-ter c.p.).
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, DPR 9 ottobre 1990, n. 309).
- Sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.).
- Illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo (art. 407, co. 2, lett. a), n. 5), c.p.p.).

Le norme in esame riguardano la criminalità organizzata, fenomeno che provoca un elevato allarme sociale nella collettività a causa della maggiore potenzialità delinquenziale delle organizzazioni rispetto al singolo autore di reato, ovvero della maggiore pericolosità del programma criminoso dell'organizzazione rispetto al disegno criminoso del singolo individuo.

Le fattispecie di cui sopra si riferiscono alla semplice partecipazione, nonché alla promozione, direzione, costituzione, organizzazione di un'associazione, composta da tre o più persone e dotata, anche in minima parte, di una “strutturazione” (divisione di compiti, gerarchie etc.), e di “stabilità” che permettono di distinguere dal semplice concorso di persone nel reato, caratterizzato, invece, dall'occasionalità e accidentalità dell'accordo criminoso.

Lo scopo dell'associazione deve essere, anche se non unico e prevalente, quello di realizzare un programma criminoso, cioè la commissione di uno o più reati.

L'art. 24-ter, riferendosi genericamente ai reati di cui all'art. 416 c.p., considera come “ipotesi base” la commissione, in forma organizzata di qualsiasi delitto, ad esclusione di quelli, ritenuti più gravi, di cui all'art. 416 c. 6 c.p. nonché dei delitti previsti dal 407 c. 2 lett. a) n. 5 c.p.p.

Altre ipotesi aggravate a cui fa riferimento l'art. 24-ter sono quelle in cui i delitti (qualsiasi delitto) vengano commessi in forma associata avvalendosi della forza di intimidazione del sodalizio di tipo mafioso e della condizione di assoggettamento e di omertà che ne deriva, e quella in cui i delitti medesimi vengano commessi al fine di agevolare l'attività delle associazioni di tipo mafioso.

E' opportuno precisare che è associazione di tipo mafioso quella in cui coloro che ne fanno parte si avvalgono della forza intimidatrice e della condizione di assoggettamento e di omertà che ne deriva, per commettere delitti, nonché per acquisire in modo diretto o indiretto la gestione o il controllo di attività economiche, concessioni, autorizzazioni, appalti e servizi pubblici o per realizzare profitti o vantaggi ingiusti ovvero impedire il libero esercizio del voto o di procurare voti a sé o ad altri. E' punita, inoltre, la condotta di chi agevola l'attività delle associazioni di tipo mafioso o ottiene la promessa di voti in cambio di erogazione di denaro.

Le fattispecie associative, soprattutto quelle a carattere generale (art. 416 e art. 416-bis) comportano, almeno in astratto, la possibilità che, a fronte di qualunque delitto, possa essere contestato ad un soggetto individuato tra quelli di cui all'art. 5, comma 1, lett. a) e b) del Decreto, in presenza di una pianificazione di più delitti e di più autori, non tutti necessariamente dipendenti, anche il delitto associativo e, conseguentemente, la responsabilità amministrativa per l'ente di appartenenza ai sensi del D.Lgs. 231.

#### Configurabilità dei reati nel contesto dell'azienda

Il fenomeno della criminalità di tipo mafioso è, per sua natura, particolarmente incline ad attuare meccanismi di infiltrazione e condizionamento di grande pericolosità in modo assolutamente trasversale rispetto ai differenti campi imprenditoriali ed a seconda delle sue concrete ed esclusive esigenze. La peculiarità delle associazioni di tipo mafioso sono da un lato la forza di intimidazione e la conseguente condizione di assoggettamento e di omertà che si sviluppa sia all'interno della struttura associativa sia all'esterno, dall'altro le finalità che non sono necessariamente la commissione di delitti, ma anche il controllo dell'economia e della politica.

Come è noto, i delitti associativi sono reati a concorso necessario, nel senso che richiedono necessariamente la partecipazione di più persone per la configurazione del reato.

A tale riguardo la giurisprudenza ha elaborato negli anni la figura del concorso esterno nell'associazione mafiosa: il reato di concorso esterno in associazione mafiosa si verrebbe a configurare con la condotta di un soggetto esterno all'associazione a delinquere che apporti un contributo causale determinante al perseguimento degli scopi illeciti e alla vita stessa dell'associazione.

L'Azienda proprio per l'attività economica che è chiamata a svolgere, assume la qualifica di Stazione Appaltante e affida ad imprese esterne lavori di costruzione/ristrutturazione, ambito nel quale, purtroppo, si conoscono bene le capacità di infiltrazioni malavitose.

