MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ex D.Lgs. 231/2001 integrato con sistema anticorruzione

Rev. 1 - Approvato da A.U. il 21 giugno 2024
F.TO

SOMMARIO

PARTE I
Il Sistema Preventivo 231

1. IL D.LGS. 8 GIUGNO 2001 N. 231

1.1. Linee Generali e Obiettivi

Il Decreto Legislativo n. 231, emanato in data 8 giugno 2001 su Legge Delega 29 settembre 2000 n. 300, è il risultato di un complesso processo di moralizzazione pubblica e societaria - da cui è scaturita anche l'imposizione di un attento controllo della legalità e della prevenzione anticorruzione - avviato su scala internazionale a partire dagli anni '90.

Si inseriscono in tale processo:

- l'importante Convenzione OCSE[1] «*sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali*» (stipulata a Parigi il 17 dicembre 1997, entrata in vigore il 15 febbraio 1999) e diretta a costruire un sistema di prevenzione generale della illegalità e della corruzione anche nell'ambito delle persone giuridiche;
- le 20 Linee Guida *"anticorruzione"* del GRECO[2], adottate dal Comitato dei Ministri del Consiglio d'Europa il 6 novembre 1997.

Anche in Italia, la decisione di adottare la Legge Delega n. 300/2000[3] - con la conseguente emanazione del Decreto Legislativo 231/2001 – è scaturita dalla considerazione che, mai come nel momento attuale, si assiste ad una crescente ed inammissibile proliferazione di disfunzioni, danni e condotte illecite, derivanti dalla gestione di strutture societarie, anche e soprattutto a carattere privatistico. Da qui la presa di coscienza: - che il *rischio di impresa* debba includere nel suo nucleo portante anche il cd. *rischio da illegalità*; - che la previsione di tale rischio (storicamente ricadente sulla collettività a causa del rigido principio di responsabilità penale personale in capo alla sola persona fisica) debba essere addossata a chi, della personalità giuridica, ne usufruisce in pieno di tutti i benefici.

Ciò premesso: il Decreto Legislativo 8 giugno 2001, n. 231, recante "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche*

---

[1] OCSE: L'*Organizzazione per la Cooperazione e lo Sviluppo Economico* (prima denominazione: OECE, Organizzazione per la cooperazione economica europea) è un organismo internazionale nato allo scopo di superare il periodo post bellico attraverso forme di cooperazione e di coordinamento (soprattutto in campo economico) tra le nazioni europee. Conta attualmente 37 membri attivi; è stato ufficialmente costituito in sostituzione dell'OECE a Parigi nel 1960.

[2] GRECO: Gruppo di Stati contro la Corruzione, nonché organo di controllo contro la corruzione del Consiglio d'Europa, con sede a Strasburgo. Istituito nel 1999 con un accordo di 17 Stati membri del Consiglio d'Europa, conta attualmente 49 membri, anche Stati non europei come gli Stati Uniti.

[3] Avente ad oggetto «*Ratifica ed esecuzione dei seguenti Atti internazionali elaborati in base all'art. K. 3 del Trattato sull'Unione europea: Convenzione sulla tutela degli interessi finanziari delle Comunità europee, fatta a Bruxelles il 26 luglio 1995, del suo primo Protocollo fatto a Dublino il 27 settembre 1996, del Protocollo concernente l'interpretazione in via pregiudiziale, da parte della Corte di Giustizia delle Comunità europee, di detta Convenzione, con annessa dichiarazione, fatto a Bruxelles il 29 novembre 1996, nonché della Convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione europea, fatta a Bruxelles il 26 maggio 1997 e della Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali, con annesso, fatta a Parigi il 17 dicembre 1997. Delega al Governo per la disciplina della responsabilità amministrativa delle persone giuridiche e degli enti privi di personalità giuridica».*

prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300", ha introdotto - per la prima volta nell'ordinamento italiano - la responsabilità degli enti.

Tale responsabilità, sebbene formalmente denominata "amministrativa", è in realtà – a tutti gli effetti – assimilabile ad una responsabilità "*penale"*.

La riprova testuale è fornita dallo stesso Decreto 231, interamente strutturato su principi, nozioni e disciplina, di diritto penale e diritto processuale penale: i *reati presupposti* richiamati dagli articoli 24 e ss.; la nozione di "*commissione del reato*" (art. 5); l'applicabilità all'ente dell'*amnistia* (art. 8); l'applicazione delle disposizioni del codice di procedura penale (art. 34); l'estensione all'ente delle disposizioni processuali relative all'imputato (art. 35); la valutazione della responsabilità dell'ente nell'ambito di un processo penale e da parte di un Giudice Penale (art. 36); l'improcedibilità per le stesse cause di improcedibilità dell'azione penale (art. 37); l'applicazione delle misure cautelari in base alle norme processuali penali (art. 45); l'annotazione dell'illecito nel registro delle notizie di reato di cui all'art. 335 c.p.p. (art. 55); la scansione degli atti e delle fasi processuali in base al codice di procedura penale (artt. 56-81); i riti alternativi strettamente penalistici come il *patteggiamento ex* art. 444 c.p.p., il *giudizio abbreviato ex* 438 c.p.p. e il *procedimento per decreto ex* art. 459 c.p.p. (artt. 62, 63 e 64); etc. etc.

La natura della responsabilità da Decreto 231 è *diretta* e va ad affiancarsi a quella, già presente nel codice di procedura penale, di *responsabilità indiretta*.

A quest'ultimo proposito, va ricordato che la *responsabilità indiretta* dell'ente è azionabile, ai sensi degli artt. 83 e ss. c.p.p. (su richiesta della persona già costituita parte civile nel processo penale o del pubblico ministero in caso di minore o infermo di mente), a seguito di un fatto di reato che abbia prodotto un danno risarcibile dal punto di vista civilistico.

La responsabilità dell'ente *si aggiunge* a quella della persona fisica che ha commesso materialmente il fatto illecito e rimane *autonoma* e *diretta*, continuando a sussistere *«anche quando: a) l'autore del reato non è stato identificatoo non è imputabile; b) il reato si estingue per una causa diversa dall'amnistia»* (art. 8).

L'obiettivo dell'ampliamento della responsabilità a carico degli enti è di creare un più efficace deterrente anti-illegalità, così contribuendo alla politica di abbattimento del rischio di commissione dei cd. *white collar crime* anche attraverso il coinvolgimento, nella punizione di taluni illeciti penali, del patrimonio degli enti e degli interessi economici dei soci.

La caratteristica dell'impianto normativo 231 è rappresentata da un'architettura normativa piuttosto complessa nella quale, unitamente all'introduzione di uno specifico sistema punitivo per gli enti, viene prevista una serie di apposite regole di prevenzione delittuosa.

La responsabilità dell'ente scatta in presenza di un fatto di reato (espressamente indicato dal Legislatore come "*reato presupposto"*), "*anche nella forma del tentativo"*, commesso a "vantaggio" o nell' "interesse" della Società, ad opera di soggetti che:

a) rivestono funzioni di rappresentanza, di amministrazione, di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale;

b) esercitano, anche di fatto, la gestione e il controllo dello stesso;

c) sono sottoposte alla direzione e alla vigilanza di uno dei soggetti indicati nel punto precedente (articolo 5 del D.Lgs. 231/2001).

L'unico limite al principio di *autonomia della responsabilità dell'ente* - che, però, si è detto rimanere ferma anche nel caso in cui l'autore del reato non è stato identificato o non sia

imputabile - è l'effettiva «presenza di un reato commesso nell'interesse o a vantaggio dell'ente medesimo » (Cass. pen., sez. V, 4 aprile 2013, n. 20060).

A dimostrazione della peculiarità del Sistema 231, è il principio che: ove l'ente abbia provveduto a strutturare un idoneo (v. in base ai canoni ed elementi essenziali previsti per legge) Modello di Organizzazione, Gestione e Controllo, «*non risponde*» (art. 6), ovvero potrà salvarsi dalla grave responsabilità derivante dalla commissione del *reato presupposto* commesso dal suo dipendente/esponente aziendale.

Parimenti, l'ente andrà esente da responsabilità se il *reato presupposto* è stato commesso dalla persona fisica nel suo esclusivo (proprio o di terzi) interesse, eludendo le misure preventive disposte del Modello Organizzativo 231.

Ne deriva che il Sistema 231 prevede una convergenza di responsabilità, a carico sia della persona fisica che dell'ente, con la conseguenza che la commissione del "fatto illecito" - per entrambi antigiuridico - finisce per essere assoggettato ad una duplice sanzione:

- di natura strettamente personale, a carico della persona fisica;
- di natura amministrativa, a carico dell'ente.

Entrambe le imputazioni/incolpazione e le responsabilità – dell'ente e della persona fisica che ha commesso uno dei "*reati presupposti*" dagli art. 24 e ss. del D.Lgs. 231/2001 – saranno giudicate all'interno dello stesso processo penale.

Alle predette, diverse e convergenti, responsabilità - l'amministrativa in capo all'ente, la penale in capo al dipendente e personale apicale - la giurisprudenza aggiunge, poi, quella strettamente personale dell'amministratore colpevole di avere omesso di adottare un *Modello di Organizzazione, Gestione e Controllo*-attuale, idoneo ed efficiente[4].

Attualmente, l'idea di una legge che colpisca duramente, all'interno di uno stesso processo penale, sia gli enti che le persone fisiche che li rappresentano ed operano per essi, continua ad essere condivisa e propulsata dall'unanime orientamento europeo ed internazionale.

Valga al riguardo: la Convenzione di Merida del 2003, firmata da ben 134 Stati, entrata in vigore come risoluzione ONU il 14 dicembre 2005, ratificata in Italia con Legge 3 agosto 2009 n.116; il Protocollo d'intesa Italia - Montenegro "*in materia di contrasto agli illeciti nella P.A.*" firmato in data 16 settembre 2009; l'atto costitutivo della nuova rete europea delle agenzie anticorruzione EACN istituzionalizzata a livello di Unione Europea; il Nuovo Sistema Anticorruzione italiano *ex* Legge 190/2012 e provvedimenti attuativi conseguenti, costantemente al vaglio degli organismi internazionali[5]; la costante ed unanime giurisprudenza di merito e di legittimità.

La responsabilità da D.Lgs. 231/2001 si considera automaticamente provata in tutti i casi di:

- "*assenza di modelli organizzativi idonei a prevenire reati della specie di quelli accertati*" (Tribunale Milano, 28 aprile 2008);

[4] In questi termini: Tribunale Milano, Sez. VIII, 13 febbraio 2008, n. 1774

[5] V., da ultimo, la valutazione della legislazione anticorruzione italiana da parte della Commissione Europea al Consiglio e al Parlamento Europeo, pubblicata in data 3 febbraio 2014 come Relazione dell'Unione sulla lotta alla corruzione in Italia.

- presenza di modelli "*che si limitino a prevedere generico Codice Etico che dovrebbe ispirare la condotta dei funzionari della società"* (Tribunale Milano, 27 aprile 2004, in *Riv. dottori comm.* 2004, 904);
- difettosa costruzione di un modello di organizzazione che "*non preveda strumenti idonei a identificare le aree di rischio nell'attività della società e a individuare gli elementi sintomatici della commissione di illeciti"* (Tribunale Milano, 28 ottobre 2004, Siemens AG c.);
- *inidoneità strutturale del Modello o carenza di uno dei suoi elementi essenziali* (Trib. Vicenza, 19 marzo 2021, n. 2177 c/Banca Popolare di Vicenza.)

Sarà solo la positiva dimostrazione di avere adottato un Modello di Organizzazione, Gestione e Controllo efficace e a idonea azione preventiva - idoneità eventualmente verificabile attraverso un supporto giudiziario di natura peritale (Tribunale Roma, 22 novembre 2002, Soc. Fin. S.p.a., in Foro it. 2004, II, 318) - a condurre ad una "dichiarazione di non punibilità ex art. 6" (v., tra le prime decisioni in tal senso, G.I.P. Trib. Milano 17 novembre 2009, Impregilo).

Il "*non rispondere*" se si "*prova che …*", è quella che viene sinteticamente definita "*efficacia esimente del Modello di Organizzazione, Gestione e Controllo*".

Si tratta di un principio giuridico importante in base al quale: la "*colpa da mancata organizzazione*", contestata all'ente nella cui struttura sia stato commesso un reato di quello previsti dal D.Lgs 231/2001, potrà essere superata solo con la positiva dimostrazione di una "*non colpa*", ovvero attraverso la prova di avere predisposto, prima che il reato fosse commesso, un'adeguata organizzazione aziendale idonea a controllare, prevedere e prevenire, possibili condotte illecite intra-aziendali.

Ciò comporta la necessità di una "inattaccabile" *prova di diligenza aziendale*; con la conseguenza che la Società non potrà limitarsi a sostenere che è stato adottato un Modello di Organizzazione '231 (eventualmente anche solo di mera "facciata"…), ma dovrà analiticamente dimostrare che l'ente ha attivato un reale ed efficiente meccanismo di organizzazione e di controllo di tutte le possibili condotte illecite perpetrabili all'interno di uno dei tanti gangli della propria attività imprenditoriale.

Solo tale prova potrà consentire di "difendersi" assumendo che il reato è stato commesso non a causa di una carenza di organizzazione ma in conseguenza di una elusione fraudolenta del Modello di Organizzazione, Gestione e Controllo (art. 6, co.1, lett. c) del D.Lgs. 231/2001).

Di fatto, è la stessa filosofia e politica legislativa "di tipo premiale" portata avanti dal D.Lgs. 3 agosto 2009 n. 106 (*Disposizioni integrative e correttive* al D.Lgs. 9 aprile 2008 n. 81 in materia di *tutela della salute e della sicurezza nei luoghi di lavoro*), attraverso l'introduzione del comma 3 nell'art. 16 del D.Lgs. 81/2008[6].

Proprio in materia di *sicurezza sui luoghi di lavoro*, del resto, il nesso logico con i Modelli di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 è immediato e diretto, atteso che tra i reati compresi nel predetto provvedimento legislativo vi è anche quello presupposto dall'art. 25 septies, "*Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*".

[6] Art. 16, comma 3:.«*La delega di funzioni non esclude l'obbligo di vigilanza in capo al datore di lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite. L'obbligo di cui al primo periodo si intende assolto in caso di adozione ed efficace attuazione del modello di verifica e controllo di cui all'articolo 30, comma 4*»

1.2. I Reati presupposti

La responsabilità amministrativa dell'ente scatta in caso di commissione di un *reato presupposto*, ovvero di uno dei reati richiamati dal DLgs. 231/2001 nel Capo I, Sez. III, dello stesso Decreto.

Tali fattispecie delittuose - oggetto di plurimi interventi legislativi di natura integrativa e/o correttiva[7] - sono quelle espressamente indicate agli artt. 24, 24-*bis*, 24-*ter,* 25, 25-*bis*, 25 *bis.*1, 25 ter, 25-*quarter*, 25-*quarter*.1, 25-*quinquies*, 25-*sexies*, 25-*septies*, 25-*octies*, 25-*novies*, 25-*decies*, 25-*undecies*, 25-*duodecies, 25-terdecies,* 25-*quaterdecies,* 25 *quinquiesdecies, 25 sexiesdecies, 25 octies.1, 25 octies.1,* 25-*septiesdecies*, 25-*duodevicies.*

Sul piano strutturale, ognuna delle succitate norme rinvia ad un gruppo, sia omogeneo che eterogeneo, di "reati presupposti".

L'esatta individuazione dei *"reati presupposti"* - quali fattispecie normative espressamente richiamate dal D.Lgs. 231/2001 - è fondamentale giacché saranno soltanto questi, e non altri, a potere giuridicamente legittimare l'affermazione di una "responsabilità amministrativa" *ex* D.Lgs. 231/2001.

Anche la Suprema Corte di Cassazione è del tutto univoca sul punto: *«qualora il reato commesso nell'interesse o a vantaggio di un ente non rientri tra quelli che fondano la responsabilità ex d.lg. n. 231 del 2001 di quest'ultimo, ma la relativa fattispecie ne contenga o assorba altra che invece è inserita nei cataloghi dei reati presupposto della stessa, non è possibile procedere alla scomposizione del reato complesso o di quello assorbente al fine di configurare la responsabilità della persona giuridica. (Fattispecie relativa all'annullamento del provvedimento di sequestro preventivo a fini di confisca del profitto del reato di truffa aggravata ai danni dello Stato contestato ad una società in seguito alla sua enucleazione da quello di frode fiscale contestato invece agli amministratori della medesima)»* (Cass. Pen., Sez. II, 29 settembre 2009, n. 41488, che ha annulla senza rinvio, Trib. Lib. Varese, 12 febbraio 2009).

Per comprendere appieno il significato giuridico di "*Reato Presupposto*", va innanzitutto chiarito che il D.Lgs. 231/2001 non è una legge introduttiva di nuove fattispecie di reato.

---

7 V: la L. 48/2008 che ha introdotto l'art. 24 bis; la L. 94/2009, che ha introdotto l'art. 24 ter; la L. 99/2009 che ha inserito gli artt. 25 bis.1, 25 novies e 25 decies; il D.Lgs. 61/2002 e la L. 262/2005 che hanno apportato modifiche all'art. 25 ter; la L. 7/2003 che ha inserito l'art. 25 quater; la L. 7/2006 che ha inserito l'art. 25 quater.1; le L.ggi 228/2003 e 38/2006 che hanno inserito l'art. 26 sexies; la L. 123/2007 e il D.Lgs. 81/2008 che hanno apportato modifiche all'art. 25 septies; il D.Lgs. 231/2007 che ha inserito l'art. 25 octies; la L. 99/2009 che ha inserito l'art. 25 novies; la L. 116/2009 che ha inserito l'art. 25 novies/decies; il Dlgs. 121/2001 che ha inserito l'art. 25 undecies; il DLgs. 109/2012, che ha inserito l'art. 25 duodecies; la L. 190/2012 che ha inserito gli artt. 319-quater c.p. e 2635 c.c. negli articoli 25 e 25-ter; la L. 186/2014 che ha inserito nell'art. 25 octies l'art. 648 ter.1 c.p.; il D.Lgs. 39/2014 che ha inserito l'art. 609-undecies c.p. nell'art. 25-quinquies; la L. 68/2015 che ha introdotto i delitti ambientali ex artt. 452-bis e ss. c.p.; la L. 69/2015, che ha modificato i reati di cui agli artt. 317, 318, 319, 319-ter, 319-quater (presupposti dall'art. 25), 416-bis c.p. (presupposto dall'art. 24-ter) e 2621 - 2622 c.c. (presupposti dall'art. 25-ter); la L. 199/2016 che ha inserito nell'art. 25 quinquies il neo art. 603 bis c.p.; il D.Lgs. 38/2017 che ha introdotto l'art. 2635 bis c.c.; la Legge 20 novembre 2017 n. 277 che ha introdotto il reato di cui all'art. 25 terdecies; il D.Lgs. 21/2018 che ha inserito, tra i reati ambientali, l'art. 452 quaterdecies c.p.; la Legge 3/2019 che ha inserito il nuovo art. 346 bis c.p.; la L. 3.5.2019 che ha inserito l'art. 25 quaterdecies; l'art. 39 del D.L. 124/2019 conv. in L. 157/2019 che ha introdotto l'art. 25 quinquiesdecies (*Reati Tributari*); il D.lgs. 75/2020 che ha esteso il raggio azione dei reati presupposti dall'art. 25 quinquiesdecies (*Reati Tributari*) ed introdotto i *reati di contrabbando* ex art. 25 sexiesdecies; il D.Lgs. 184/2021, che ha introdotto gli artt. 493 ter e 493 quater c.p.; la L. 22/2022 che introdotto gli artt. 25 septiesdecies e 25 duodevicies; il DL 105/2023 conv. in L. 137/2023, che ha introdotto nell'art. 24 i reati ex artt. 353 e 353 bis c.p., e nell'art. 25 octies l'art. 512 bis c.p.