La selezione e la valutazione di affidabilità di tutti i soggetti (società e persone fisiche) che hanno rapporti con l'azienda, rappresenta uno dei presidi di prevenzione di infiltrazione criminale, da attuarsi attraverso l'acquisizione, anzitutto, delle dichiarazioni previste dalla normativa sugli appalti pubblici di cui al D.Lgs.163/2006 ed, in via generale, di quanto previsto dal Codice Antimafia (D.Lgs. 159/2011).<sup>4</sup>

Per quanto attiene al reato di cui all'art. 416 c.p. Associazione a delinquere, si ravvisa che esso può avere molteplici finalità, se associato ad altri reati, anche non rientranti nel novero dei reati 231: ad es: ambiente, tributario, fallimento, etc. L'associazione a delinquere è una fattispecie di illecito che non può escludersi tout court dai reati configurabili e, di conseguenza, andrà presidiato attraverso apposite previsioni contenute nel Codice Etico e attraverso un funzionamento corretto dell'organizzazione nel suo insieme.

### **8.1.2. Destinatari della parte speciale "G"**

Destinatari della presente parte speciale sono tutti i soggetti che intrattengono per conto dell'Azienda rapporti con soggetti terzi, in particolare coloro i quali curano i processi commerciali o amministrativo finanziari.

### **8.1.3. Regole di Carattere Generale**

Gli organi di A.T.E.R. ed i dipendenti o consulenti nell'ambito delle funzioni ad essi attribuiti hanno l'obbligo di rispettare le norme di legge, del Codice Etico e le regole previste dal presente Modello, con espresso divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti che realizzino le fattispecie di reato sopra elencate.

In particolare le procedure aziendali sono caratterizzate dalla separazione dei ruoli di impulso decisionale, di esecuzione e realizzazione, nonché di controllo, con adeguata formalizzazione e documentabilità delle fasi principali del processo.

In coerenza con il Codice Etico e le procedure aziendali, i medesimi hanno l'obbligo di:

- a) porre in essere correttamente e legalmente, in modo trasparente e collaborativo, tutte le attività di gestione delle risorse finanziarie;
- b) monitorare e tener traccia della provenienza e dell'impiego dei flussi finanziari, dei beni e delle altre risorse aziendali, nonché delle operazioni compiute in relazione ad essi;
- c) prestare attenzione e controllo su operazioni che per caratteristiche, entità o natura o per qualsivoglia altra circostanza conosciuta, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, inducano a ritenere – in base agli elementi a disposizione ed utilizzando la normale

---

<sup>4</sup> Il codice antimafia mantiene la distinzione fra comunicazione antimafia ed informazione antimafia: la prima (da richiedere alla Prefettura per la stipula dei contratti di importo superiore a 150.000 euro ed inferiore alla soglia comunitaria) attesta la sussistenza o meno di cause di decadenza, di sospensione e di divieto di cui all'art. 67, la seconda (da richiedere sempre alla Prefettura per la stipula di contratti di importo pari o superiore alla soglia comunitaria e per l'autorizzazione di subcontratti di importo superiore a 150.000 euro) comprende, inoltre, anche l'attestazione della sussistenza o meno di eventuali tentativi di infiltrazione mafiosa.

diligenza – che il denaro, i beni o le utilità oggetto delle operazioni medesime appaiano di provenienza delittuosa.

#### **8.1.4. Protocolli Specifici**

Oltre ai protocolli esistenti in Azienda e già citati in precedenza con riferimento ad altre fattispecie di rischio, che qui si intendono per richiamati, l'Azienda ha già predisposto ed adottato:

- ✓ Codice Etico;
- ✓ Regolamento di Contabilità

L'Azienda ha inoltre adottato dei protocolli per la "tracciabilità dei flussi finanziari ai sensi della l. 136/2010 e della l. 217/2010", da applicare obbligatoriamente per tutti i pagamenti relativi ad una commessa pubblica di lavori, servizi e/o forniture.

L'Azienda sta inoltre provvedendo:

- ✓ ad adottare una procedura che disciplini la tracciabilità dei flussi finanziari;
- ✓ ad inserire una clausola risolutiva espressa in tutti i contratti con i consulenti esterni e agenti operante in caso di violazione del Modello e Codice Etico.