Il Decreto in oggetto si limita, infatti, ad individuare quegli specifici reati - già presenti nel sistema - che, ritenuti a rischio di verificazione all'interno di un Ente, si richiede siano previsti ed evitati attraverso un idoneo Modello di Organizzazione ex art. 6, co. 1, lett. a), nel Decreto 231; dal che consegue che la determinazione esterna della prescrizione – ovvero quella da cui scaturisce la sanzione fissata dal Decreto 231 (*"sarai punito con la sanzione pecuniaria XX se commetti il reato YY"*) – è appunto rappresentata dal reato richiamato, che per tale ragione si chiama *reato presupposto*.

In altri termini, i "*reati presupposti":*

- non sono stati introdotti dal D.Lgs. 231/2001;
- hanno una loro pregressa vita ed esistenza autonoma;
- sono semplicemente *richiamati* dal D.Lsg. 231/2001 (analogamente a quanto accade nelle "norme penali in bianco", in cui la sanzione è determinata in via immediata e la prescrizione, ovvero lo specifico comportamento vietato, è invece indicata in via mediata e *ab externo*).

Importante precisazione: spesso i *reati presupposti* vengono richiamati dal Decreto 231 solo in via parziale, nel senso che la loro rilevanza ai fini della responsabilità amministrativa dell'ente è limitata (pena la violazione del principio di legalità) al solo caso in cui sia stata commessa quella specifica porzione di reato richiamato dal Legislatore.

Il Decreto 231 riporta parecchi casi di richiamo/rilevanza parziale, da evidenziare con precisione nella mappatura dei reati di ogni Modello di Organizzazione, Gestione e Controllo 231.

Questo l'elenco dei reati presupposti:

❒ Art. 24 (*Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture*):

✓ Malversazione a danno dello Stato (art. 316-*bis* c.p.);
✓ Indebita percezione di erogazioni a danno dello Stato (art. 316-*ter* c.p.)*;*
✓ Turbata libertà degli incanti (art. 353 c.p.);
✓ Turbata libertà del procedimento di scelta del contraente (art. 353 bis c.p.);
✓ Frode nelle pubbliche forniture (art. 356 c.p.);
✓ Truffa in danno dello Stato (art. 640, co. 2 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*).

❒ Art. 24-*bis* (*Delitti informatici e trattamento illecito dati*):

✓ Falsità in un documento informatico pubblico o 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 programmi diretti a danneggiare o interrompere un sistema informatico (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 od 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.).

❒ Art. 24-*ter* (*Delitti di criminalità organizzata*):
✓ Associazione per delinquere (art. 416 c.p.);
✓ Associazioni di tipo mafioso (art. 416-*bis* c.p.);
✓ Scambio elettorale politico mafioso (art. 416-*ter* c.p.);
✓ Sequestro di persona a scopo di estorsione (art. 630 c.p.);
✓ Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9.10.1990 n. 309).

❒ Art. 25 (*Concussione e corruzione*):
✓ Peculato (art. 314, I comma) [reato rilevante *ex* Decreto 231 se *"il fatto offende gli interessi finanziari dell'Unione europea"*]
✓ Peculato mediante profitto dell'errore altrui (art. 316) [reato rilevante *ex* Decreto 231 se *"il fatto offende gli interessi finanziari dell'Unione europea*"];
✓ Concussione (art. 317 c.p.);
✓ Corruzione per un atto d'ufficio (art. 318 c.p.);
✓ Corruzione per un atto contrario ai doveri di ufficio (art. 319);
✓ 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);
✓ Istigazione alla corruzione (art. 322 c.p.);
✓ Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.);
✓ Abuso di ufficio (art. 323 c.p.) [reato rilevante *ex* Decreto 231 *"il fatto offende gli interessi finanziari dell'Unione europea*"];
✓ Traffico di influenze illecite (art. 346-*bis* c.p.).

❒ Art. 25-*bis* (*Falsità in monete, in carte di pubblico credito e in valori di bollo*):
✓ 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 bollati 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.).

❒ Art. 25-*bis* 1. (*Delitti contro l'industria e il commercio*):
✓ Turbata libertà dell'industria o del commercio (art. 513 c.p.);
✓ Illecita concorrenza con minaccia o violenza (art. 513-*bis* c.p.);
✓ Frodi contro le industrie nazionali (art. 514 c.p.);
✓ Frode nell'esercizio del commercio (art. 515 c.p.);
✓ Vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.);
✓ Vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
✓ Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-*ter* c.p.);
✓ Contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-*quater* c.p.).

❒ Art. 25-*ter* (*Reati societari*):
✓ False comunicazioni sociali (art. 2621 c.c.);
✓ False comunicazioni sociali delle società quotate (art. 2622 c.c.);
✓ Impedito controllo (art. 2625, comma 2, c.c.);
✓ Indebita restituzione dei conferimenti (art. 2626 c.c.);
✓ Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);
✓ Illecite operazioni sulle azioni o quote sociali o della società controllata (art. 2628 c.c.);
✓ Operazioni in pregiudizio dei creditori (art. 2629 c.c.);
✓ Omessa comunicazione del conflitto di 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.);
✓ Corruzione tra privati (art. 2635 c.c.);
✓ Istigazione alla corruzione tra privati (art. 2635-*bis* 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).

❒ Art. 25-*quater* (*Delitti con finalità di terrorismo o di eversione dell'ordine democratico*):

✓ Sono idonei a rientrare nel raggio di applicazione di tale norma tutti i delitti *"aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal Codice Penale e dalle leggi speciali*", quale categoria normativa aperta che, oltre alle disposizioni di legge previste nel Libro II, Titolo I, Capo I, II, III, IV e V, del Codice Penale – articoli dal 241 al 307 c.p. – si ritiene altresì comprensiva della relativa legislazione speciale.

❒ Art. 25-*quater* 1. (*Pratiche di mutilazione degli organi genitali femminili*):
✓ Art. 583-*bis* c.p.

❒ Art. 25-*quinquies* (*Delitti contro la personalità individuale*):
✓ 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.);
✓ Intermediazione illecita e sfruttamento del lavoro (art. 603-*bis* c.p.);
✓ Adescamento di minorenni (art. 609-*undecies* c.p.).

❒ Art. 25-*sexies* (*Abusi di mercato*):
I reati specificamente richiamati dall'art. 25-*sexies* sono quelli di abuso di informazioni privilegiate e di manipolazione del mercato previsti dal T.U. di cui al Decreto Legislativo 24 febbraio 1998 n. 58:
✓ Abuso di informazioni privilegiate (art. 184 D.Lgs. 1998 n. 58);
✓ Manipolazione del mercato (art. 185 D.Lgs. 1998 n. 58).

❒ Art. 25-*septies* (*Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro*).
Entrambi i richiamati *reati presupposti* presuppongono la violazione della normativa sulla sicurezza sul lavoro di cui ai D.Lgs. 9 aprile 2008 n. 81/D.Lgs. 3 agosto 2009 n. 106, e sono i seguenti:
✓ Omicidio colposo (art. 589 c.p.);
✓ Lesioni colpose (art. 590 c.p.).

❒ Art. 25-*octies* (*Ricettazione, Riciclaggio e impiego del denaro, beni o utilità di provenienza illecita*):
✓ Ricettazione (art. 648-c.p.);
✓ Riciclaggio (art. 648-*bis* c.p.);
✓ Impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.);
✓ Autoriciclaggio (art. 648-*ter* 1. c.p.).

❒ Art. 25-*octies.1* (*Delitti in materia di strumenti di pagamento diversi dai contanti*):
✓ Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-*ter* c.p.);
✓ Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-*quater* c.p.);
✓ Trasferimento fraudolento di valori (art. 512 bis c.p.);
✓ Frode informatica (art. 640-*ter* c.p.) [reato rilevante *ex* Decreto 231 se *"se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale"*]

❒ Art. 25-*novies* D.Lgs. 231/2001 (*Delitti in materia di violazione dei diritti di autore*):
✓ I reati in oggetto sono quelli previsti agli artt. 171, 171-*bis*, 171-*ter*, 174-*quinquies*, 171-*septies* e 171-*octies* della Legge 22 aprile 1941 n. 633 come modificata dalla L. 248/2000.

❒ Art. 25-*decies* (*Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria*):
✓ Art. 377-*bis* c.p.

❒ Art. 25-*undecies* (*Reati Ambientali*):
✓ Inquinamento ambientale (art. 452-*bis* c.p.);
✓ Disastro ambientale (art. 452-*quater* c.p.);
✓ Delitti colposi contro l'ambiente (art. 452-*quinquies* c.p.);
✓ Traffico e abbandono di materiale ad alta radioattività (art. 452-*sexies* c.p.);
✓ Circostanze aggravanti (art. 452-*octies* c.p.)
✓ 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.);
✓ Reati in materia ambientale *ex* D.Lgs. 3 aprile 2006 n. 152, meglio conosciuto come Codice Ambiente (art. 137 commi 1, 2, 3, 5, 6 e 13; 256 commi 1, 3, 5, e 6; 257 commi 1 e 2; 258 comma 4; 259; 260; 260-*bis* commi 6, 7 e 8; 279 comma 5);
✓ Reati relativi all'applicazione in Italia della convenzione sul commercio internazionale delle specie animali e vegetali in via di estinzione *ex* Legge 7 febbraio 1992 n. 150 (art. 1 commi 1 e 2; art. 2 commi 1 e 2; art. 6 commi 1 e 4);
✓ Reati del codice penale richiamati dall'art. 3-*bis* della citata Legge 150/1992 n. 150 (artt. 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 491-*bis*, 492, 493)*;*
✓ Reati previsti dalla Legge 28 dicembre 1993, n. 549 (*Misure a tutela dell'ozono stratosferico e dell'ambiente)* – (art. 3 *"Cessazione e riduzione dell'impiego delle sostanze lesive"*);
✓ Reati previsti dal D.Lgs. 6 novembre 2007 n. 202 (15) – artt. 8 (*inquinamento doloso*) e 9 (*inquinamento colposo*).

❒ Art. 25-*duodecies* (*Impiego di cittadini di paesi terzi il cui soggiorno è irregolare*):
✓ Artt. 12, comma 3, 3-*bis*, 3-*ter*, 5 e 22, comma 12-*bis*, del D.Lgs. 25 luglio 1998 n. 286.

❒ Art. 25-*terdecies* (*Razzismo e xenofobia*):

✓ Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa (art. 604-*bis* c.p.).

❒ Art. 25-*quaterdecies* (*Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati*):

✓ Frode in competizioni sportive (art. 1, Legge 13 dicembre 1989, n. 401;

✓ Esercizio abusivo di attività di giuoco o di scommessa (art. 4, Legge 13 dicembre cit).

❒ Art. 25-*quinquiesdecies* (*Reati tributari*):

I reati presupposti dal predetto articolo sono quelli previsti dal D.Lgs. 10 marzo 2000 n. 74, aggiornato al D.L. 124/2019, per come modificato in sede di conversione dalla Legge 157/2019:

✓ Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2);

✓ Dichiarazione fraudolenta mediante altri artifici (art. 3);

✓ Emissione di fatture o altri documenti per operazioni inesistenti (art. 8);

✓ Occultamento o distruzione di documenti contabili (art. 10);

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

Ai succitati, si aggiungono i seguenti ed ulteriori reati tributari, rilevanti però ai fini del D.Lgs. 231/2001 solo se «commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro»:

✓ Dichiarazione infedele (art. 4);

✓ Omessa dichiarazione (art. 5);

✓ Indebita compensazione (art. 10-quater).

❒ Art. 25-*sexiesdecies* (*Reati di contrabbando*):

✓ *Reati di contrabbando ex* D.P.R. 23 gennaio 1973 n. 43 (introdotti dall'art. 5 del D.Lgs. 14 luglio 2020, n. 75.

❒ Art. 25-*septiesdecies* (*Delitti contro il patrimonio culturale*):

✓ Furto di beni culturali (art. 518-*bis* c.p.);

✓ Appropriazione indebita di beni culturali (art. 518-*ter* c.p.);

✓ Ricettazione di beni culturali (art. 518-*quater* c.p.);

✓ Falsificazione in scrittura privata relativa a beni culturali (art. 518-*octies* c.p.);

✓ Violazioni in materia di alienazione di beni culturali (art. 518-*novies* c.p.);

✓ Importazione illecita di beni culturali (art. 518-*decies* c.p.);

✓ Uscita o esportazione illecite di beni culturali (art. 518 -*undecies* c.p.);

✓ Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-*duodecies* c.p.);

✓ Contraffazione di opere d'arte (art. 518 -*quaterdecies* c.p.).

❒ *Art. 25-duodevicies (Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali paesaggistici):*

✓ Riciclaggio di beni culturali (art. 518-*sexies* c.p.);

✓ Devastazione e saccheggio di beni culturali e paesaggistici (art. 518- *terdecies* c.p.)

Il dettaglio dei contenuti di tutti i suddetti Reati Presupposti è riportato nell'Allegato 4 (*Appendice Normativa)*.

Discorso a parte - nel senso che non si tratta di reati formalmente *presupposti* dal D.Lgs. 231/2001, ma che tuttavia vengono richiamati, in direzione inversa, da altra legge di richiamo allo stesso Decreto 231 - è quello che riguarda i reati collegati al *"crimine organizzato transnazionale"* di cui alla Legge 16 marzo 2006, n. 146 (*Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001*).

Con tale provvedimento legislativo, è stata innanzitutto introdotta - all'art. 3 - la definizione di "*reato transazionale*": «*Ai fini della presente legge si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché: sia commesso in più di uno Stato; ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato*».

Inoltre, all'art. 10 della stessa Legge 146/2006, è stata disposta l'applicazione della responsabilità amministrativa degli enti di cui al D.Lgs. 231/2001 per i seguenti reati connotati dal requisito della "transnazionalità" di cui al succitato art. 3:

- *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 decreto del Presidente della Repubblica 23 gennaio 1973, n. 43);*
- *associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 del testo unico di cui al decreto del Presidente della Repubblica 9 ottobre 1990, n. 309);*
- *disposizioni contro le immigrazioni clandestine (art. 12, commi 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.).*

Tra i succitati reati, alcuni sono già inseriti nel novero dei reati presupposti dal D.Lgs. 231/2001 quali reati "nazionali", altri sono esclusi e dunque rimangono rilevanti ai fini della responsabilità ex D.Lgs. 231/2001 *solo* se commessi con modalità "transazionali".

A) Sono *reati presupposti,* sia nella veste *transazionale* che in quella *nazionale* (ed infatti sono formalmente richiamati dal D.Lgs. 231/2001), i seguenti delitti:

- art. 377 bis, quale reato presupposto dall'art. 25 decies;
- articoli 416, 416 bis c.p. e 74 D.P.R. 309/1990, quali reati presupposti dall'art. 24 ter;

B) Sono *reati presupposti,* ove siano commessi con modalità cd. "transazionale" *ex* art. 3 della Legge 146/2006 (ed infatti non sono formalmente richiamati dal D.Lgs. 231/2001), i seguenti delitti:

- art. 291 quater di cui al D.P.R. 23 gennaio 1973, n. 43;
- art. 12 commi 3, 3 bis, 3 ter e 5, del T.U. di cui al D.Lgs. 25 luglio 1998, n. 286;
- art. 378 c.p..

1.3. Il Sistema Sanzionatorio

La peculiarità del sistema sanzionatorio 231 è di essere costituito da norme punitive scaturenti da articoli in cui:

- la *prescrizione* è rappresentata dai *reati presupposti* richiamati (es., l'art. 24 richiama quali reati presupposti gli artt. 316-*bis*, 316-*ter*, 640 comma 2, n. 1, 640-*bis* e 640-*ter*);
- la *sanzione* è, invece, fissata direttamente dal Legislatore 231 modificando soltanto la natura della pena, da "reclusione" e/o "multa" tipica del codice penale a "sanzione pecuniaria per quote" (es., l'art. 24 dispone: «in relazione alla commissione dei delitti di cui agli articoli 316-*bis*, 316-*ter*, 640 comma 2 n. 1, 640-*bis* e 640-*ter* c.p. se commessi in danno dello Stato o di altro ente pubblico, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote»).

Il sistema del *sanzionamento per quote* è regolato dall'art. 10: «1. Per l'illecito amministrativo dipendente da reato si applica sempre la sanzione pecuniaria. 2. La sanzione pecuniaria viene applicata per quote in un numero non inferiore a cento né superiore a mille. 3. L'importo di una quota va da un minimo di lire cinquecentomila ad un massimo di lire tre milioni».

La *concreta commisurazione della sanzione pecuniaria ex* Decreto 231 viene disposta dal Giudice Penale in base ai criteri stabiliti dall'art. 11: «... gravità del fatto... grado della responsabilità dell'ente ... attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti ... condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione».

Gli enti nei quali viene commesso uno dei *reati presupposti* indicati dal Legislatore senza che sia stato approntato un adeguato sistema di gestione del rischio, attraverso la predisposizione di un MOGC 231, vanno incontro alle seguenti *sanzioni amministrative,* fissate dall'art. 9 del Decreto 231:

a) *sanzione pecuniaria* (determinata per "quota", in base alle diverse e singole fattispecie richiamate dagli artt. 24-25-*sexiesdecies*);
b) *sanzioni interdittive*;
c) *confisca*;
d) *pubblicazione della sentenza*.

Le *sanzioni interdittive* di cui al superiore punto *sub* b) – previste, in via generale, dagli artt. 9, 13 e 14, e in via specifica dagli artt. 24-25-*sexiesdecies,* a seconda dei diversi *reati presupposti* richiamati – sono:

- ✓ l'interdizione dall'esercizio dell'attività;
- ✓ la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

✓ il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;

✓ l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi;

✓ il divieto di pubblicizzare beni o servizi.

A differenza delle pene accessorie del codice penale, le *sanzioni interdittive* del Decreto 231 sono contraddistinte da una certa discrezionalità.

L'art. 13 dispone infatti che le *sanzioni interdittive* si applicano quando ricorra almeno una delle seguenti condizioni:

- un profitto di rilevante entità, o la commissione del reato da soggetti in posizione apicale ovvero sottoposti all'altrui direzione e il reato è stato agevolato da gravi carenze organizzative, o una reiterazione degli illeciti;
- hanno una durata non inferiore a tre mesi e non superiore a due anni;
- non si applicano nei casi previsti dall'art. 12, comma 1, ovvero se «a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; b) il danno patrimoniale cagionato è di particolare tenuità».

Anche l'art. 14 (*Criteri di scelta delle sanzioni interdittive*) conferisce al Giudice ampi poteri nella determinazione del tipo e della durata delle sanzioni interdittive, in base ai criteri stabiliti dall'art. 11 per la commisurazione della sanzione pecuniaria e tenendo anche «conto dell'idoneità delle singole sanzioni a prevenire illeciti del tipo di quello commesso».

Pertanto:

a) «il divieto di contrattare con la pubblica amministrazione può anche essere limitato a determinati tipi di contratto o a determinate amministrazioni» (art. 14, secondo comma);

b) «se necessario, le sanzioni interdittive possono essere applicate congiuntamente » (art. 14 terzo comma);

c) «l'interdizione dall'esercizio dell'attività si applica soltanto quando l'irrogazione di altre sanzioni interdittive risulta inadeguata» (art. 14 quarto comma).

Sempre nell'ambito delle *sanzioni interdittive*, riveste una particolare importanza l'art. 15 (*Commissario giudiziale*), in base al quale «se sussistono i presupposti per l'applicazione di una sanzione interdittiva che determina l'interruzione dell'attività dell'ente, il giudice, in luogo dell'applicazione della sanzione, dispone la prosecuzione dell'attività dell'ente da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata».

L'applicazione della succitata norma è, però, condizionata al fatto che: «a) l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività; b) l'interruzione dell'attività dell'ente può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione».

In tale evenienza, sarà il Commissario a proseguire l'attività e a curare l'efficace adozione ed attuazione dei Modelli di Organizzazione

Non avverrà nulla di tutto questo ove la *sanzione interdittiva* sia applicata, in via definitiva, in ragione delle situazioni di gravi illiceità, presenti o passate, riscontrate dal Giudice (art. 16).

La severità del sistema punitivo raggiunge i suoi massimi livelli laddove, prima ancora che sia emessa una sentenza definitiva, scatti:

a) l'irrogazione delle misure cautelari reali di cui all'art. 45 D.Lgs. 231/2001: *"Quando sussistono gravi indizi per ritenere la sussistenza della responsabilità dell'ente per un illecito amministrativo dipendente da reato e vi sono fondati e specifici elementi che fanno ritenere concreto il pericolo che vengano commessi illeciti della stessa indole di quello per cui si procede, il pubblico ministero può richiedere l'applicazione quale misura cautelare di una delle sanzioni interdittive previste dall'articolo 9, comma 2, presentando al giudice gli elementi su cui la richiesta si fonda …"*;

b) l'imposizione, *ex* art. 53 D.Lgs. 231/2001, di un sequestro funzionale alla futura confisca: *"Il giudice può disporre il sequestro delle cose di cui è consentita la confisca a norma dell'articolo 19. Si osservano le disposizioni di cui agli articoli 321, commi 3, 3-bis e 3-ter, 322, 322-bis e 323 del codice di procedura penale, in quanto applicabili*";

c) "*l'applicazione congiunta di una misura cautelare interdittiva e di una misura cautelare reale"* (Cassazione penale, Sez. Un., 27 marzo 2008, n. 26654, Soc. F. e altro).

In un quadro di questo tipo: ove nell'ambito di una determinata attività societaria venga commesso uno solo tra gli svariati *reati presupposti* del D.Lgs. 231/2001 – uno tra le centinaia di delitti richiamati dagli artt. 24 e ss. della stessa legge - l'unica difesa che potrà consentire di scongiurare la mannaia delle succitate sanzioni in capo all'ente è l'avere approntato, prima della verificazione del fatto, "*modelli di gestione e di organizzazione idonei a prevenire reati della stessa specie di quello verificatosi*".

2. MODELLI 231 E RELATIVE COMPONENTI ESSENZIALI

2.1 Linee guida e best practice

L'art. 6 del Decreto 231 riconosce all'ente la possibilità di andare esente da responsabilità amministrativa se dimostra di avere adottato un Modello di Organizzazione, Gestione e Controllo (anche detto Modello, Modello 231 o MOGC), idoneo a prevedere, prevenire, evitare o quanto meno ridurre, il rischio di verificazione dei *reati presupposti*.

I requisiti di base di un Modello, richiesti dal predetto art. 6, sono:

- assegnazione del «*compito di vigilare sul funzionamento e l'osservanza dei modelli, di curare il loro aggiornamento ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo*»;
- individuazione delle «*attività nel cui ambito possono essere commessi reati*»;
- previsione di «*specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire*»;
- individuazione delle «*modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati*»;
- previsione di «*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*»;
- introduzione di «*un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello*»;
- inserimento della *tutela da whistlebowing* (*infra*).

Dal punto di vista contenutistico, poiché il D.Lgs. 231/2001 non offre elementi specifici al di là dei succitati elementi essenziali/inderogabili ex art. 6, la prassi e l'esperienza sviluppatesi nel corso del ventennio successivo alla emanazione del D.Lgs. 231/2001 hanno evidenziato che:

A) data la varietà di strutture organizzative di volta in volta adottate in funzione, sia delle dimensioni sia del diverso mercato geografico o economico in cui essi operano, non si possono fornire riferimenti puntuali in tema di modelli organizzativi e funzionali, se non sul piano metodologico;

B) le disposizioni del D.Lgs. 231/2001 non prevedono modelli di organizzazione e di gestione schematizzabili a *priori*, con la coseguenza che il modello deve risultare coerente con la natura e le dimensioni della struttura organizzativa, nonché con le peculiarità dell'attività svolta e l'ente ha il dovere di predisporre i modelli organizzativi in piena autonomia e secondo un approccio cd. "sartoriale", potendo semmai – opportunamente – seguire e rispettare le più accreditate Linee Guida o Studi in materia.

Le principali Linee Guida in materia sono rappresentate da

- *Linee Guida di Confindustria* (approvate il 7 marzo 2002, aggiornate nel mese marzo 2014 e, da ultimo, nel mese di giugno 2021), le quali, pur a distanza di 20 anni dalla promulgazione del D.Lgs. 231/2001, confermano la necessità di evitare approcci e casistiche decontestualizzate rispetto a quelle direttamente applicabili alle singole realtà operativ»;
- *Circolare n. 83607 emessa dal Comando Generale della Guardia di Finanza* (III Reparto Operazioni – Ufficio Tutela Economia e Sicurezza) del 19 marzo 2012, anch'essa in piena sintonia con le Linee Guida di Confindustria nell'annotare che: «le disposizioni del D.Lgs.

231/2001 non prevedono modelli di organizzazione e di gestione schematizzabili *a priori*... il modello deve risultare coerente con la natura e le dimensioni della struttura organizzativa, nonché con le peculiarità dell'attività svolta ... l'ente può, quindi, predisporre i modelli organizzativi in piena autonomia, oppure utilizzare i modelli redatti dalle associazioni di categoria a condizione però che venga specificatamente pensato e progettato, secondo un approccio "sartoriale", per quel determinato ente nel quale dovrà trovare applicazione»;

- *Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del D.Lgs. 8 giugno 2001, n. 231,* a cura del Gruppo di Lavoro Multidisciplinare costituito da rappresentanti del Consiglio Nazionale Dottori Commercialisti ed Esperti contabili, Associazione Bancaria Italiana, Consiglio Nazionale Forense e Confindustria, del dicembre 2018;
- *Norma ISO 31000.2018* (in italiano *UNI ISO 31000)*[8]*,* di marca internazionale, che: fornisce principi e linee guida generali per la gestione del rischio utilizzabili per qualsiasi organizzazione e struttura (pubblica o privata); non è specifica per alcuna industria o settore (né è formalmente certificabile trattandosi di Linee Guida); è stata pubblicata per la prima volta nel mondo nel novembre del 2009, aggiornata nel febbraio 2018, pubblicata in Italia il 25 novembre 2010.

Nel presente Modello 231, la Norma ISO 31000 – la cui illustrazione è contenuta nell'Allegato 3 - è stata applicata per l'analisi e la valutazione del rischio di verificazione dei reati presupposti.

Nel presente Modello 231, si ritiene altresì integralmente richiamato – anche ai fini della sua sottoposizione al raggio di vigilanza dell'Organismo di Vigilanza – il Sistema Gestionale 37001:2016 adottato dalla Società.

2.2 Raggio di azione, principi e gestione del rischio da reato presupposto

Dal punto di vista logistico, il Modello regolamenta l'intera attività dell'ente – pur se ai soli fini della prevenzione dei *reati presupposti* – in tutte le sue parti, settori ed estrinsecazioni (amministrativo, tecnico e operativo).

Dal punto di vista soggettivo, il Modello deve obbligatoriamente essere implementato e rispettato dai cd. *destinatari*, ovvero dai soggetti che operano "con" e "per" l'ente.

La soggezione dei *destinatari* al Modello è, tuttavia, diversificata a seconda che gli stessi siano "intranei" all'ente (nel senso di operare in via esclusiva e continuativa per l'ente, nei vari livelli e funzioni) o "estranei" all'ente (v. fornitori, collaboratori, consulenti e coloro che prestano la loro attività in via occasionale e non continuativa). Per quest'ultimi soggetti, il Modello e il Codice Etico e di Comportamento saranno applicabili solo parzialmente, ovvero in quelle specifiche parti che impattano con l'attività loro resa all'ente (es. i fornitori di beni saranno senz'altro soggetti alle regole sulla selezione ed ingresso all'albo fornitori; i fornitori di servizi

[8] la Norma ISO 31000 è stata redatta da ISO che: è la più importante Organizzazione internazionale per la normazione; è stata fondata nel 1947; i suoi membri sono gli Organismi Nazionali di Standardizzazione di 146 Paesi del mondo; ha il suo quartier generale a Ginevra; svolge funzioni consultive, tra i tanti, per l'UNESCO e l'ONU. Anche l'Autorità Nazionale Anticorruzione ne consiglia l'applicazione metodologica ai fini della predisposizione dei Piani Triennali Prevenzione Corruzione e Trasparenza.

dovranno obbligatoriamente attenersi ai protocolli stabiliti per l'esecuzione dello specifico servizio rifornito; tutti gli estranei dovranno attenersi alle regole comportamentali del Codice Etico).

Sul piano dei contenuti, tutti i sistemi di gestione del rischio sono basati – per via logica ed in termini generali – su alcuni principi ed azioni fondamentali:

- *Focalizzare lo specifico rischio* (es. rischio di terremoto, rischio di inquinamento batterico delle acque, rischio di cedimento di un ponte, rischio di deterioramento di un prodotto alimentare, rischio di commissione del reato di riciclaggio, e così via in una casistica numericamente ricca ricca quanto lo possono essere tutte le possibili occasioni offerte dalla realtà).
- *Capire dove tale rischio può annidarsi maggiormente*, ossia individuare le aree e le situazioni "sensibili" (nel caso, ad esempio, del rischio di avvelenamento sui luoghi di lavoro in una fabbrica di pesticidi, è certamente a maggior rischio di incolumità personale il reparto dove si miscelano gli acidi piuttosto che l'ufficio dove si emettono le fatture elettroniche, esattamente come in un cantiere è quasi geneticamente "a rischio di incidenti sul luogo di lavoro" una prestazione d'opera su una impalcatura alta dieci metri).
- *Individuare le cause predisponenti o le situazioni che possono agevolare o aumentare il rischio* (es., una possibile causa predisponente del reato di furto è diffondere indiscriminatamente la notizia di possedere nella propria abitazione priva di antifurto gioielli di alto valore; parimenti, rappresenta una possibile occasione di commissione del reato di corruzione la partecipazione ad una trattativa privata con un ente pubblico);
- *Individuare chi potrebbe maggiormente attualizzare il rischio* e chi, invece, ha l'obbligo di monitorarlo e controllarlo, ossia capire esattamente "chi fa cosa";
- *Predisporre dei conseguenziali sistemi di gestione e di controllo* – sia delle "situazioni a rischio oggettivo", sia delle "azioni a rischio soggettivo" – avendo sempre presente: da un lato, i soggetti che potrebbero concretizzare il rischio (v., commettere un *reato presupposto*); dall'altro, coloro che hanno invece il dovere e l'obbligo di controllare gli stessi soggetti (non dimenticando che, in un corretto sistema di gestione di rischio, più che un monitoraggio/controllo di tipo piramidale dovrebbe assicurarsi un controllo reciproco in chiave di circolarità).

L'ormai ventennale vita "sul campo" dei Modelli 231 ha, poi, generato la condivisione di alcuni principi generali (da personalizzare in base alla specifica realtà aziendale), ritenuti comuni alla elaborazione di tutti i Modelli 231:

✓ *Specificità*

Un Modello di Organizzazione, Gestione e Controllo 231, per essere idoneo e rivestire efficacia esimente, deve essere "ritagliato su misura dell'ente" (assolutamente inidoneo, quindi, un Modello meramente teorico e disallineato rispetto alla concreta realtà dell'ente per il quale viene predisposto).

✓ *Adeguatezza*

Un Modello può considerarsi adeguato solo quando dimostri di avere la reale capacità di prevenire i *reati presupposti* indicati dal Legislatore.

✓ *Attuabilità e condivisione*

In linea con i principi di specificità e di concretezza, i protocolli e le misure organizzative previsti nel Modello devono essere effettivi, concretamente attuabili in riferimento alla struttura dell'ente e dei suoi processi operativi, ma soprattutto condivisi da tutti gli esponenti aziendali (non è, ad esempio, condiviso un Modello "calato" dall'alto senza che sia stata correttamente programmata una azione di informazione e formazione, nei confronti di tutti i destinatari del MOGC, sulle misure preventive da applicare o sui comportamenti da tenere/evitare).

✓ *Efficienza*

Il sistema di gestione del rischio deve rispondere ad un principio di efficienza, inteso come coerenza fra le caratteristiche dell'ente e la complessità del Modello (il che, ad esempio, comporta che va tenuta in debita considerazione anche la sua sostenibilità economica, finanziaria e organizzativa).

✓ *Dinamicità*

Come tutti i sistemi di controllo interno e di gestione del rischio, il Modello e tutta la documentazione ad esso attinente devono essere oggetto di costante attività di verifica e di aggiornamento, da attuarsi attraverso un'analisi periodica e/o continuativa di efficacia ed efficienza.

✓ *Unità*

Il Modello deve essere sviluppato procedendo ad una valutazione dei rischi e dei processi sensibili che abbracci l'intera struttura dell'ente, sul presupposto che, pur nella diversità delle singole aree di rischio, l'organizzazione deve essere coinvolta nella sua interezza.

✓ *Coerenza*

L'elaborazione del Modello deve mostrare una coerenza di fondo fra tutte le sue parti, tal che le misure preventive programmate/in programmazione siano in linea con la pianificazione e le strategie dell'ente, e le decisioni del vertice amministrativo non siano in contrasto con gli indirizzi e gli obiettivi indicati nel Modello.

✓ *Neutralità*

Pur in presenza di inevitabili profili soggettivi e discrezionali di valutazione, la redazione del Modello dovrà essere basata su criteri di neutralità, al fine di non far venir meno l'imparzialità, la ragionevolezza e la verificabilità di giudizio (ne deriva, ad esempio, che i soggetti incaricati della definizione delle procedure di controllo devono avere un adeguato grado di indipendenza, soprattutto nel rilevare eventuali carenze organizzative).

✓ *Integrazione tra Modello 231 e altri sistemi aziendali di gestione e controllo*

Un corretto processo di definizione del Modello richiede la verifica preliminare degli eventuali sistemi aziendali di gestione/controllo o certificazioni già esistenti, al fine di valutarne l'effettivo funzionamento ed opportunità di integrazione con lo stesso Modello.

✓ *Trasparente gestione delle risorse finanziarie*

Tale principio è strettamente conseguente al principio di tracciabilità e replicabilità di tutte le azioni aziendali.

✓ *Formazione e diffusione*

Il processo di informazione e formazione costituisce un aspetto di rilevante importanza ai fini della corretta ed adeguata implementazio-

Avuto riguardo alla *gestione del rischio da reato presupposto,* in via di assoluta sintesi, i due momenti fondamentali per la predisposizione di un idoneo ed efficace Modello 231 sono:

A) la mappatura dei rischi da reato (*Crime Risk Assessment)*;

B) la gestione degli specifici rischi individuati (*Crime Risk Management*).

Va da sé che le due succitate fasi vanno, poi, corredate con i succitati elementi e requisiti di cui all'art. 6 del Decreto 231.

A) La mappatura dei rischi

Attraverso tale attività viene effettuata l'individuazione e l'identificazione di tutti i probabili rischi di *reati presupposti* (v. quelli espressamente indicati dal Legislatore agli artt. 24 e ss.) verificabili nell'ambito dell'attività aziendale.

La *mappatura* è quella che dovrà servire a individuare: *dove* (v. in quale area/settore di attività) è possibile che si annidi il rischio di commissione di reati; *chi* specificamente svolge un ruolo, sia attivo che passivo; *ad opera di chi* (ossia da parte di quali singoli soggetti fisici) è probabile che sia provocato un evento pregiudizievole per gli obiettivi di prevenzione generale e speciale indicati dal D.Lgs. 231/2001; *come,* concretamente, vengono poste in essere le azioni e le attività aziendali (e quindi come, materialmente, potrebbe essere consumato un eventuale reato); *perché* un determinato tipo di condotta, o l'espletamento di una determinata funzione, può essere più o meno a rischio di reato.

Una corretta mappatura dei processi e/o delle aree e/o delle funzioni e/o delle attività "a rischio di reati" (ovviamente, non necessariamente devono essere condotte tutte le quattro predette analisi) è quella che permetterà di affrontare la *fase diagnostica* di individuazione di tutti i possibili rischi di reato, al fine di predisporre - in via successiva e conseguenziale - la *fase terapeutica* di gestione dello stesso rischio (*crime risk management*).

Una fondamentale chiarificazione di ordine generale è quella che afferisce alla definizione di processo o di *attività sensibile.*

Rappresentano situazioni *sensibili* quelle in relazione alle quali è ritenuta *probabile* (dunque non "possibile") la commissione di condotte o eventi di reato.

La loro individuazione è della massima importanza giacché sarà solo la probabilità di accadimento di un determinato evento illecito a fare scattare il dovere di prevedibilità ed evitabilità delle azioni e delle cause scatenanti lo stesso evento illecito.

Allo stesso modo, sarà solo l'individuazione delle concrete *probabilità* infauste a poter segnare il limite di doverosità tra la corretta azione di prevenzione di tutto ciò che sia realmente prevedibile e prevenibile e - viceversa - la non ipotizzabile previsione o evitabilità di tutto ciò che, eventualmente, sia solo astrattamente "possibile".

L'analisi dei rischi dovrà riguardare tutti i *rischi potenziali*, avuto specifico riguardo alle specifiche modalità attuative dei reati nelle diverse aree aziendali.

Ciò potrà consentire di:

- definire l'ambito di applicazione delle attività dell'impresa sia in termini fisici (localizzazioni, ecc.) che di personale (dipendenti, collaboratori, pubblico);
- individuare i criteri tecnici con cui confrontare i rischi di reato;
- valutare le modalità, i livelli e le possibilità di esposizione ai rischi di reato;

- evidenziare – sulla base della preliminare individuazione/identificazione dei rischi di reato - le misure di prevenzione e protezione adottate (tecniche, organizzative e procedurali) al fine di ridurre o gestire gli stessi rischi.

Il risultato dell'analisi dei rischi lavorativi dovrebbe portare ad una valutazione di ragionevole "adeguatezza" (cioè dell'idoneità delle misure tecniche, organizzative, procedurali presenti in azienda al fine di eliminare, minimizzare o gestire i rischi di reato).

Strumentale alla succitata attività propedeutica è l'inventariazione degli ambiti aziendali di attività, da condurre attraverso approcci di tipo diverso: per attività, per funzioni, per processi.