#### **8.1.5. Flussi Informativi ed Attività l'Organismo di Vigilanza**

L'Organismo di Vigilanza potrà discrezionalmente attivarsi con controlli, verifiche ed ispezioni, anche con controlli a campione o a seguito di segnalazione, delle fasi di ciascuna Operazione a Rischio, evitando per quanto possibile di interferire con i processi decisionali aziendali, ma intervenendo prontamente con gli strumenti a sua disposizione per prevenire e, se del caso, reprimere, ogni comportamento che sia in contrasto con le regole aziendali.

L'Organismo di Vigilanza ha accesso, per i fini della attività ad esso attribuita, ad ogni documentazione aziendale che esso ritenga rilevante per la prevenzione e repressione di comportamenti contrari alle regole aziendali dettate dal Codice Etico e dal presente Modello.

Gli organi aziendali devono segnalare all'Organismo di Vigilanza ogni Operazione a Rischio.

Inoltre all'Organismo di Vigilanza devono essere tempestivamente segnalate le seguenti informazioni:

- esistenza di procedimenti penali che coinvolgono personale dell'Azienda quali imputati, testimoni o persone informate dei fatti;
- previsione di assunzione e/o di definizione di un accordo di consulenza da parte dell'Azienda con personale straniero non comunitario e/o di soggetti destinati a svolgere le attività presso paesi esteri.

Ulteriori certificazioni (certificato penale generale, certificato dei carichi pendenti), dovranno essere richieste nel caso di assunzione di personale, nomina di dirigenti e definizione di accordi e convenzioni con altri soggetti con i quali la società E.R.P. decide di entrare in rapporti di collaborazione/partnership.



## 9. ESCLUSIONI / NON APPLICABILITÀ

### 9.1.1. Le Fattispecie di Reato Previste dal Decreto ma non applicabili

In questa parte vengono richiamati i reati non trattati in dettaglio, in quanto, per la specifica attività svolta dall'Azienda, essi risultano non applicabili.

### 9.1.2. FALSITÀ IN MONETE, IN CARTE DI PUBBLICO CREDITO ED IN VALORI DI BOLLO (art. 25 bis del Decreto)

Le fattispecie di reato di cui all'Art. 25-bis D.Lgs. 231/2001 sono le seguenti:

- Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.).
- Alterazione di monete (art. 454 c.p.).
- Spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.).
- Spendita di monete falsificate ricevute in buona fede (art. 457 c.p.).
- Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.).
- Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.).
- Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.).
- Uso di valori di bollo contraffatti o alterati (art. 464 c.p.).
- Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.).
- Introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

#### **Configurabilità dei reati nel contesto dell'Azienda**

I reati afferenti a tale categoria sembrano non trovare alcuna applicazione concreta nelle società di E.R.P. in relazione alla tipologia di attività svolta dalle società.

Le uniche specifiche attenzioni andranno previste in relazione ai seguenti due aspetti:

- acquisto, utilizzo e gestione dei valori di bollo al fine dell'eventuale applicazione del reato di cui all'art. 464 c.p.;
- utilizzo senza specifica autorizzazione di progetti di terzi o di soluzioni realizzative che, in base ai loro caratteri di originalità e novità, siano coperti da diritti di proprietà industriale, al fine dell'eventuale applicazione del reato di cui all'art. 473 c.p.

### 9.1.3. DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO

Le fattispecie di reato di cui all'Art. 25-bis. 1 D.Lgs. 231/2001 sono le seguenti:

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

Tali reati fanno riferimento a fattispecie che turbano la libertà e la concorrenza dell'industria e del commercio o a frodi nell'esercizio del commercio tramite ad es. la vendita di sostanze non genuine o con segni mendaci, l'usurpazione di titoli di proprietà industriale, la contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari.

#### **Configurabilità dei reati nel contesto dell'Azienda**

I reati afferenti a tale categoria sembrano non trovare un'applicazione concreta nell'Azienda in relazione alle concrete attività aziendali svolte. Non ricorrono, infatti, i presupposti per la commissione dei reati quali essere un produttore di sostanze alimentari, di prodotti agroalimentari o

di prodotti industriali, di operare nel settore del commercio o di utilizzare prodotti coperti da un titolo di proprietà industriale

#### **9.1.4. REATI CON FINALITÀ DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO.**

L'articolo 25-quater non elenca specificamente i reati per i quali è prevista la responsabilità dell'ente, limitandosi a fare un rinvio generale "aperto" a tutte le ipotesi attuali e future di reati aventi finalità terroristiche od eversive previsti dal codice penale e dalle leggi speciali.