Superfluo - da ultimo - rilevare che la descritta attività di analisi dovrà essere costantemente revisionata e verificata nella sua validità attuale; il che potrà essere effettuato anche sessioni di periodici *due diligence* od *audit specifici, a fortiori* nei casi in cui emergano degli "*indicatori di sospetto*", o si verifichino fatti o circostanze nuovi (v. assunzione di nuovo personale), o si intraprendano nuove/particolari operazioni commerciali (v. magari in territori con alto tasso di corruzione, o attraverso l'adozione di nuove e complesse procedure).

Importante attività valutativa da condurre nell'ambito della fase di mappatura dei rischi è la *ponderazione.*

Tale attività comporta la valutazione del livello di accettabilità o di non eludibilità dello stesso rischio, anche attraverso una valutazione comparativa del rischio maggiore.

Il che comporta:

- che è certamente necessario definire una soglia che possa consentire di porre un limite alla quantità/qualità delle misure di prevenzione da introdurre per evitare la commissione dei reati considerati (soglia in assenza della quale la quantità/qualità di controlli preventivi istituibili rischierebbe di diventare virtualmente infinita, con le intuibili conseguenze in termini di operatività aziendale);
- che va preso razionalmente atto della oggettiva impossibilità di eliminare, in termini di azzeramento totale, il rischio stesso (si ricordi del resto che, anche nel diritto penale, vale il noto brocardo latino *ad impossibilia nemo tenetur).*

La necessità di operare una opportuna valutazione e ponderazione dei rischi cd. accettabili nasce soprattutto laddove:

- il rischio non sia oggettivamente eliminabile al 100%;
- il rischio contrapposto sia di maggiore valenza rispetto, ad esempio, al rischio di commissione di reati (v., a titolo di esempio, il caso in cui sia necessario procedere in emergenza, e bypassando i comuni passaggi di autorizzazione a più firme, all'acquisto di uno strumento di protezione individuale utile a scongiurare un pericolo imminente di lesione alla incolumità fisica).

In termini di immediata comprensibilità, *ponderare gli eventuali e diversi rischi* significa:

- avere piena consapevolezza della contemporaneità di più rischi da dovere affrontare e superare;
- valutare quale sia il rischio minore e decidere di intraprenderlo sulla base di un modello di priorità condiviso e debitamente motivato;
- dare formalmente atto di come, e perché, si sia deciso di affrontare il rischio minore rispetto ad uno maggiore;

- essere in grado di controllare a posteriori - anche attraverso la succitata motivazione della decisione – l'effettuazione dell'avvenuta ponderazione del rischio;
- controllare e vigilare il successivo "rientro a regime" delle procedure ordinarie rispetto, ad esempio, all'adozione di quelle eccezionali assunte in situazioni di emergenza.

Nel Modello 231 di *ADR Trasporti S.R.L.*, la fase di mappatura sarà affrontata attraverso l'applicazione della metodologia ISO 31000:2018.

B) La gestione dei rischi

La definizione più sintetica ed immediata di *Risk Management* potrebbe essere la seguente: «il processo di misurazione o valutazione del rischio e, soprattutto, di definizione delle strategie volte a gestirlo al fine di ridurlo/azzerarlo».

Il processo di gestione del rischio (evento che, quando si verifica, causa danni), o *Risk Management,* è stato definito in modo più puntuale come «*l'insieme di attività, metodologie e risorse coordinate per guidare e tenere sotto controllo una organizzazione con riferimento ai rischi*» (UNI 11230).

Nei fatti, e secondo una più ampia accezione, ci si riferisce sempre all'insieme dei processi mediante i quali una entità (che potrebbe essere una impresa, una organizzazione o una istituzione) individua, analizza, valorizza, elimina o tiene sotto controllo - attraverso lo sviluppo di strategie volte a governarli - i rischi legati ai vari processi produttivi, con l'obiettivo di minimizzare le perdite (intese in senso ampio e non solo sotto il profilo economico-finanziario) e di massimizzare l'efficacia e l'efficienza dei processi produttivi.

Non basta. Un corretto sistema di gestione dei rischi criminali, per operare efficacemente, non potrà certamente ridursi ad un'attività una tantum, dovendosi invece tradurre in un processo gestionale continuo e costante, da reiterare nei momenti di cambiamento aziendale (apertura di nuove sedi, ampliamento di attività, acquisizioni, riorganizzazioni, ecc.), e da mantenere comunque al massimo livello di attenzione in relazione ai cd. "rischi costanti" (v., ad esempio, in materia di salute e sicurezza sui luoghi di lavoro o come specificamente per l'attività svolta da *ADR Trasporti S.R.L.*).

Una corretta gestione del rischio dovrebbe, insomma, portare ad un abbattimento dello stesso rischio sino ad una riduzione e mantenimento livello di cd. "accettabilità tecnica" (v. la soglia minimale e oggettivamente non eliminabile al 100%).

Ciò significa che il MOGC e le misure preventive in esso stabilite dovrebbero essere tali che l'agente che voglia commettere un reato potrebbe materialmente commetterlo – ossia attuare il suo proposito criminoso – *solo* aggirando fraudolentemente lo stesso MOGC (e quindi, ad esempio, utlizzando artifizi e/o raggiri).

Scontato, in tale quadro, sottolineare che l'insieme di misure che l'agente, se vuol delinquere, sarà costretto a "forzare", dovrà essere realizzato in relazione alle specifiche attività dell'ente considerate a rischio ed ai singoli reati ipoteticamente collegabili alle stesse[9].

[9] Una logica di questo tipo è coerente con i consolidati riferimenti internazionali in tema di controllo interno e di corporate governance ed è alla base dei sistemi di autovalutazione dei rischi (*Control Self Assessment*) già presenti nelle più avanzate realtà aziendali italiane e, comunque, in rapida diffusione nel nostro sistema economico anche dietro l'impulso di recenti regolamentazioni. Il riferimento internazionale comunemente accettato come modello di riferimento in tema di governance e controllo interno è il "*CoSO Report*", prodotto in USA nel 1992 dalla Coopers & Lybrand (ora PricewaterhouseCoopers) su incarico del *Committee of Sponsoring*

A titolo meramente esemplificativo e non esaustivo, si segnala che, tra le attività e gli strumenti tipici di un corretto sistema di gestione del rischio criminale, sono da annoverare:

- *Sistema organizzativo* sufficientemente formalizzato e chiaro, soprattutto per quanto attiene alle attribuzione di responsabilità, alle linee di dipendenza gerarchica, alla descrizione dei compiti assegnati alle singole funzioni e ai singoli soggetti.
- *Proceduralizzazione dell'attività e delle azioni.*
- *Tracciabilità di tutte le azioni,* al fine di consentire l'individuazione di chi e cosa possa o debba fare, attraverso quali specifiche azioni e strumenti.
- *Progettazione ed adozione* di adeguati sistemi di registrazione dell'attività e delle azioni.
- *Programmazione di affidabili procedure manuali ed informatiche*, tali da regolamentare lo svolgimento delle attività attraverso la previsione di opportuni punti di controllo (quadrature, approfondimenti informativi su particolari soggetti quali agenti, consulenti, intermediari).
- *Separazione di compiti* fra coloro che svolgono fasi (attività) cruciali di un processo a rischio. Si consideri, ad esempio, l'importanza di tale criterio gestionale nell'ambito dell'area della gestione finanziaria, nella quale il controllo procedurale si avvale - potremmo dire "per tradizione" - di strumenti consolidati quali: l'abbinamento delle firme, le riconciliazioni, la supervisione, la separazione di compiti a seguito della contrapposizione di funzioni come la funzione acquisti e la funzione finanziaria.
- *Uso ordinario di poteri autorizzativi e di firma*, da assegnare in coerenza con le responsabilità organizzative e gestionali, eventualmente prevedendo, ove richiesto, una puntuale indicazione delle soglie di approvazione delle spese.
- *Azione costante di formazione ed addestramento,* quali componenti essenziali per la funzionalità dello stesso Modello.
- *Valido ed efficace sistema di comunicazione,* attraverso il quale possa crearsi la circolazione delle informazioni e dei flussi informativi all'interno dell'azienda e quindi accrescersi il valore, sia del coinvolgimento di tutti i soggetti interessati, sia di una conseguente azione di impegno e consapevolezza da parte di tutti i soggetti operanti *con o per* l'azienda.
- *Coinvolgimento di tutti i "destinatari" del MOGC*, da realizzarsi attraverso azioni quali: la consultazione preventiva in merito alla individuazione e valutazione dei rischi ed alla definizione delle misure preventive; l'organizzazione di riunioni periodiche.
- *Codice Etico,* quale documento rappresentativo dei principi morali ed etici che la società ritiene essenziali e non derogabili, sia per il corretto perseguimento della legalità aziendale, sia nell'ottica di una azione di prevenzione generale e speciale.
- *Progettazione di un efficace ed esaustivo sistema di controllo,* in grado di vigilare, contrastare, ridurre o, eventualmente, bloccare i rischi identificati. Le componenti di controllo dovranno, ovviamente, integrarsi in un sistema organico nel quale l'eventuale debolezza di una

---

Organizations of the Treadway Commission (con l'*Institute of Internal Auditors* e l'AICPA fra le Sponsoring Organizations) che lo ha adottato e proposto quale modello di riferimento per il sistema di controllo delle imprese. Ad esso si sono ispirate le regolamentazioni nazionali di tutti i principali paesi (Regno Unito, Canada, ecc.).
Il *CoSO Report* rappresenta anche in Italia la *best practice* formalmente riconosciuta per le società quotate in Borsa (cfr. la menzione contenuta nello stesso Codice di Autodisciplina adottato dal Comitato per la Corporate Governance delle Società Quotate presso la Borsa Italiana nel 1999 ed aggiornato da ultimo nel 2006), oltre a costituire un evidente riferimento concettuale della Guida Operativa Collegio Sindacale del 2000, delle Circolari dell'ISVAP e della Banca d'Italia.

componente dovrà essere controbilanciata dal rafforzamento di una o più delle altre componenti in chiave compensativa.

Dalle richiamate azioni gestionali derivano - in via conseguenziale - alcuni fondamentali principi, che di seguito sono richiamati a mero titolo esemplificativo posto che nella II parte del presente Modello saranno singolarmente esaminati sia i *Protocolli Generali* che i *Protocolli Specifici*:

- *"Ogni operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua"*, ossia per ogni operazione deve essere garantito un adeguato supporto documentale attraverso il quale possa procedersi, in ogni momento, all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione ed alla individuazione chi ha fisicamente autorizzato, effettuato, registrato, verificato l'operazione stessa;
- *"Nessuno può gestire in autonomia un intero processo"*; il che comporta che deve essere rigorosamente rispettato il principio di separazione dei compiti e delle funzioni;
- *"A nessuno possono essere attribuiti poteri illimitati";*
- "*I poteri e le responsabilità devono essere chiaramente definiti e conosciuti all'interno dell'organizzazione";*
- "*I poteri autorizzativi e di firma devono essere coerenti con le responsabilità organizzative assegnate"*.

Logicamente insita nella fase di gestione del rischio è la parte che riguarda i *controlli*, sul presupposto che qualunque sistema di gestione di rischio è destinato a fallire sul nascere ove non venga programmato e strutturato un costante, corretto ed esaustivo, sistema di controlli.

Tale sistema dovrà essere fondato sui seguenti, fondamentali, principi:

- devono essere previsti ed utilizzati specifici sistemi di controllo, generali e speciali;
- tutti i sistemi di controllo devono integrarsi con i meccanismi di gestione del rischio principale ed essere compatibili e convergenti tra di loro in una ideale architettura di sistema;
- i controlli dovranno essere strutturati razionalmente e sempre documentati;
- tutti dovranno collaborare alla funzione di controllo, mettendo a disposizione i resoconti (analitici e sintetici, periodici e *ad hoc*) relativi alla specifica attività realizzata;

Ciò significa che lo stesso sistema dovrà contenere le seguenti componenti essenziali:

✓ Previsione e strutturazione di meccanismi di controllo centrale, come ad esempio quelli ad opera degli organi societari deputati a tale funzione (v. l'Organismo di Vigilanza previsto dal MOGC);
✓ Predisposizione di meccanismi di allerta;
✓ Verifica di possibili circostanze predisponenti;
✓ Controlli, correzioni ed eliminazione, delle eventuali cause scatenanti;
✓ Programmazione ed effettuazione di controlli a campione;
✓ Programmazione di controlli di processo;
✓ Monitoraggio e vigilanza sul funzionamento complessivo del sistema dei controlli;
✓ Integrazione delle componenti di controllo in un sistema organico;
✓ Documentazione di tutti i controlli e della loro effettuazione.

Il "controllo", peraltro, rappresenta un presidio anti rischio inderogabile - che potremmo senza esagerazione definire il "principe del risk management" - al fine di potere individuare e saggiare con immediatezza: - l'efficacia del sistema di gestione di rischio; - l'eventuale presenza di punti di criticità dello stesso sistema; - l'effettuazione e la correttezza delle azioni prescritte; - la presenza di eventuali disfunzioni o anomalie delle stesse azioni.

Il controllo rappresenta, inoltre, il fondamentale antecedente logico ed organizzativo della conseguente fase di predisposizione ed adozione delle misure correttive in quanto da esso derivano una serie di *feedback* fondamentali per migliorare il sistema organizzativo.

2.3 L'Organismo di Vigilanza

In base a quanto disposto dall'art. 6, lettera b), del D.Lgs. 231/2001: condizione essenziale ed inderogabile dell'efficacia di un Modello di Organizzazione, Gestione e Controllo, nonché della correlativa operatività dell'"esimente" dall'eventuale responsabilità amministrativa della Società, è che «*il compito di vigilare sul funzionamento e l'osservanza dei modelli, di curare il loro aggiornamento, sia stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo*».

Anche l'art. 7, co. 4, lett. a) del D.Lgs. 231/2001 ribadisce che l'efficace attuazione del Modello richiede una sua verifica periodica, nonché la sua eventuale modifica e/o aggiornamento quando – anche su input dell'Organismo di Vigilanza – siano emersi: significative violazioni delle prescrizioni fissate; punti o ragioni di criticità del MOGC; mutamenti nell'organizzazione o nell'attività.

Ne deriva che l'Organismo di Vigilanza rappresenta - soprattutto per le caratteristiche di autonomia ed indipendenza espressamente richieste per legge - una sorte di "vigilante" super partes, dotato di autonomi poteri di iniziativa e di controllo, che, nell'interesse della Legalità, controlla e sottopone a monitoraggio periodico/costante l'efficacia del Modello 231 e la sua piena osservanza da parte di tutti i "destinatari".

Per garantire l'autonomia e l'indipendenza nello svolgimento dei compiti che gli sono stati affidati, l'OdV:

- non può essere direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo;
- riferisce direttamente all'Organo Amministrativo, come unità di staff in posizione gerarchica la più elevata possibile;
- deve avere le competenze e gli strumenti tecnico-professionali adeguati alle funzioni che è chiamato a svolgere (v. competenze di natura organizzativa e giuridica);
- non potrà essere sindacato o censurato nelle sue valutazioni da alcun organismo dell'ente, rimanendo la sua posizione totalmente avulsa da qualsivoglia forma di interferenza e/o condizionamento da parte dell'ente.
- deve essere posto nelle condizioni di *effettività* nel senso di potere assolvere realmente ai complessi e delicati compiti di cui la Legge lo investe.

Al fine di consentire una azione di vigilanza quanto più possibile efficace ed incisiva, l'art. 6 del Decreto 231 prevede che siano assicurati all'Organismo di Vigilanza precisi e specifici "*obblighi di informazione".*

Si tratta dei *flussi informativi* verso l'OdV - da parte di tutte le funzioni aziendali e/o dipendenti dell'ente - che il Modello 231 dovrà necessariamente declinare e comunicare con obbligo di osservanza.

I *Flussi Informativi* di *ADR Trasporti S.R.L.* sono riportati *infra,* nella Parte II.

Sul piano strettamente operativo, ogni Modello 231 stabilisce - in aderenza ai principi generali ormai consolidati e unanimemente condivisi - le fondamentali norme di funzionamento del proprio Organismo di Vigilanza (composizione, durata, incompatibilità, poteri-doveri, etc.).

Tali norme di funzionamento sono inserite nello *Statuto OdV* di *ADR Trasporti S.R.L.*, *infra* nella Parte II.

Lo stesso Organismo di Vigilanza adotta poi – nell'ambito della sua autonomia di azione – un proprio *Regolamento OdV*.

2.4 Il Sistema Disciplinare 231

Altro requisito essenziale per garantire l'effettività del Modello ed una efficace azione dell'Organismo di Vigilanza è la definizione di un sistema disciplinare commisurato alla violazione dei Protocolli e/o di ulteriori regole del Modello e del Codice Etico.

Tale requisito è inderogabilmente richiesto dall'art. 6, comma 2, lett. e) del D.Lgs. 231/2001: *"In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze … e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".*

Dal punto di vista generale, è vigente il principio di piena indipendenza ed autonomia tra procedimento penale e procedimento disciplinare, considerato che la condotta illecita tenuta da un dipendente-destinatario del MOGC può assumere una plurima valenza patologica (di reato, devoluto all'Autorità Giudiziaria ordinaria; di illecito disciplinare, sanzionabile dal datore di lavoro).

La logica di fondo dell'ordinamento – che è anche quella dell'art. 6 del Decreto 231 – è che ogni categoria di persone fisiche o entità giuridica (società, istituzioni, ordini professionali, federazioni sportive, etc.) può liberamente decidere, in piena autonomia ed indipendentemente dalla connotazione dei fatti in termini di rilevanza penale, le proprie regole disciplinari, di natura sia sostanziale che processuale.

Questa regola di autonomia vale per tutti i procedimenti disciplinari.

Nel caso di un Modello di Organizzazione, Gestione e Controllo *ex* Decreto 231, è lo stesso Legislatore ad *imporre,* espressamente, l'adozione di un autonomo sistema disciplinare quale presidio a supporto dell'azione preventiva.

In punto di diritto, l'unico e reale condizionamento ai contenuti del potere disciplinare *ex* Decreto 231 può essere rappresentato da leggi di livello gerarchico superiore (come la Costituzione, il codice civile o lo Statuto dei lavoratori *ex* Legge 20 maggio 1970 n. 300) e *non* da altro tipo di fonte normativa di livello secondario, come ad esempio i Contratti Collettivi Nazionali di Lavoro.

Nonostante tale premessa, la soluzione pragmatica unanimemente condivisa in tema di sistema disciplinare 231 è – anche al fine di evitare possibili e defatiganti contenziosi di natura

lavoristica – quella di strutturare la parte dei Modelli che riguarda il sistema disciplinare rinviando:

- ai CCNL, per ciò che riguarda le specifiche sanzioni applicabili (richiamo, censura, multa, sospensione, etc.);
- all'art. 7 dello Statuto dei lavoratori e alle norme generali di diritto, per ciò che afferisce alle regole di tipo processuale.

Si ritiene, quindi, che il sistema disciplinare 231 debba attenersi ai seguenti principi generali:

- Forma scritta;
- Comunicazione delle norme disciplinari ai dipendenti mediante affissione in luogo accessibile a tutti [10];
- Responsabilità disciplinare sempre rigorosamente personale, in ossequio al divieto di responsabilità oggettiva;
- Contestazione della condotta censurata in termini di immediatezza, chiarezza, univocità, aderenza alla violazione di specifici fatti o condotte in contrasto con il MOGC (in qualunque sua parte o protocollo) o con il Codice Etico e di Comportamento (in qualunque sua parte o norma);
- Contestazione degli addebiti in forma scritta specifica[11], immediata ed immutabile;
- Conduzione e conclusione del procedimento disciplinare entro un tempo certo e ragionevole;
- Riconoscimento del diritto di difesa pieno;
- Redazione dei provvedimenti di natura disciplinare (sia istruttori che decisori) con motivazione esaustiva, logica, non contraddittoria, aderente ai fatti, alle norme, alla condotta contestata e al corredo probatorio emerso in sede di istruttoria disciplinare;
- Sanzioni giuste, proporzionali e compatibili con la natura/specie/modalità dell'azione, con la gravità della violazione contestata[12] e del pericolo causato con l'azione oggetto di incolpazione, con l'occasionalità o reiterazione della stessa violazione, con le circostanze oggettive e soggettive del fatto contestato, con la personalità dell'incolpato ed il suo vissuto personale/professionale, con il grado e l'intensità della colpa, del pentimento o della resipiscenza mostrata dall'incolpato;
- Punibilità del tentativo, ove lo stesso sia certo, univoco e determinato;
- Aggravamento sanzionatorio in caso di comportamento reiterato;
- Divieto di avviare un procedimento disciplinare per un fatto già giudicato e/o sanzionato in precedenza (in applicazione del generale divieto di *bis in idem)*;
- Rigoroso rispetto delle norme in materia di *whistleblowing ex* D.Lgs. 10 marzo 2023, n. 24 (*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*), tenuto conto che lo stesso ha anche previsto l'obbligo di

[10] V. pubblicazione in "bacheca lavoratori", o sul sito aziendale, o diffusione con apposita circolare, o comunicato, anche se rimane sempre preferibile una consegna personale con debita sottoscrizione «per presa visione».

[11] «La contestazione deve fornire le indicazioni necessarie ed essenziali per individuare, nella sua materialità, i fatti oggetto di contestazione» (Cass. civ., sez. L., 16 ottobre 2019, n. 26199).

[12] Il principio è fissato anche dall'art. 2106 c.c. (*Sanzioni disciplinari*): «L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo alla applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione».

inserire del Sistema Disciplinare 231 specifiche sanzioni da irrogare in caso di violazione della stessa stessa normativa a tutela dei "segnalanti".

Il potere disciplinare *ex* Decreto 231 è attribuito (salvo poteri interni tramite delega) al Datore di lavoro o al Legale Rappresentate dell'ente.

L'Organismo di Vigilanza 231 è privo di tale potere, anche se allo stesso è certamente riconosciuto un potere/dovere di segnalazione/impulso e di conduzione di eventuali accertamenti o verifiche di supporto istruttorio al procedimento disciplinare.

Il *Sistema Disciplinare 231* è riportato in Allegato 1.

2.5 Il Codice Etico e di Comportamento

Sebbene l'art. 6, comma 3, del D.Lgs. 231/2001 faccia un richiamo meramente generico ai "*codici di comportamento redatti dalle associazioni rappresentative degli enti*", è opinione unanime – pienamente condivisa e confermata anche in sede giurisprudenziale – che tra gli elementi essenziali di un Modello di Organizzazione, Gestione e Controllo, ex D.Lgs. 231/2001 debba esserci, alla stregua di parte essenziale ed inderogabile, un *Codice Etico e/o di Comportamento.*

Per tradizione, un *Codice Etico* racchiude i principi generali e valoriali prescelti da una collettività o da un ente che svolga un'attività economica, quale fondamenti del proprio agire.

In campo nazionale, avuto specifico riguardo alle amministrazione pubbliche e parapubbliche, si è preferito adottare la figura del *Codice di Comportamento* (v. D.P.R. 16 aprile 2013 n. 62), cui è stata conferita anche l'importante funzione di *misura preventiva anticorruzione.*

Al fine di evitare equivoci di natura linguistica, la differenza tra *Codice Etico* e *Codice di Comportamento* è stata adeguatamente chiarita - su un piano strettamente sostanziale - dall'Autorità Nazionale Anticorruzione: «*I codici di comportamento non vanno confusi con i codici "etici", comunque denominati. I codici etici hanno una dimensione "valoriale" e non disciplinare … I codici di comportamento, invece, fissano doveri di comportamento che hanno una rilevanza giuridica che prescinde dalla personale adesione, di tipo morale, ovvero dalla personale convinzione sulla bontà del dovere. Essi vanno rispettati in quanto posti dall'ordinamento giuridico*» (Delibera ANAC n. 177 del 19 febbraio 2020).

Le due dimensioni - *valoriale* in senso lato, *comportamentale* e di rilevanza disciplinare in senso stretto - non si escludono affatto ed anzi possono utilmente agire in posizione di appaiamento al fine di innalzare e rafforzare ulteriormente i canoni di moralità valoriale e comportamentale alla cui stregua un ente vuole operare.

È, appunto, questa la scelta adottata da *ADR Trasporti S.R.L.*

In chiave operativa, le norme di un *Codice Etico e di Comportamento* a corredo di un Modello 231: da un lato, sono ontologicamente generali; dall'altro, sono direttamente applicabili ed imperative nei confronti di tutti coloro che operano "con" o "per" l'ente – compresi i cd. destinatari estranei, come i consulenti, i collaboratori e i fornitori – alla stregua di *regole di convivenza civica* che lo stesso ente richiede e pretende siano rispettate *a casa propria*.

Tale valenza impositiva fa sì che il *Codice Etico e di Comportamento* diventi parte integrante del Modello 231, con ciò permettendo di coprire efficacemente quei possibili "spazi vuoti", eventualmente non proceduralizzabili ma certamente sanzionabili in via disciplinare.

Dal punto di vista contenutistico, il *Codice Etico e di Comportamento* è un documento interno predisposto dall'ente in assoluta libertà e autonomia, dunque pienamente personalizzabile in aderenza all'attività esercitata o alle proprie scelte gestionali.

In via generale, il *Codice Etico e di Comportamento* è articolato in parti, o sezioni, o articoli, di cui si riportano alcuni esempi per nuclei essenziali:

- ✓ *Principi generali e norme di comportamento*
- ✓ *Rapporti esterni*
- ✓ *Rapporti interni*
- ✓ *Obbligo di riservatezza*
- ✓ *Uso di beni aziendali e risorse informatiche*
- ✓ *Rispetto dei beni ambientali*
- ✓ *Gestione contabile e finanziaria*
- ✓ *Conflitti di interesse*

Per ciò che riguarda la sua efficacia giuridica, la violazione del *Codice Etico e di Comportamento* costituisce, in base a chi fisicamente la ponga in essere:

- giusta causa di azione disciplinare (per i dipendenti);
- inadempimento alle obbligazioni contrattuali con ogni conseguente effetto di legge e di contratto (per i collaboratori, professionisti o fornitori esterni);
- giusta causa di revoca dei poteri e/o di estromissione societaria (per dirigenti, amministratori o organi che rivestono cariche sociali).

Trattandosi di un documento della massima importanza ai fini dell'organizzazione e della vita aziendale, il *Codice Etico e di Comportamento* deve essere correttamente comunicato, diffuso, nonché accompagnato da una adeguata attività formativa.

Il *Codice Etico e di Comportamento* è riportato in Allegato 2.

2.6 Il Whistleblowing

L'istituto del *whistleblowing* - di origini anglosassoni - è tra i più importanti cardini della filosofia anticorruzione introdotta dalla Legge 6 novembre 2012 n. 190 (*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*).

Sul piano pratico, nasce come istituto giuridico volto a riconoscere protezione ai dipendenti che abbiano denunciato eventuali condotte illecite di cui siano venuti a conoscenza sui luoghi di lavoro (o in occasione dell'attività lavorativa) e che, per tale motivo, siano stati ingiustamente discriminati o abbiano subito ritorsioni (licenziamenti, declassamenti, trasferimenti punitivi etc.).

La citata Legge 190/2012 ha previsto tale tipo di protezione solo per i dipendenti pubblici e nell'ambito delle Pubbliche Amministrazioni.

Con la Legge 30 novembre 2017 n. 179 (*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*), la tutela da *whistleblowing* è stata estesa al settore privato e, dunque, anche ai dipendenti delle aziende private.

La stessa Legge 179/2017 ha esteso il suo raggio di applicazione al D.Lgs. 231/2001, aggiungendo all'art. 6 i commi 2 *bis*, 2 *ter* e 2 *quater*, che appunto prevedono l'obbligatorio inserimento nei Modelli di Organizzazione 231 di principi e procedure "anti - ritorsione".

Attualmente, la Legge 179/2017 è stata superata dal D.Lgs. 10 marzo 2023, n. 24 (*Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*), con il quale è stato rivisto e regolamentato in via definitiva questo importante strumento normativo al fine di renderlo espressamente funzionale, sia alla logica della "protezione anti ritorsione" che a quella della "incentivazione alla segnalazione di illeciti".

Significative, a quest'ultimo proposito, le indicazioni dell'art. 2 sulle *"definizioni"* di legge:

«*Ai fini del presente decreto, si intendono per:*

«a) «violazioni»: comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

1) illeciti amministrativi, contabili, civili o penali ….;

2) condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazioni dei modelli di organizzazione e gestione ivi previsti ….;

3) illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali … relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;

4) atti od omissioni che ledono gli interessi finanziari dell'Unione Europea…;

5) atti od omissioni riguardanti il mercato interno … comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonchè le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalita' della normativa applicabile in materia di imposta sulle società;

6) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione …

b) «informazioni sulle violazioni»: informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico … nonchè gli elementi riguardanti condotte volte ad occultare tali violazioni;

c) «segnalazione» o «segnalare»: la comunicazione scritta od orale di informazioni sulle violazioni;

……
m) «ritorsione»: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla
persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto…. ».

Tra le modifiche di maggiore rilievo del neo D.Lgs. 24/2023 è la previsione della cd. "protezione anti - ritorsione" non solo per i dipendenti di enti pubblici e privati, ma anche per i soggetti che risultano coinvolti a vario titolo con l'attività dell'ente: collaboratori autonomi; liberi professionisti che prestano consulenza o lavorano per l'ente; volontari e tirocinanti anche non retribuiti; azionisti; amministratori; ex dipendenti; candidati ad una posizione lavorativa; facilitatori (es. associazioni, famiglia del segnalante) e colleghi che operano all'interno del medesimo contesto lavorativo del segnalante; eccetera.

Quali possibili esempi di "ritorsione", il D.Lgs. 24/2023 indica: a) il licenziamento, la sospensione o misure equivalenti; b) la retrocessione di grado o la mancata promozione; c) il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro; d) la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa; e) le note di merito negative o le referenze negative; f) l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria; g) la coercizione, l'intimidazione, le molestie o l'ostracismo; h) la discriminazione o comunque il trattamento sfavorevole; i) la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione; l) il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; m) i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi; n) l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro; o) la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; p) l'annullamento di una licenza o di un permesso; q) la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Agli specifici fini del D.Lgs. 231/2001, il succitato D.Lgs. 24/2023 ha abrogato gli ex commi 2 ter[13] e 2 quater[14] dell'art. 6 (già introdotti dalla Legge 179/2017), lasciando operativo il solo comma 2 bis che testualmente dispone:
«I modelli di cui alla lettera a) del comma 1 prevedono:

[13] «*2-ter. L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo».*

[14] «*2-quater. Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. È onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa».*

a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate».

In via generale, il D.Lgs. 24/2023 ha rivisto in via unitaria la precedente regolamentazione del *whistleblowing* (frutto della duplice normativa, di tipo pubblicistico ex Legge 190/2012 e di tipo privatistico ex Legge 179/2017) e stabilito i seguenti principi e norme regolatrici:

A) Le segnalazioni possono essere "*interne*" al proprio ente, o "*esterne*" (ossia, come si vedrà di qui a poco, inviate all'Autorità Nazionale Anticorruzione).

B) Al fine di assicurare una corretta ed affidabile "*segnalazione interna"*, i Modelli 231 devono prevedere canali di segnalazione affidati ad una persona o a un ufficio autonomo dedicato (a cui, entro sette giorni, la segnalazione dovrà essere trasmessa dando contestuale notizia della trasmissione alla persona segnalante).

C) Le segnalazioni sono effettuate in forma scritta, anche con modalità informatiche, o orale.

D) Nell'ambito della gestione del canale di "*segnalazione interna"*, la persona o l'ufficio a cui è affidata la segnalazione dovrà: - rilasciare alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione; - mantenere le interlocuzioni con la persona del segnalante ed eventualmente richiedere integrazioni; - dare diligente seguito alle segnalazioni; - fornire riscontro entro tre mesi dalla data dell'avviso di ricevimento; - mettere a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti, sia per effettuare le *"segnalazioni interne"* che per effettuare le "*segnalazioni esterne"*.

E) Le informazioni sulle "*segnalazioni*" dovranno essere esposte e rese facilmente visibili nei luoghi di lavoro, nonchè accessibili alle persone che pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico con l'ente; se dotati di un proprio sito internet, i soggetti del settore privato pubblicano dette informazioni anche in una sezione dedicata del suddetto sito.

F) La persona segnalante può effettuare una *"segnalazione esterna"* se, al momento della sua presentazione, ricorre una delle seguenti condizioni: a) non è prevista, nell'ambito del suo contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto per legge; b) la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito; c) la persona segnalante ha fondati motivi di ritenere che, se

effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione; d) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

G) L'organo deputato alle "*segnalazioni esterne*" è l'Autorità Nazionale Anticorruzione (che entro il mese di giugno 2023 provvederà ad emettere apposite Linee Guida), la quale attiverà un canale che garantisca riservatezza dell'identità del segnalante e del contenuto. Le "*segnalazioni esterne"* sono effettuate in forma scritta tramite la piattaforma informatica, oppure in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole. La "*segnalazione esterna"* presentata ad un soggetto diverso dall'ANAC è trasmessa a quest'ultima, entro sette giorni dalla data del suo ricevimento, dando contestuale notizia della trasmissione alla persona segnalante. L'ANAC designerà personale specificamente formato per la gestione del canale di segnalazione esterna, provvedendo anche a: a) fornire a qualsiasi persona interessata informazioni sull'uso del canale di segnalazione esterna e del canale di segnalazione interna; b) dare avviso alla persona segnalante del ricevimento della segnalazione esterna entro sette giorni dalla data del suo ricevimento; c) mantenere le interlocuzioni con la persona segnalante e richiedere a quest'ultima, se necessario, integrazioni; d) dare diligente seguito alle segnalazioni ricevute; e) svolgere l'istruttoria necessaria a dare seguito alla segnalazione, anche mediante audizioni e acquisizione di documenti; f) dare riscontro alla persona segnalante entro tre mesi o, se ricorrono giustificate e motivate ragioni, sei mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei sette giorni dal ricevimento; g) comunicare alla persona segnalante l'esito finale, che può consistere anche nell'archiviazione o nella trasmissione alle autorità competenti o in una raccomandazione o in una sanzione amministrativa.

H) Le *segnalazioni* non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse. L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante. Nell'ambito del procedimento penale, l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 c.p.p. (*obbligo del segreto*). Nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del segnalante.

I) Ogni trattamento dei dati personali deve essere effettuato a norma del Regolamento (UE) 2016/679, del D.Lgs. 30 giugno 2003, n. 196 e del D.Lgs. 18 maggio 2018, n. 51.

J) Le "*segnalazioni interne ed esterne"*, e la relativa documentazione, sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

K) Gli enti o le persone segnalanti non possono subire alcuna ritorsione. In caso di domanda risarcitoria presentata all'autorità giudiziaria, se si dimostra di aver effettuato una segnalazione e di avere subito un danno, si presume, salvo prova contraria, che il danno sia conseguenza di tale segnalazione. Gli eventuali atti ritorsivi sono nulli; le persone eventualmente licenziate avranno diritto di essere reintegrate sul posto di lavoro; l'autorità giudiziaria eventualmente adita adotta tutte le misure, anche provvisorie, necessarie ad assicurare la tutela alla situazione giuridica soggettiva azionata, ivi compresi il risarcimento del danno, la reintegrazione nel posto di lavoro, l'ordine di cessazione della condotta ritorsiva e la dichiarazione di nullità degli atti adottati in violazione del D.Lgs. 24/2023.

L) Avuto riguardo alle *sanzioni* eventualmene applicabili, le stesse sono applicate dall'ANAC nella misura di: a) da 10.000 a 50.000 euro quando accerta che sono state commesse ritorsioni o quando accerta che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza; b) da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme a quella prevista per legge, nonchè quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute; c) da 500 a 2.500 euro, nel caso di cui all'articolo 16, comma 3 (v. condanna del segnalante per diffamazione o calunnia).

M) Il Sistema Disciplinare adottato ai sensi del D.Lgs 231/2001 deve prevedere sanzioni nei confronti di coloro che si sono resi responsabili delle condotte sanzionabili ai sensi della precedente lett. L).

Nello specifico caso di *ADR Trasporti S.R.L.*, la *tutela da whistleblowing* - e il relativo canale di comunicazione per le *"segnalazioni interne"* - è stata affidata ad un legale di fiducia della Società, e la gestione del canale interno di segnalazione è stata regolata attraverso la *Procedura Whistleblowing* debitamente pubblicata sul sito aziendale.