Le principali fattispecie di reato presenti nel nostro ordinamento sono le seguenti:

- Associazione con finalità di terrorismo anche internazionale o di eversione all'ordine democratico (Art. 270 bis c.p.).
- Assistenza agli associati (Art. 270 ter c.p.).
- Arruolamento con finalità di terrorismo anche internazionale (Art. 270 quater c.p.).
- Addestramento ad attività con finalità di terrorismo anche internazionale (Art. 270 quinquies c.p.).
- Attentato per finalità terroristiche o di eversione (Art. 280 c.p.).
- Atto di terrorismo con ordigni micidiali o esplosivi (Art. 280 bis c.p.).
- Sequestro di persona a scopo di terrorismo o di eversione (Art. 289 bis c.p.).
- Istigazione a commettere alcuno dei delitti preveduti dai Capi primo e secondo Titolo I, Libro II del codice penale (artt. 241 e segg. c.p., artt. 276 e segg. c.p.), (Art. 302 c.p.).
- Violazioni previste dall'art. 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo (New York, 9 dicembre 1999).

In questo ambito occorre richiamare anche l'art. 270 sexies del c.p. - Condotte con finalità di terrorismo: "Sono considerate con finalità di terrorismo le condotte che, per la loro natura o contesto, possono arrecare grave danno ad un Paese o ad un'organizzazione internazionale e sono compiute allo scopo di intimidire la popolazione o costringere i poteri pubblici o un'organizzazione internazionale a compiere o astenersi dal compiere un qualsiasi atto o destabilizzare o distruggere le strutture politiche fondamentali, costituzionali, economiche e sociali di un Paese o di un'organizzazione internazionale, nonché le altre condotte definite terroristiche o commesse con finalità di terrorismo da convenzioni o altre norme di diritto internazionale vincolanti per l'Italia".

#### **Configurabilità dei reati nel contesto dell'Azienda**

I reati afferenti a tale categoria sembrano in astratto non configurabili nell'Azienda in quanto, per la loro commissione, deve realizzarsi una condotta non compatibile con l'attività svolta nonché con la natura societaria.

Unica fattispecie della categoria che fa eccezione è il reato di Assistenza agli associati (art. 270 ter c.p.).

È penalmente rilevante, infatti, il fornire assistenza a soggetti ricollegabili alle associazioni terroristiche, ovvero dare loro rifugio, vitto, ospitalità, mezzi di trasporto o strumenti di comunicazione.

Nelle Aziende operanti nel contesto E.R.P. tale tipologia di reato può trovare configurazione nel processo di assunzione di nuovo personale (qualora non vengano espletati adeguati formali controlli sul candidato, anche verificando il casellario giudiziale e/o il certificato di carichi pendenti) e nel processo di inserimento di nuovi assegnatari (nonché componenti il nucleo familiare o loro ospiti) negli alloggi e conseguenti comunicazioni alle autorità competenti.

Quest'ultimo aspetto, naturalmente, deve tenere in considerazione la normativa vigente (es. normativa antiterrorismo di cui all'art. 2 del decreto legge 20 giugno 2012, n. 79, convertito in legge n. 131/2012).

Infine si cita anche il D.Lgs. 231/2007 il quale pone una serie di presidi per prevenire il fenomeno del finanziamento del terrorismo (oltre che il riciclaggio).

#### **9.1.5. PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI**

La fattispecie di reato di cui all'Art. 25-quater.1 D.Lgs. 231/2001 è la seguente:

- Pratiche di mutilazione degli organi genitali femminili (art. 583-bis c.p.).

#### **Configurabilità dei reati nel contesto dell'Azienda**

Trattasi di reati per la cui realizzazione è necessario che si ponga in essere una condotta materiale concretamente incompatibile con il tipo di attività svolta dall'Azienda.

### **9.1.6. DELITTI CONTRO LA PERSONALITÀ INDIVIDUALE**

Le fattispecie di reato di cui all'Art. 25-quinquies D.Lgs. 231/2001 sono le seguenti:

- Riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.).
- Prostituzione minorile (art. 600-bis c.p.).
- Pornografia minorile (art. 600-ter c.p.).
- Detenzione di materiale pornografico (art. 600-quater c.p.).
- Pornografia virtuale (art. 600-quater.1 c.p.).
- Iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-quinquies c.p.).
- Tratta di persone (art. 601 c.p.).
- Acquisto e alienazione di schiavi (art. 602 c.p.).