PARTE II
Il Modello 231 di *ADR TRASPORTI SRL*

1. CHI SIAMO E COME OPERIAMO

1.1. Costituzione e governance di *ADR Trasporti S.R.L.*

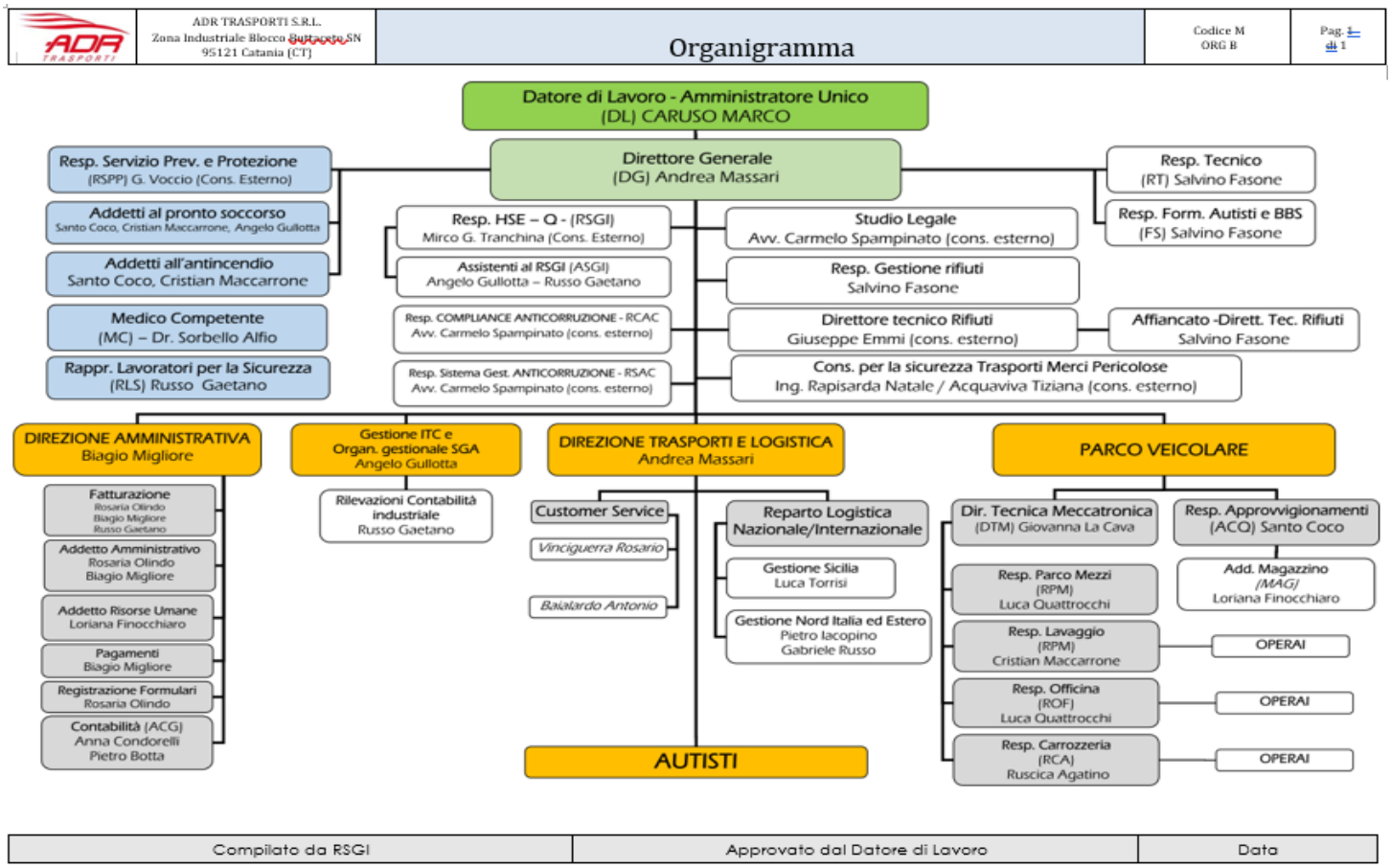
ADR Trasporti S.R.L. viene costituita in data 4 novembre 2009, tra i signori Marco Caruso (nato a Catania il 5 novembre 1979) e Gaetano Gennaro (nato a Catania l'8 settembre 1975), con sede a Catania, via Napoli 116.

In data 12 settembre 2014, il sig. Gaetano Gennaro vende il 40% della sua quota al sig. Marco Caruso e il restante 10% al sig. Gaetano Russo. Per effetto della duplice predetta cessione, i soci rimangono: il sig. Marco Caruso al 90%; il sig. Gaetano Russo al 10%.

In data 6 luglio 2015, viene comunicata variazione di codice fiscale/partita IVA – 04740540879 - e trasferimento di sede legale in in Catania, 95121, Zona Industriale Blocco Buttaceto s.n.. Sede secondaria - ma solo come allocazione di parcheggio - è quella di Priolo Gargallo (SR), Contrada Mostringiano s.n., 96010. La Società è iscritta alla C.C.I.A.A. di Catania al n. 316099.

Sistema di governance prescelto: quella ad Amministratore Unico.

Si riporta di seguito l'Organigramma Aziendale:



In ADR è stato regolamente nominato un Revisore Contabile.

1.2. Attività svolta

L'oggetto sociale indicato nell'art. 4 del succitato Atto Costitutivo/Statuto è l'attività di: «-*svolgimento di tutti i servizi di autotrasporto merci e prodotti vari per conto terzi per qualsiasi località sia nazionale che estera, con automezzi sia propri, sia dei singoli soci, sia presi in affitto nonché svolgere servizi di spedizione di qualsiasi merce, avvalendosi di qualsiasi mezzo di trasporto sia pubblico che privato; - trasporto di cose e persone con furgoni, camion, autotreni, autobotti, autobus, in gestione diretta o in concessione; - gestire officine per la riparazione degli automezzi propri, dei soci e di terzi; - deposito di merci con custodia e servizi di imballaggio e trasporto; - noleggio di automezzi compresi i camion, le autogrù, i carrelli elevatori e i camion con grù; - carico, scarico e posizionamento di macchinari e casseforti; - traslochi, facchinaggio, trasporti eccezionali e soccorso stradale; - assumere la concessione in appalto di servizi di trasporti anche dallo stato e da enti pubblici; - istituire o gestire impianti e magazzini necessari per l'esercizio delle attività sociali; - acquistare, prendere in affitto, costruire e sotto qualsiasi forma disporre di aree e magazzini destinati alla sosta e al ricovero degli autoveicoli sociali, dei soci, e di terzi nonché di tutte le attrezzature, merci e macchine sociali e di terzi; - trasporto e smaltimento di rifiuti, anche speciali e tossici, nonché il lavaggio, la disinfezione e la bonifica dei mezzi di trasporto, anche di terzi, che operano tali tipi di attività; - l'attività di lavaggio di automezzi; - acquistare, prendere in affitto o sotto qualsiasi altra forma, le macchine e le attrezzature necessarie all'espletamento dell'attività sociale……*».

Nel tempo, la Società si è concretamente specializzata nell'*attività di trasporto di prodotti chimici in ADR,* che è appunto diventata l'attività societaria principale.

A quest'ultimo proposito, l'ADR è l'Accordo Europeo che regolamenta i trasporti di merci e rifiuti pericolosi su strada pubblica, siglato a Ginevra il 30 settembre 1957 ed entrato in vigore il 29 gennaio 1968, a sua volta volta modificato da un Protocollo emanato a New York il 21 agosto 1975 ed entrato in vigore il successivo il 19 aprile 1985.

In Italia l'ADR è stato recepito nell'Ordinamento attraverso la Legge 12 agosto 1962 n. 1839 (*Ratifica ed esecuzione dell'Accordo europeo relativo al trasporto internazionale di merci pericolose su strada, con annessi Protocollo ed Allegati, adottato a Ginevra il 30 settembre 1957*).

Nel merito, la denominazione in lingua inglese del summenzionato Accordo è: *European Agreement concerning the International Carriage of Dangerous Goods by Road.*

L'acronimo ADR deriva dalla denominazione in lingua francese: ***A****ccord européen relatif au transport international des marchandises* ***D****angereuses par* ***R****oute* (traduzione in italiano: *"Accordo europeo relativo al trasporto internazionale su strada delle merci pericolose"*).

Dall'aggiornamento dell'1 gennaio 2021 (ADR 2021), l'Accordo ha perso l'aggettivo "europeo", diventando *Accordo relativo al trasporto internazionale su strada delle merci pericolose.*

In via generale, va ricordato che la materia del trasporto di merci pericolose su strada è stata sempre sentita ed affrontata a livello mondiale (valga, per tutte, la costituzione del *Comitato di esperti sul trasporto di merci pericolose e sul sistema globale armonizzato di classificazione ed etichettatura delle sostanze chimiche* presso l'ECOSOC - Consiglio economico e sociale delle Nazioni Unite, le cui raccomandazioni vengono appplicate in tutto il mondo).

Avuto specifico riguardo all'Europa, la normativa sul trasporto interno delle merci pericolose ADR (ma anche di riflesso quelle dell'ADN e del RID) è stata accolta nell'ordinamento europeo per mezzo della *Direttiva 2008/68/CE del Parlamento europeo e del Consiglio del 24 settembre 2008*.

In parallelo, dal punto di vista della legislazione chimica, sono stati introdotti anche il *Regolamento (CE) n. 1272/2008 del Parlamento europeo e del Consiglio del 16 dicembre 2008 , relativo alla classificazione, all'etichettatura e all'imballaggio delle sostanze e delle miscele* ed il suo complementare *Regolamento (CE) n. 1907/2006 del Parlamento europeo e del Consiglio del 18 dicembre 2006 concernente la registrazione, la valutazione, l'autorizzazione e la restrizione delle sostanze chimiche.*

Per ciò che, in particolare, concerne l'ADR, il Legislatore Italiano ha riformato la disciplina ed emanato il D.lgs. 27 gennaio 2010, n. 35 *(Attuazione della direttiva 2008/68/CE, relativa al trasporto interno di merci pericolose),* fermo restando comunque che la disciplina era già pienamente operativa nell'ordinamento italiano dal 1° gennaio 1997, per mezzo del D.M. del Ministro dei Trasporti e della Navigazione del 4 settembre 1996.

Sul piano strettamente operativo, le *disposizioni ADR* riguardano:

A) La classificazione delle sostanze pericolose in riferimento al trasporto su strada;
B) La determinazione e classificazione come pericolose delle singole sostanze;
C) Le condizioni di imballaggio delle merci,
D) Le caratteristiche degli imballaggi e dei contenitori;
E) Le modalità costruttive dei veicoli e delle cisterne;
F) I requisiti per i mezzi di trasporto e per il trasporto, compresi i documenti di viaggio;
G) L'abilitazione dei conducenti i mezzi trasportanti merci pericolose;
H) Le esenzioni dal rispetto delle norme dell'Accordo.

In merito al superiore punto sub A), la pericolosità dei vari materiali viene definita in base ai rischi che le sostanze rivestono nei confronti delle persone e dell'ambiente e la suddivisione iniziale è in classi:

- Classe 1 Materiali e sostanze esplosive
- Classe 2 Gas
- Classe 3 Liquidi infiammabili
- Classe 4.1 Materie solide infiammabili
- Classe 4.2 Sostanze soggette ad auto combustione
- Classe 4.3 Sostanze che, a contatto con l'acqua, sprigionano gas infiammabili
- Classe 5.1 Materie comburenti
- Classe 5.2 Perossidi organici
- Classe 6.1 Sostanze tossiche
- Classe 6.2 Prodotti infettivi
- Classe 7 Materiali radioattivi
- Classe 8 Materiali corrosivi
- Classe 9 Materiali con pericolosità varia e pericolosi per l'ambiente

In ordine al superiore punto sub C), si possono distinguere tre categorie, a cui sono associati tre tipi di codici alfanumerici, nei quali figurano delle determinate lettere di riconoscimento:

- gruppo I (alta pericolosità), lettera X;
- gruppo II (media pericolosità), lettera Y;
- gruppo III (bassa pericolosità), lettera X.

Il gruppo di imballaggio è indicato nel documento di trasporto ADR qualora assegnato, preceduto facoltativamente dalla sigla GI oppure PG (*packaging group*).

Circa il superiore punto sub G), il Certificato di Formazione Professionale (CFP) abilita alla guida di tutti i veicoli adibiti al trasporto nazionale o internazionale di merci pericolose, indipendentemente dalla massa.

Il CFP è necessario per i conducenti di veicoli adibiti al trasporto, sia nazionale che internazionale, di merci pericolose:

- con cisterne fisse o smontabili di capacità superiore a 1.000 litri
- con batteria di capacità totale superiore a 1.000 litri
- in container-cisterna, cisterne mobili o CGEM, aventi capacità individuale superiore a 3.000 litri per unità di trasporto (di qualunque massa), che trasportano esplosivi in quantità superiore ai limiti di esenzione di ADR (di qualunque massa), che trasportano materiali radioattivi, esclusi i colli esenti. Per il trasporto di colli di tipo A (ONU 2915 e 3332), se il loro numero non supera 10 e l'indice di trasporto totale è inferiore a 3, è sufficiente un certificato del datore di lavoro attestante che il conducente è stato adeguatamente sensibilizzato sui pericoli delle radiazioni connessi al trasporto
- con altri mezzi, aventi massa complessiva superiore a 3,5 t e che trasportano materie in quantitativi superiori ai limiti di esenzione di ADR.

Più da vicino, il certificato di formazione professionale (*CFP)* per conducenti è costituito da:

- un'abilitazione di base per il trasporto in colli e alla rinfusa, superiori ai limiti di esenzione, esclusi esplosivi e radioattivi;
- tre abilitazioni di specializzazione, conseguibili solo dopo aver superato l'esame relativo al corso base, per il trasporto di merci: in cisterne, della classe 1 (eccetto esplosivi 1.4 S), della classe 7 (radioattivi).

Di estrema importante in materia anche la figura del *Consulente ADR,* tenuto conto che nell'accordo ADR è disposto: «*ogni impresa, la cui attività comporta trasporti di merci pericolose, oppure operazioni di imballaggio, di carico, di riempimento o di scarico, connesse a tali trasporti, designa uno o più consulenti per la sicurezza dei trasporti di merci pericolose, in seguito denominati «consulenti», incaricati di facilitare l'opera di prevenzione dei rischi per le persone, per i beni o per l'ambiente inerenti a tali attività».*

La figura del "Consulente ADR" (*consulente per la sicurezza dei trasporti di merci pericolose*) è nata con la direttiva CE 96/35 ed è stata recepita in Italia con il D.Lgs 4 febbraio 2000 n. 40 (*Attuazione della direttiva 96/35/CE relativa alla designazione e alla qualificazione professionale dei consulenti per la sicurezza dei trasporti su strada, per ferrovia o per via navigabile di merci pericolose*), poi sostituito dal D.Lgs. 27 gennaio 2010 n. 35, il cui articolo 4 (*Obblighi del consulente*) dispone:

«1. Il consulente, in seguito alla verifica delle prassi e delle procedure indicate nell'allegato I, redige una relazione nella quale, per ciascuna operazione relativa all'attività dell'impresa, indica

le eventuali modifiche procedurali ovvero strutturali necessarie per l'osservanza delle norme in materia di trasporto, di carico e scarico di merci pericolose nonchè per lo svolgimento dell'attivita' dell'impresa in condizioni ottimali di sicurezza.

2. Il consulente redige la relazione di cui al comma 1 annualmente e ogni qualvolta intervengano eventi modificativi delle prassi e delle procedure poste alla base della relazione stessa ovvero delle norme in materia di trasporto, carico e scarico di merci pericolose.

3. Il consulente consegna la relazione di cui al comma 1 al capo dell'impresa.

4. Quando nel corso di un trasporto ovvero di una operazione di carico o scarico si sia verificato un incidente che abbia recato pregiudizio alle persone, ai beni o all'ambiente, il consulente, dopo aver raccolto tutte le informazioni utili, provvede alla redazione di una relazione d'incidente.

5. La relazione di cui al comma 4 e' trasmessa al capo dell'impresa e, per il tramite degli uffici provinciali della motorizzazione civile e dei trasporti in concessione, al Ministero dei trasporti e della navigazione - Dipartimento dei trasporti terrestri».

Considerata la delicatezza delle sue funzioni, l'art. 5 del succitato D.Lgs.40/2000, sostituito dal D.Lgs.35/2000 dispone in ordine alla "Qualificazione dei consulenti": «*1. Il consulente deve avere una conoscenza sufficiente dei rischi inerenti il trasporto e le operazioni di carico e scarico di merci pericolose e delle disposizioni normative vigenti in materia, nonché dei compiti definiti nell'allegato I, e deve possedere un certificato di formazione professionale rilasciato dal Ministero dei trasporti e della navigazione - Dipartimento dei trasporti terrestri, a seguito del superamento di un apposito esame*».

In chiave di *dimensionamento aziendale, ADR Trasporti S.R.L.* conta attualmente circa 62 dipendenti ed utilizza circa 35 autoveicoli.

La clientela è costituita da società che svolgono attività di natura privatistica.

Per incidens: in parallelo all'attività di trasporto, la Società gestisce anche l'importante settore aziendale dedicato al modernissimo *impianto di lavaggio per bonifica cisterne*, realizzato con testine rotanti e caldaie per la produzione di acqua ad alta temperatura.

Dal punto di vista logistico, la sede legale ed operativa della Società, è ubicata in Catania Via A. Pittari s.n. (Z.I.), all'interno di un complesso immobiliare dotato di officine ed uffici, oltre che di magazzino ed area mensa.

A breve, è prevista l'inaugurazione del cd. *Terminal Intelligente* (unicum nel territorio siciliano), per il quale la Società ha avviato il processo per ottenere l'autorizzazione provinciale per la messa in riserva di rifiuti liquidi in cisterna, pericolosi e non, all'interno del terminal di seguito descritto, con l'obiettivo di di implementare il servizio di movimentazione e di stoccaggio dei tank container di merce pericolosa e non.

L'idea imprenditoriale consiste nella creazione di un nuovo piazzale (Terminal) all'interno di un lotto di terreno esistente nel territorio del Comune di Catania**,** Zona Industriale a 300 metri dallo Scalo Ferroviario, per aumentare lo spazio di operatività e ampliare l'offerta di servizi ai clienti attuali e futuri.

Tale terminal, della superficie di circa 15.000 mq**,** permetterà ai clienti della Società di poter sostare le cisterne/tank contenenti i loro prodotti, pericolosi e non.

A tal fine, il Terminal garantirà, sia per questioni di sicurezza sia per questioni di trasparenza, la possibilità di poter verificare tramite una *Pesa Certificata ed Omologata***,** posta all'ingresso del terminal, il peso del prodotto dopo lo scarico o il carico.

Il suddetto terminal potrà contenere circa 330 tank e un centinaio di cisterne.

Va da sé che l'elevato numero di mezzi in sosta sul piazzale richiederà un sistema di sicurezza e videosorveglianza elevato ad avanzata tecnologia, nonché di un sistema di controllo, da remoto, della condizione dei singoli mezzi, oltre che della segnalazione di eventuali problematiche che potrebbero rilevarsi al suolo (alert per un eventuale sversamento di materiale), così da potersi tempestivamente attivare per il contenimento delle eventuali perdite.

Sul piano pratico, si prevede:

- che in detto piazzale sia realizzato un pavimento industriale che sarà atto ad impedire che eventuali sversamenti possano causare dispersione nell'ambiente;
- che ogni stallo per automezzo abbia una dimensione di mt.20.00 x 3.00 e sia realizzato con una pendenza tale da poter far defluire, nelle vasche di depurazione, i liquidi nel minor tempo possibile;
- che, tramite la tecnologia di un sistema intelligente, il depuratore metta in quarantena tutto quello che non potrà depurare, come ad esempio i prodotti ad alta concentrazione, i quali verranno a loro volta smaltiti presso centri di recupero o di smaltimento autorizzati;
- che l'impianto possa contenere, senza problemi, lo sversamento contemporaneo di un consistente numero di tank;
- che - a rafforzare la sicurezza all'interno del terminal - siano allocate sei vasche di contenimento, progettate e realizzate per contenere, in caso di sversamento, i tank danneggiati.
- che, attraverso una *reach stacker* di nuova tecnologia e grazie al sistema avanzato di sensori di cui sarà dotato il terminal e con l'aiuto della domotica, siano generati diversi alert di rilevamento di liquidi diversi dalle acque meteoriche;
- che l'operazione di spostamento dei tank danneggiati all'interno delle vasche di contenimento sia effettuato dal personale qualificato preposto, nel minor tempo possibile;
- che le linee di alimentazione elettrica dell'impianto di depurazione siano indipendenti rispetto all'impianto elettrico generale, in quanto il funzionamento del depuratore è distribuito 24 ore/giorno e su 7 giorni/settimana;
- che tutte le giunzioni tra vasche e pozzetti**,** nonché tutte le tubazioni e qualsiasi altro elemento di collegamento ad essi abbinato, siano sigillate a perfetta tenuta idraulica;
- che l'impianto di trattamento riceva le acque provenienti dal lotto in oggetto mediante la condotta collegata ad un sistema generale di canalette e condotte posizionate sul piazzale generale;
- che il piazzale sia livellato con pendenze verso il centro baricentrico dell'area, mediante una pendenza adeguata, la quale verrà delineata in fase di realizzazione del massetto rifinito con pavimentazione industriale.