### **Configurabilità dei reati nel contesto dell'Azienda**

Trattasi di reati per la cui realizzazione è necessario che si ponga in essere una condotta materiale che sembra concretamente difficilmente compatibile con il tipo di attività svolta dall'Azienda.

### **9.1.7. DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO DI AUTORE**

Le fattispecie di reato di cui all'Art. 25-novies D.Lgs. 231/2001 sono le seguenti:

- Messa a disposizione del pubblico in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, e senza averne diritto di un'opera o di parte di un'opera dell'ingegno protetta (art. 171, co. 1, lett a-bis), L. 633/1941).
- Reato di cui al punto precedente commesso su un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera stessa, qualora ne risulti offeso l'onore o la reputazione dell'autore (art.171, co. 3, L. 633/1941).
- Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale o imprenditoriale ovvero concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi di protezione di programmi per elaboratori (art. 171-bis, co. 1, L. 633/1941).
- Riproduzione su supporti non contrassegnati SIAE, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati al fine di trarne profitto; estrazione o reimpiego della banca dati in violazione delle disposizioni sui diritti del costituente e dell'utente di una banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis, co. 2, L. 633/1941).
- Reati commessi a fini di lucro, per uso non personale, e caratterizzati da una delle seguenti condotte descritte all'art. 171-ter, comma 1, L. 633/1941:
  - ❖ abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio, di dischi, nastri o supporti analoghi ovvero di ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento (lett. a).
  - ❖ abusiva riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, di opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, multimediali, anche se inserite in opere collettive o composite o banche dati (lett. b).
  - ❖ introduzione nel territorio dello Stato, detenzione per la vendita o la distribuzione, distribuzione, messa in commercio, concessione in noleggio o cessione a qualsiasi titolo, proiezione in pubblico, trasmissione a mezzo televisione con qualsiasi procedimento, trasmissione a mezzo radio, delle duplicazioni o riproduzioni abusive di cui alle lettere a) e ) senza aver concorso nella duplicazione o riproduzione (lett. c).
  - ❖ detenzione per la vendita o la distribuzione, messa in commercio, vendita, noleggio, cessione a qualsiasi titolo, proiezione in pubblico, trasmissione a mezzo radio o televisione con qualsiasi procedimento, di videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, o altro supporto per il quale è prescritta l'apposizione del contrassegno SIAE, privi del contrassegno medesimo o dotati di contrassegno contraffatto alterato (lett. d).

- ❖ ritrasmissione o diffusione con qualsiasi mezzo di un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato, in assenza di accordo con il legittimo distributore (lett. e).
- ❖ introduzione nel territorio dello Stato, detenzione per la vendita o la distribuzione, distribuzione, vendita, concessione in noleggio, cessione a qualsiasi titolo, promozione commerciale, installazione di dispositivi o elementi di decodificazione speciale che consentono l'accesso a un servizio criptato senza il pagamento del canone dovuto (lett. f).
- ❖ fabbricazione, importazione, distribuzione, vendita, noleggio, cessione a qualsiasi titolo, pubblicizzazione per la vendita o il noleggio, o detenzione per scopi commerciali, di attrezzature, prodotti o componenti ovvero prestazione di servizi aventi impiego commerciale o prevalente finalità di eludere efficaci misure tecnologiche di protezione ovvero progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di tali misure (lett. f-bis).
- ❖ abusiva rimozione o alterazione di informazioni elettroniche sul regime dei diritti di cui all'articolo 102-quinquies, ovvero distribuzione, importazione a fini di distribuzione, diffusione per radio o per televisione, comunicazione o messa a disposizione del pubblico di opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse (lett. h).
- Reati caratterizzati da una delle seguenti condotte descritte all'art. 171-ter, comma 2, L. 633/1941:
  - ❖ riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre 50 copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi (lett. a).
  - ❖ immissione a fini di lucro in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera o parte di un'opera dell'ingegno protetta dal diritto d'autore, in violazione del diritto esclusivo di comunicazione al pubblico spettante all'autore (lett. a-bis).
  - ❖ realizzazione delle condotte previste dall'art. 171-ter, co. 1, L. 633/1941, da parte di chiunque eserciti in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, ovvero importazione di opere tutelate dal diritto d'autore e da diritti connessi (lett. b).
  - ❖ promozione od organizzazione delle attività illecite di cui all'art. 171-ter, co. 1, L. 633/1941 (lett. c).
- Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno, da parte di produttori o importatori di tali supporti, ovvero falsa dichiarazione circa l'assolvimento degli obblighi sul contrassegno (art. 171-septies, L. 633/1941).
- Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di 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 (art. 171-octies, L. 633/1941).

La legge n. 99 del 2009 ha inserito, tra i reati presupposto del D.Lgs. 231/2001, una serie di fattispecie contenute nella c.d. "legge sul diritto d'autore" (legge 22 aprile 1941 n. 633).

Le norme in esame tutelano il diritto morale e di utilizzo economico da parte del loro autore, delle opere dell'ingegno aventi carattere creativo, per es. quelle letterarie, musicali, arti figurative, cinematografiche, fotografiche, teatrali etc. nonché il software e le banche dati. A titolo esemplificativo e non esaustivo, si osserva che rientrano tra le opere dell'ingegno le fotografie, le sequenze video, poesie, commenti, recensioni, articoli e altri contenuti scritti, i files di musica di qualsiasi formato.

#### **Configurabilità dei reati nel contesto dell'Azienda**

Trattasi di reati (in particolare quelli di cui agli art. 171, 171 ter, 171 septies, 171 octies L. 633/1941) che non sembrano potersi concretamente realizzare nel contesto delle attività svolte dall'Azienda, in particolare per quanto attiene ai reati circa l'utilizzo di opere dell'ingegno, in quanto, in base alle informazioni disponibili, non sembra sussistere alcuna ipotesi applicabile.

Fanno eccezione i reati di cui all' art. art. 171-bis, co. 1 e co.2, L. 633/1941, i quali richiedono specifici protocolli relativi all'utilizzo del software e delle banche dati, al fine di prevenire la loro commissione.

I protocolli necessari per prevenire la commissione di tali reati si intrecciano fortemente con quelli relativi alla gestione dei sistemi informatici aziendali (ed alla normativa sulla privacy) in quanto, in

entrambi i casi, il loro compimento potrebbe essere sintomo di deficit organizzativi sul versante informatico (es. installazione, utilizzo di software privo di licenza, accesso ed utilizzo di banche dati esterne oltre gli scopi e le finalità aziendali, etc.).

#### **9.1.8. REATI TRANSAZIONALI (LEGGE 16 MARZO 2006, N. 146, ARTT. 3 E 10)**

Le fattispecie di reato previste dal D.Lgs. 231/01 sono le seguenti:

- Associazione per delinquere (art. 416 c.p.).
- Associazione di tipo mafioso (art. 416-bis c.p.).
- Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-quater del testo unico di cui al DPR 23 gennaio 1973, n. 43).
- Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74, DPR 9 ottobre 1990, n. 309).
- Disposizioni contro le immigrazioni clandestine (art. 12, co. 3, 3-bis, 3-ter e 5, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286).
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.).
- Favoreggiamento personale (art. 378 c.p.).

#### **Configurabilità dei reati nel contesto dell'Azienda**

Tale categoria di illeciti non risulta essere configurabile in astratto, se non limitatamente all'ipotesi di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci davanti all'autorità giudiziaria, per la quale dovranno essere inseriti appositi presidi all'interno del Codice Etico e/o di protocolli ad hoc.

#### **9.1.9. IMPIEGO DI LAVORATORI IRREGOLARI**

Le fattispecie di reato previste dall'Art. 25 duodecies del D.Lgs. 231/01 sono le seguenti:

- Impiego di lavoratori irregolari (art.22 c.12 bis D.Lgs. 286/1998).

Il 9 agosto 2012 è stato introdotto nel D.Lgs. 231/01 l'art. 25 duodecies intitolato "Impiego di cittadini di paesi terzi il cui soggiorno è irregolare". La condotta di riferimento è il comma 12 bis dell'articolo 22 del D.Lgs. 286/1998:

#### **Configurabilità dei reati nel contesto dell'Azienda**

Tale reato potrebbe configurarsi, in linea di principio, pur assumendo una probabilità alquanto bassa, nel caso in cui l'azienda assuma alle proprie dipendenze un lavoratore straniero il quale disponga di un permesso di soggiorno non valido e regolare in quanto scaduto, non rinnovato, o revocato.

Di conseguenza, i protocolli di assunzione e di gestione del personale dovranno prevedere appositi presidi a prevenzione del rischio in oggetto, per assicurare una puntuale verifica del possesso del permesso di soggiorno (in fase di selezione) ed una sua verifica periodica da parte delle funzioni di amministrazione del personale.