1.3. Abilitazioni, Classificazioni, Qualificazioni e Certificazioni

ADR Trasporti SRL è abilitata ad effettuare trasporti in ADR per tutte le succitate classi richiamate al precedente punto sub 1.2., tranne che per la Classe 1 (*Materiali e sostanze esplosive*) e la Classe 7 (*Materiali radioattivi*).

Tutti i veicoli di ADR sono, quindi, regolarmente muniti del *Barrato rosa* (v. il "certificato di approvazione per i veicoli che trasportano alcune merci pericolose" rilasciato dal Ministero delle Infrastrutture e della mobilità sostenibili) e tutti gli autisti sono regolarmente in possesso del *Patentino ADR*.

Si riportano di seguito le ulteriori, specifiche, connotazioni aziendali.

Abilitazioni:

- Albo Nazionale persone fisiche e giuridiche trasporto conto terzi al n° CT/8708151/T.
- Albo Nazionale Gestori Ambientali (PA008883): Cat. 4 (*Raccolta e trasporto di rifiuti speciali non pericolosi*), Classe c; Cat. 5 (*Raccolta e trasporto di rifiuti pericolosi*), Classe c.
- Posizione meccanografica d'archivio EoMJ7R.
- Licenza Europea CEE n°00066701 per trasporto internazionale di merci su strada conto terzi.
- Autorizzazione Regione Sicilia per trasporto merci in categoria 4-5 C.
- Iscrizione PA 08883.

Classificazioni ATECORI:

- 49.41 (*Trasporto di merci su strada*)
- 43.12 (*Preparazione del cantiere edile e sistemazione del terreno*)
- 45.20.1 (*Riparazioni meccaniche di autoveicoli*)
- 45.20.2 (*Riparazione di carrozzerie di autoveicoli*)
- 45.20.3 (*Riparazione di impianti elettrici e di alimentazione per autoveicoli*)
- 45.20.91 (*Lavaggio autoveicoli*)
- 81.29.99 (*altre attività di pulizia nca*)

Certificazioni:

- **Rating di legalità**: ***
- **UNI EN ISO 9001: 2015**, per le attività di "*Trasporto per conto terzi di merci varie, di materia pericolosa classificata ADR e di rifiuti speciali pericolosi e non pericolosi. Servizi di lavaggio e bonifica di veicoli cisterna e di contenitori industriali".*
- **UNI EN ISO 14001: 2015**, per le attività di "*Trasporto per conto terzi di merci varie, di materia pericolosa classificata ADR e di rifiuti speciali pericolosi e non pericolosi. Servizi di lavaggio e bonifica di veicoli cisterna e di contenitori industriali".*
- **UNI ISO 45000: 2018**, per le attività di "*Trasporto per conto terzi di merci varie, di materia pericolosa classificata ADR e di rifiuti speciali pericolosi e non pericolosi. Servizi di lavaggio e bonifica di veicoli cisterna e di contenitori industriali".*
- **ISO 37001:2016,** per le attività di "*Trasporto per conto terzi di merci varie, di materia pericolosa classificata ADR e di rifiuti speciali pericolosi e non pericolosi. Servizi di lavaggio e bonifica di veicoli cisterna e di contenitori industriali".*

Le succitate certificazione si intendono integralmente richiamate nel presente Modello, anche al fine di poterle eventualmente sottoporre al raggio di vigilanza dell'OdV.

Per ciò che riguarda lo specifico **Sistema di Gestione 37001:2016** inoltre, oltre al suo richiamo integrale nel presente Modello, è **in fase di programmazione l'attività di coordinamento diretto tra l'Organismo di Vigilanza 231 e la Funzione di Conformità 37001:2016.**

Sistema Gestionale SQAS:

ADR Trasporti S.R.L. adotta il Sistema Gestionale SQAS: n. 1610032135 per il Trasporto; n. 1578922912 per il Lavaggio.

Il sistema SQAS (Safety and Quality Assessment System) nasce nel 1990 su iniziativa di CEFIC - European Chemical Industry Council, nell'ambito del programma Responsible Care, con lo scopo di migliorare il livello di sicurezza durante il trasporto, lo stoccaggio e la gestione di sostanze particolarmente a rischio quali sono i prodotti chimici.

Si tratta di un sistema di valutazione delle performance ambientali, di sicurezza e qualità dei Fornitori di servizi logistici alle Aziende Chimiche**.**

Da chiarire che SQAS non è una certificazione, ma un sistema per monitorare i fornitori di servizi logistici in maniera indipendente e armonizzata, in modo da garantire uniformità di valutazione a tutti i livelli, la verifica infatti è sempre condotta da auditor indipendenti, riconosciuti e qualificati.

La validità dell'Assessment SQAS è triennale, ma viene lasciata facoltà alle aziende di richiedere verifiche intermedie aggiuntive, parziali, per attestare i miglioramenti ottenuti su specifiche aree che avessero avuto valutazione non soddisfacente.

2. GESTIONE DEL RISCHIO DA REATI PRESUPPOSTI

2.1. Mappatura rischi dai *reati presupposti*

Come chiarito nella Parte I, i due momenti fondamentali per la predisposizione di un buon Modello di Organizzazione, Gestione e Controllo, ex D.Lgs. 231/2001 sono:

a) la **"*mappatura dei rischi di reato*"** (***Crime Risk Assessment***);
b) la "***gestione del rischio di reati***" (**Crime Risk Management**).

Premessa metodologica di primario rilievo è che la generica nozione di *risk assessment* (o *analisi del rischio*) comunemente usata in campo aziendale è assolutamente aspecifica atteso che individua la ricerca di tutti i possibili rischi che possono derivare dall'esercizio di una determinata attività, in base alle peculiari aree di attività o di produzione cui si riferiscono (v. ad es.: *"rischio di scadenza e deterioramento",* in relazione ai prodotti di una azienda alimentare; *"rischio di inquinamento da scarico",* avuto riguardo alle movimentazioni portuali di una compagnia petrolifera; *"rischio di sovraccarico di magazzino",* per una società che si occupa di stoccaggio; "*rischio di piccoli furtidei prodotti in scaffale*" nella gestione di un supermercato; "*rischio di avvelenamento chimico"*in una una società farmaceutica; "*rischio infortunistico*", all'interno di tutti i posti di lavoro; e così via in un elenco tendenzialmente indefinibile).

La nozione di *"crime risk assessment"* individua - invece e con esattezza - lo specifico raggio di azione cui sono rivolti la *mappatura* e l'*analisi dei rischi di natura penale,* ovvero lo specifico "*rischio di commissione di reati*" (*rectius*, dei reati esattamente indicati dal Legislatore e rientranti nella categoria dei *reati presupposti*).

In relazione a tali reati, il Legislatore chiede agli enti destinatari del D.Lgs. 231/2001 una attività di razionale *prevenzione*.

Del resto, sia il Decreto Legislativo 231/2001 che la Legge 190/2012 (entrambi presupposti logico-normativi del "nostro" Modello 231), sono provvedimenti legislativi emessi allo specifico scopo di prevenire i *reati* e le *condotte illecite.*

Avuto riguardo alle specifiche modalità di individuazione *del rischio di reati*– ossia la corretta effettuazione della fase di "*crime risk assessment",* propedeutica alla fase di "*crime risk management"* – è doveroso chiarire *come*, concretamente, è stata condotta tale fase e la correlata *mappatura del rischio di reati*.

Va chiarito sul punto che una delle possibili modalità di effettuazione di tale analisi è quella della "*mappatura dei processi"* o della "*individuazione dei processi a rischio"*.

Ciò dipende dal fatto che qualunque attività aziendale è costituita da un insieme di *processi*[15] tra loro interrelati.

Va, tuttavia, chiarito che la ricerca dei rischi di reato non si muove, necessariamente, nell'ambito dei *processi*, potendo essere utilmente effettuata anche in relazione alle *funzioni* (quale criterio di raggruppamento degli organi aziendali in unità organizzative) o alle *aree di attività*.

[15] Per "*processo*" si intende qualsiasi porzione dell'attività aziendale (amministrativa o societaria, pubblica o privata) che si sviluppi per azioni ed attraverso funzioni aziendali correlate tra di loro in un sistema organico.

La possibile fungibilità dei predetti concetti e nozioni - *processi, funzioni, aree* - è richiamata anche nelle Linee Guida Confindustria: «*Lo svolgimento di tale fase* (n.d.s. quella del "crime risk assessment") *può avvenire secondo approcci diversi: per attività, per funzioni, per processi. Essa comporta il compimento di una revisione periodica esaustiva della realtà aziendale, con l'obiettivo di individuare le aree che, in ragione della natura e delle caratteristiche delle attività effettivamente svolte, risultano interessate dal potenziale compimento di taluno dei reati contemplati dalla norma».*

Giova, altresì, considerare che, nello specifico caso dell'attività amministrativa pubblica (con la quale l'attività aziendale potrebbe eventualmente impattare), si preferisce utilizzare il termine di "*procedimento",* cui è correlata l'unità organizzativa affidata ad un *responsabile*[16]*.*

Nella legislazione anticorruzione si parla anche - genericamente - di *"uffici esposti al rischio corruzione*" (v. al citato art. 1, comma 5, Legge 190/2012) o di *"attività"*.

A quest'ultimo proposito, la Legge 190/2012 ad esempio dispone - all'art. 1 comma 53 - che sono *«maggiormente esposte a rischio di infiltrazione mafiosa»* le «*seguenti attività: a) trasporto di materiali a discarica per conto di terzi; b) trasporto, anche transfrontaliero, e smaltimento di rifiuti per conto di terzi; c) estrazione, fornitura e trasporto di terra e materiali inerti; d) confezionamento, fornitura e trasporto di calcestruzzo e di bitume; e) noli a freddo di macchinari; f) fornitura di ferro lavorato; g) noli a caldo; h) autotrasporti per conto di terzi; i) guardiania dei cantieri*»;

Qualunque sia la denominazione utilizzata, è certo che dall'individuazione dei *processi* - o delle *aree*, o delle *funzioni*, o dei *procedimenti*, o delle *attività,* o degli *uffici* – ritenuti maggiormente "a rischio di reato" dovranno scaturire degli *idonei ed efficaci protocolli,* quali modalità di gestione del rischio da svolgersi attraverso *principi ed azioni generali* cui la Società è tenuta ad adeguarsi nella sua operatività quotidiana, se del caso anche attraverso l'ausilio ed il supporto di specifiche procedure *ad hoc*.

A prescindere dalla possibile analisi dei *processi*, delle *funzioni* o delle *attività*, rimane tuttavia fermo che il dato di partenza ai fini di una corretta *mappatura dei rischi da reato* all'interno di una struttura aziendale rimane: l'analisi dei *reati presupposti* nel loro possibile e concreto estrinsecarsi all'interno di una specifica realtà aziendale.

Diventa dunque essenziale stimare la *concreta prevedibilità del rischio da reato* attraverso una lucida analisi delle condotte di reato concretamente consumabili all'interno una determinata area di attività lavorativa, in correlazione: alle eventuali circostanze predisponenti; alle funzioni societarie che sovrintendono quella stessa area; ai relativi processi di lavoro o attività poste in essere.

La corretta mappatura dei reati concretamente consumabili, attraverso prevedibili condotte illecite poste in essere nell'ambito di determinati processi (o aree, o procedimenti, o attività), permetterà di affrontare correttamente: da un lato ed in via propedeutica, la *fase diagnostica* di individuazione di tutti i possibili rischi di reato; dall'altro ed in via consequenziale, la *fase terapeutica* di gestione dello stesso rischio.

[16] Il punto è stato oggetto di disciplina *ad hoc,* ad opera della Legge 7 agosto 1990, n. 241 (*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*), il cui art. 4 ha così statuito: «*le pubbliche amministrazioni sono tenute a determinare per ciascun tipo di procedimento relativo ad atti di loro competenza l'unità organizzativa responsabile della istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale*».

Altro nodo problematico della fase di *crime risk assessment* è quello della correlazione tra *"rischio"* e *"oggetto del rischio".*

Partendo, dunque, dal presupposto che i reati da prendere in considerazione non sono "tutti" i possibili reati esistenti nel sistema penale ma solo i "reati presupposti": la circoscrizione degli specifici reati "a rischio" rappresenta un presupposto logico essenziale al fine di individuare con esattezza l'*oggetto del rischio*, e quindi la conseguente determinazione del processo, o area, o attività *sensibile* (ossia soggetta al "rischio di commissione reato").

In caso contrario – parlare, cioè, di area o di processo *sensibile* senza avere concretamente presente da *cosa*, con esattezza, possa scaturire tale *sensibilità* – la mappatura rimane dichiaratamente astratta e "alla cieca".

Per raggiungere tale risultato, è tuttavia necessario comprendere il livello di *sensibilità* del processo (o dell'area di attività o delle funzioni) rispetto a tutti gli eventuali fattori scatenanti la stessa sensibilità.

Teoricamente, una analitica mappatura dei rischi di reato dovrebbe essere effettuata rapportando - in parallelo - *singolo processo con singolo reato presupposto*.

Ciò però, tenuto conto che i *reati presupposti* dal D.Lgs. 231/2001 e dalla Legge 190/2012 raggiungono la soglia delle centinaia, potrebbe condurre ad un raffronto tra parallelismi multipli non sempre coordinati, o coordinabili, tra di loro.

L'adozione di tale metodologia - che potremmo definire dei "*parallelismi multipli: singolo processo con singolo reato"* - se non adeguatamente corretta attraverso una logica di coordinazione concettuale potrebbe, infatti, finire per diventare poco "ragionevole", atteso che sopprimerebbe uno dei valori salienti della pregevole logica di caratterizzazione giuridica del sistema penale italiano, basato quasi interamente sulle classificazioni familiari: i delitti contro la pubblica amministrazione; i delitti contro il patrimonio; i reati ambientali; i delitti contro la persona; e via di seguito.

Per incidens, la strutturazione delle fattispecie delittuose per tipologie comuni ha lo scopo di fissare razionalmente, all'interno di ogni *famiglia di reati,* regole e principi affini (criteri di competenza, oggetto giuridico sottostante, principi di estrinsecazione della condotta, etc.).

Ciò premesso (v. il su richiamato sistema "ordine concettuale" adottato nel sistema penale), va preso atto che il D.Lgs. 231/2001 ha sovente adottato - a volte senza alcuna giustificazione logica - una collocazione casuale e confusa dei *reati presupposti*.

Si consideri ad esempio:

- che, il reato di *"malversazione a danno dello Stato" ex* art. 316 c.p. e il reato di *"concussione" ex* art.317 c.p. sono stati illogicamente collocati, il primo nell'art. 24 e il secondo nell'art. 25 del D.Lgs. 231/2001, e ciò pur facendo parte della stessa famiglia dei *"Delitti contro la pubblica amministrazione"*;
- che, nel succitato art. 24 del D.Lgs. 231/2001 è stato inserito il reato presupposto di "*truffa in danno dello Stato*" *ex* art. 640 c.p., pur trattandosi di un "*Reato contro il patrimonio*" e non di un *"Delitto contro la pubblica amministrazione*".

Accanto alla constatazione delle richiamate discrasie di natura legislativa si pongono, poi, delle ragioni di doverosa razionalizzazione di un buon Modello 231; *a fortiori* ove si consideri che lo stesso Modello, al di là della sua idoneità a prevenire i reati, non può non rispettare

irrinunciabili principi di ordine sistematico, né può fare a meno di assicurare una efficiente intelligenza organizzativa ed una auspicabile ottimizzazione aziendale.

É, insomma, oggettivamente illogico mappare, in parallelo, ogni singolo processo con ogni singolo reato - afferente, ad esempio,all'uso e all'abuso degli strumenti informatici - laddove gli specifici *reati presupposti* di "natura informatica" sono numero 23 e sono tutti disordinatamente distribuiti tra gli artt. 24-*bis*, 25-*quinquies*, 25-*novies* del D.Lgs. 231/2001.

Maggiormente logico accorpare gli stessi reati informatici, prendendo atto che gli stessi reati sono connessi tra di loro in ragione dello stesso strumento adoperato (computer, software, hardware), dell'analogo uso predisponente l'abuso (utilizzazione computer) e dello stesso titolare della relativa funzione di garanzia (consulenti e collaboratori informatici).

Ne deriva l'opportunità di inquadrare, mappare, valutare e gestire il *processo sensibile* sottostante all'*area risorse informatiche* - normalmente affidato alla stessa funzione aziendale – attraverso la preliminare riunione logica di tutti i reati cd. informatici inseriti nel D.Lgs. 231/2001: r*eati contro il patrimonio commessi mediante l'uso del mezzo informatico* presupposti dall'art. 24-*bis; reati lato sensu informatici,* presupposti dallo stesso art. 24-*bis* ma facenti parte di altra famiglia penalistica; *reati a mezzo web contro la personalità individuale,* presupposti dall'art. 25-*quinquies;* reati che derivano dalla *violazione del diritto di autore* (presupposti dall'art. 25-*novies*).

Da qui, l'esigenza di *riordinare* – alla stregua di punto di riferimento da cui partire ai fini della analisi e valutazione del concreto rischio di verificazione di reato all'interno di determinate aree o processi aziendali – il *corredo normativo presupposto*, ovvero tutti i *reati presupposti* dal D.Lgs. 231/2001, attraverso una risistemazione logica aderente, sia alla loro specifica natura penalistica, sia al raggio di azione societario entro cui possono muoversi.

In altri termini, diventa strategicamente necessario procedere ad una operazione di riordino logico della normativa di cui si chiede la *non* violazione, accorpando in aree comuni tutti i "reati presupposti" connessi per raggio di azione e similitudini giuridiche.

Tale quadro normativo - che, alla fine, altro non è se non il riordino concettuale di quanto prescritto dal D.Lgs. 231/2001 o dalla Legge 190/2012 – diventerà il *riferimento universale* delle specifiche illiceità penali di cui si chiede la prevenzione, ovvero la causa normativa produttiva della "sensibilità" dei processi di lavoro.

Sulla base di queste premesse logiche, la metodologia di *crime risk assessment* adottata nel presente Modello 231 è condotta attraverso due diversi momenti:

A) *Individuazione delle macro aree normative,* ovvero individuazione e accorpamento sistematico dei reati presupposti in base agli elementi di reciproca assonanza logico-giuridica, attraverso le quali - *in via deduttiva* - si individueranno le tipologie dei reati presupposti, riunificati per "famiglie" e classificazioni omogenee;

Analisi di reati e condotte, attraverso la quale - *in via induttiva* – si valuterà ogni singolo reato presupposto, sia dal punto di vista della sua formalità normativa che in relazione a *come* lo stesso potrebbe concretamente essere consumato, *perché* e *da parte di chi.* In tale sottofase sarà anche effettuata una *stima della probabilità e della gravità del rischio,* utilizzando la metodologia suggerita dalla norma UNI ISO 31000:2018 (La *Norma ISO 31000:2018 e la Mappatura e Gestione dei rischi* sono riportate in Allegato 3).

Si riportano di seguito le *macro aree normative utilizzate ai fini della mappatura*, ovvero quelle in cui possono logicamente riunirsi tutte le fattispecie normative presupposte che si prestino ad essere analizzate attraverso criteri esegetici comuni e situazioni normative analoghe, nonché ad essere prevenibili utilizzando la stessa tipologia di protocolli e regole procedurali:

- ❒ Area Reati contro la Pubblica Amministrazione
- ❒ Area Reati contro il Patrimonio della Pubblica Amministrazione
- ❒ Area Rapporti con il Mercato Privato
- ❒ Area a Rischio di commissione Reati contro la Fede Pubblica, l'Ordine Pubblico, l'Ordine Democratico, gli interessi dello Stato
- ❒ Area Finanza e Contabilità
- ❒ Area Risorse Umane
- ❒ Area Gestione Risorse Informatiche
- ❒ Area Sicurezza Lavoratori
- ❒ Area Reati Ambientali
- ❒ Area Reati contro il Patrimonio Culturale

➢ Macro aree normative e reati presupposti

Area Reati contro la Pubblica Amministrazione

Queste le specifiche fattispecie delittuose presupposte dal D.Lgs. 231/2001:

- *art. 314, I comma, c.p. - peculato: reato presupposto dall'art. 25 [*reato rilevante ex D.Lgs. 231/2001 se *"il fatto offende gli interessi finanziari dell'Unione europea"]*
- *art. 316 c.p - peculato mediante profitto dell'errore altrui: reato presupposto dall'art. 25 [*reato rilevante ex D.Lgs. 231/2001 se *"il fatto offende gli interessi finanziari dell'Unione europea"]*
- *art. 316 bis c.p. - malversazione di erogazioni pubbliche: reato presupposto dall'art. 24;*
- *art. 316 ter c.p.- indebita percezione di erogazioni pubbliche: reato presupposto dall'art. 24;*
- *art. 317 c.p. - concussione: reato presupposto dall'art. 25;*
- *art. 318 c.p. - corruzione per un atto d'ufficio: reato presupposto dall'art. 25;*
- *art. 319 c.p. - corruzione per un atto contrario ai doveri di ufficio: reato presupposto dall'art. 25;*
- *art. 319 ter c.p. - corruzione in atti giudiziari: reato presupposto dall'art. 25;*
- *art. 319 quater - induzione indebita a dare o promettere utilità: reato presupposto dall'art. 25;*
- *art. 320 - corruzione di persona incaricata di un pubblico servizio: reato presupposto dall'art. 25;*
- *art. 322 c.p. - istigazione alla corruzione: reato presupposto dall'art. 25;*
- *art. 322 bis c.p. - peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri: reato presupposto dall'art. 25;*

- *art. 323 c.p. - abuso di ufficio: reato presupposto dall'art. 25 [*reato rilevante ex D.Lgs. 231/2001 se *"il fatto offende gli interessi finanziari dell'Unione europea"];*
- *art. 346 bis c.p. – traffico di influenze illecite*: *reato presupposto dall'art. 25;*
- *art. 353 c.p. – turbata libertà degli incanti: reato presupposto dall'art. 24;*
- *art, 353 bis c.p. – turbata libertà del procedimento di scelta del contraente: reato presupp. art. 24;*
- *art. 356 c.p. - frode nelle pubbliche forniture: reato presupposto dall'art. 24.*

Area Reati contro il Patrimonio della Pubblica Amministrazione

A differenza che per la categoria di cui sopra, i delitti in oggetto presuppongono una condotta delittuosa che abbia ad oggetto, da un lato il perseguimento di un profitto patrimoniale in capo al soggetto agente, dall'altro il correlativo danno in capo alla pubblica amministrazione, quale persona offesa.

I reati inquadrabili in questa categoria sono:

- *art. 640 c.p. - truffa in danno dello Stato: reato presupposto dall'art. 24;*
- *art. 640 bis c.p. - truffa aggravata per il conseguimento di erogazioni pubbliche: reato presupposto dall'art. 24.*

Area Reati contro il Mercato Privato

Viene utilizzato il termine "*rapporti con il mercato privato*" per distinguere questa macro area da quella riguardante i sopra evidenziati rapporti con la pubblica amministrazione. In quell'area ricadono tutte le possibili disfunzioni ed illiceità nei rapporti con la pubblica amministrazione. Viceversa, nell'area afferente il cd. libero mercato possono inquadrarsi le attività condotte da *ADR Trasporti S.R.L.* in favore di operatori privati.

Sul piano pratico, si tratta di un'area poco riferibile alla Società, considerato che i reati in questione presuppongono l'esercizio di una attività diretta ad una produzione industriale o ad una attività commerciale, e non già a quella di prestazione di servizi pubblici concretamente effettuata da *ADR Trasporti S.R.L.*.

Le ipotesi delittuose riferibili a questa macro area sono:

- *art. 513 c.p. - turbata libertà dell'industria o del commercio: reato presupposto dall'art. 25 bis.1;*
- *art. 513 bis c.p. - Illecita concorrenza con minaccia o violenza: reato presupposto dall'art. 25 bis.1;*
- *art. 514 c.p. - frodi contro le industrie nazionali: reato presupposto dall'art. 25 bis.1;*
- *art. 515 c.p. - frode nell'esercizio del commercio: reato presupposto dall'art. 25 bis.1;*
- *art. 516 c.p. - vendita di sostanze alimentari non genuine come genuine: reato presupposto dall'art. 25 bis.1;*
- *art. 517 c.p. - vendita di prodotti industriali con segni mendaci: reato presupposto dall'art. 25 bis.1;*
- *art. 517 ter c.p. - fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale: reato presupposto dall'art. 25 bis.1;*
- *art. 517 quater c.p. - contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari: reato presupposto dall'art. 25 bis.1*

Area a Rischio di commissione Reati contro la Fede Pubblica, l'Ordine Pubblico, l'Ordine Democratico, gli interessi dello Stato.

Possono sinteticamente includersi ed accorpare in questa area generale - considerabile a mero "rischio teorico" di illegalità in vista di come concretamente opera *ADR TRASPORTI SRL* - tutte quelle situazioni limite che il Legislatore del 2001 ha, comunque, voluto inserire nella previsione di condotte criminogenetiche astrattamente verificabili all'interno di strutture aziendali complesse.

É un'area che, sul piano strettamente pratico, viaggia in parallelo con quella delle Risorse Umane, intendendo per essa il settore che sovrintende alla selezione ed al controllo, anche strettamente personale, dei soggetti che operano con e per ADR SRL.

I reati presupposti in connessione con questa macro area sono quelli:

Contro la Fede Pubblica:

- *art. 453 c.p. - falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate: reato presupposto dall'art. 25 bis;*
- *art. 454 c.p. - alterazione di monete: reato presupposto dall'art. 25 bis;*
- *art. 455 c.p. - spendita e introduzione nello Stato, senza concerto, di monete falsificate: reato presupposto dall'art. 25 bis;*
- *art. 457 c.p. - spendita di monete falsificate ricevute in buona fede: reato presupposto dall'art. 25 bis;*
- *art. 459 c.p. - falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati: reato presupposto dall'art. 25 bis;*
- *art. 460 c.p. - contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo: reato presupposto dall'art. 25 bis;*
- *art. 461 c.p. - fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata: reato presupposto dall'art. 25 bis;*
- *art. 464 c.p. - uso di valori bollati contraffatti o alterati: reato presupposto dall'art. 25 bis;*
- *art. 473 c.p. - Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni: reato presupposto dall'art. 25 bis *;*
- *art. 474 c.p. - Introduzione nello Stato e commercio di prodotti con segni falsi: reato presupposto dall'art. 25 bis *.*

* I due ultimi articoli 473 e 474 c.p. – caratterizzati da una giuridica "*plurioffensività*" - ai fini dell'*analisi delle condotte* sono stati funzionalmente inseriti nell'*Area contro la fede pubblica.*

Contro l'Ordine Pubblico:

- *art. 416 c.p. - associazione per delinquere: reato presupposto dall'art. 24 ter;*
- *art. 416 bis c.p. - associazioni di tipo mafioso: reato presupposto dall'art. 24 ter;*
- *art. 416 ter c.p. - scambio elettorale politico mafioso: reato presupposto dall'art. 24 ter;*
- *art. 630 c.p. - sequestro di persona a scopo di estorsione: reato presupposto dall'art. 24 ter;*
- *art. 74 D.P.R. 9.10.1990 n. 309 - associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope: reato presupposto dall'art. 24 ter.*

Contro l'Ordine Democratico:

Sono idonei a rientrare nel raggio di applicazione di tale norma tutti i delitti *"aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal Codice Penale e dalle leggi speciali*".

È una categoria normativa aperta che, oltre alle disposizioni di legge previste nel Libro II, Titolo I, Capo I, II, III, IV e V, del Codice Penale - articoli dal 241 al 307 c.p. - si ritiene altresì comprensiva della relativa legislazione speciale.

- *Attentati contro l'integrità, l'indipendenza e l'unità dello Stato (art. 241 c.p.);*
- *Cittadino che porta le armi contro lo Stato italiano (art. 242 c.p.);*
- *Intelligenze con lo straniero a scopo di guerra contro lo Stato italiano (art. 243 c.p.);*
- *Atti ostili verso uno Stato estero, che espongono lo Stato italiano al pericolo di guerra (art. 244 c.p.);*
- *Intelligenze con lo straniero per impegnare lo Stato italiano alla neutralità o alla guerra (art. 245 c.p.);*
- *Corruzione del cittadino da parte dello straniero (art. 246 c.p.);*
- *Favoreggiamento bellico (art. 247 c.p.);*
- *Somministrazione al nemico di provvigioni (art. 248 c.p.);*
- *Partecipazione a prestiti a favore del nemico (art. 249 c.p.);*
- *Commercio col nemico (art. 250 c.p.);*
- *Inadempimento di contratti di forniture in tempo di guerra (art. 251 c.p.);*
- *Frode in forniture in tempo di guerra (art. 252 c.p.);*
- *Distruzione o sabotaggio di opere militari (art. 253 c.p.);*
- *Agevolazione colposa (art. 254 c.p.);*
- *Soppressione, falsificazione o sottrazione di atti o documenti concernenti la sicurezza dello Stato (art. 255 c.p.);*
- *Procacciamento di notizie concernenti la sicurezza dello Stato (art. 256 c.p.);*
- *Spionaggio politico o militare (art. 257 c.p.);*
- *Spionaggio di notizie di cui è stata vietata la divulgazione (art. 258 c.p.);*
- *Agevolazione colposa (art. 259 c.p.);*
- *Introduzione clandestina in luoghi militari e possesso ingiustificato di mezzi di spionaggio (art. 260 c.p.);*
- *Rivelazione di segreti di Stato (art. 261 c.p.);*
- *Rivelazione di notizie di cui sia stata vietata la divulgazione (art. 262 c.p.);*
- *Utilizzazione dei segreti di Stato (art. 263 c.p.);*
- *Infedeltà in affari di Stato (art. 264 c.p.);*
- *Disfattismo politico (art. 265 c.p.);*
- *Istigazione di militari a disobbedire alle leggi (art.266 c.p.);*
- *Disfattismo economico (art. 267 c.p.);*
- *Associazioni sovversive (art. 270 c.p.);*
- *Associazioni con finalità di terrorismo anche internazionale o di eversione dell'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.);*
- *Finanziamento di condotte con finalità di terrorismo (art. 270 quinquies.1 c.p.)*
- *Sottrazione di beni o denaro sottoposti a sequestro (art. 270 quinquies.2 c.p.)*
- *Condotte con finalità di terrorismo (art.270 sexies c.p.);*
- *Associazioni antinazionali (art. 271 c.p.);*
- *Propaganda ed apologia sovversiva o antinazionale (art. 272 c.p.);*
- *Attentato contro il Presidente della Repubblica (art. 276 c.p.);*
- *Offesa alla libertà del Presidente della Repubblica (art. 277 c.p.);*
- *Offesa all'onore o al prestigio del Presidente della Repubblica (art. 278 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.);*
- *Atti di terrorismo nucleare (art. 280 ter c.p.)*
- *Attentato contro la Costituzione dello Stato (art. 283 c.p.);*
- *Insurrezione armata contro i poteri dello Stato (art. 284 c.p.);*
- *Devastazione, saccheggio e strage (art. 285 c.p.);*
- *Guerra civile (art. 286 c.p.);*
- *Usurpazione di potere politico o di comando militare (art. 287 c.p.);*
- *Arruolamenti o armamenti non autorizzati a servizio di uno Stato estero (art. 288 c.p.);*
- *Attentato contro organi costituzionali e contro le assemblee regionali (art. 289 c.p.);*
- *Sequestro di persona a scopo di terrorismo o di eversione (art. 289 bis c.p.);*
- *Sequestro di persona a scopo di coazione (art. 289 ter c.p.)*
- *Vilipendio della Repubblica, delle Istituzioni costituzionali e delle Forze Armate (art.290 c.p.);*
- *Vilipendio alla nazione italiana (art. 291 c.p.);*
- *Vilipendio o danneggiamento alla bandiera o altro emblema dello Stato (art. 292 c.p.);*
- *Attentati contro i diritti politici del cittadino (art. 294 c.p.);*
- *Attentato contro i Capi di Stato Eteri (art. 295 c.p.);*
- *Offesa alla libertà dei Capi di Stato Esteri (art. 296 c.p.);*
- *Offesa alla bandiera o altro emblema di uno stato estero (art. 299 c.p.);*
- *Istigazione a commettere alcuno dei delitti preveduti dai capi primo e secondo (art. 302 c.p.);*
- *Cospirazione politica mediante accordo (art. 304 c.p.);*
- *Cospirazione politica mediante associazione (art.305 c.p.);*
- *Banda armata: formazione e partecipazione (art. 306 c.p.);*
- *Assistenza ai partecipi di cospirazione e banda armata (art. 307 c.p.).*

Area Finanza e Contabilità

Sono logicamente inerenti a questa specifica area di rischio:

- **Le condotte illecite descritte nei Reati Societari**

  Sono i reati previsti dal codice civile e presupposti dall'art. 25 ter del D.Lgs. 231/2001.

Le condotte di cui si parla - sia delittuose che contravvenzionali - sono direttamente legate alla gestione della contabilità Societaria, della redazione dei bilanci e della eventuale manipolazione dei relativi dati.

Queste le ipotesi richiamate dal Legislatore del 2001 ed attualmente vigenti:

- *False comunicazioni sociali (art. 2621 c.c.);*
- *False comunicazioni sociali delle società quotate (art. 2622 c.c.);*
- *Impedito controllo (art. 2625, comma 2, c.c.);*
- *Indebita restituzione dei conferimenti (art. 2626 c.c.);*
- *Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.);*
- *Illecite operazioni sulle azioni o quote sociali o della Società controllante (art. 2628 c.c.);*
- *Operazioni in pregiudizio dei creditori (art. 2629 c.c.);*
- *Omessa comunicazione del conflitto di 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.);*
- *Corruzione tra privati (art. 2635 c.c.);*
- *Istigazione alla corruzione tra privati (art. 2635 bis 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).*

➢ **Le due fattispecie di reato previste dal Decreto legislativo 24 febbraio 1998 n. 58, meglio conosciuto come Testo Unico delle disposizioni in materia di intermediazione Finanziaria**

A differenza che nei reati societari - la cui *ratio* prescrittrice e sanzionatrice è soprattutto diretta alla salvaguardia dei soggetti pubblici e privati direttamente agenti con la Società (v. soci e creditori) - le fattispecie previste dal D.Lgs. 58/1998 hanno prevalentemente di mira la salvaguardia e la genuinità dell'intero sistema finanziario.

Le due specifiche ipotesi normative sono:

- *art. 184 D.Lgs 1998 n. 58 - abuso di informazioni privilegiate: reato presupposto dall'art. 25 sexies;*
- *art. 185 D.Lgs 1998 n. 58 - manipolazione del mercato: reato presupposto dall'art. 25 sexies.*

➢ **Altri reati formalmente inseriti nel codice penale nella parte dei Delitti contro il Patrimonio, o comunque ritenuti dal Legislatore di prevalente rilevanza patrimoniale**

- *art. 648 c.p. – ricettazione: reato presupposto dall'art. 25 octies;*
- *art. 648 bis c.p. – riciclaggio: reato presupposto dall'art. 25 octies;*
- *art. 648 ter c.p. - impiego di denaro, beni o utilità di provenienza illecita: reato presupposto dall'art. 25 octies.*
- *art. 648-ter. 1 c.p. - autoriciclaggio: reato presupposto dall'art. 25 octies;*
- *art. 493 ter c.p. - Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti*: *reato presupposto dal neo art. 25 octies.1;*

- *art. 493 quater c.p. - Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti: reato presupposto dal neo art. 25 octies.1;*
- *art. 512 bis c.p. - Trasferimento fraudolento di valori: reato presupposto dall' art. 25 octies.1;*
- *640 ter c.p. [nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o divaluta virtuale introdotta dal D.Lgs. 184/2021]: reato presupposto dal neo art. 25 octies.1.*

➢ **I "*Reati Tributari*" introdotti dall'art. 39 del D.L. 26 ottobre 2019 n. 124, convertito in Legge 19 dicembre 2019 n. 157.**

I reati tributari ex art. 39 cit. sono quelli previsti dal D.Lgs. 2000, n. 74, aggiornato al D.L. 26 ottobre 2019 n. 124 per come modificato e convertito dalla Legge 19 dicembre 2019, n. 157, ed esattamente:

- *art. 2 - Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti: reato presupposto dall'art. 25 quinquiesdecies;*
- *art. 3 - Dichiarazione fraudolenta mediante altri artifici: reato presupposto dall'art. 25 quinquiesdecies;*
- *art. 8. Emissione di fatture o altri documenti per operazioni inesistenti: reato presupposto dall'art. 25 quinquiesdecies;*
- *art. 10. Occultamento o distruzione di documenti contabili: reato presupposto dall'art. 25 quinquiesdecies;*
- *Art. 11. Sottrazione fraudolenta al pagamento di imposte: reato presupposto dall'art. 25 quinquiesdecies.*

➢ **I "*Reati Tributari*" introdotti dall'art. 5 del D.Lgs. 14 luglio 2020 n. 75**

I reati tributari richiamati dall'art. 5 del D.Lgs.75/2020 - rilevanti ai fini del D.Lgs. 231/2001 solo se se *"commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro"* - sono quelli previsti dal D.Lgs. 2000, n. 74, aggiornato al D.L. 26 ottobre 2019 n. 124 per come modificato e convertito dalla Legge 19 dicembre 2019, n. 157, ed esattamente:

- *art. 4 - Dichiarazione infedele: reato presupposto dall'art. 25 quinquiesdecies;*
- *art. 5 – Omessa dichiarazione: reato presupposto dall'art. 25 quinquiesdecies;*
- *art. 10 quater – Indebita compensanzione: reato presupposto dall'art. 25 quinquiesdecies;*

➢ **I "*Reati di contrabbando*" ex D.P.R. 23 gennaio 1973, n. 43,** *inseriti dall'art. 5 del D.Lgs.* 14 luglio 2020, n. 75 nel nuovo art. 25 *sexiesdecies.*

Area Risorse Umane

La macroarea in oggetto non ha nulla a che vedere con l'ordinaria, e strettamente aziendale, *Area Risorse Umane*. Nell'ottica, infatti, di una mappatura strettamente penalistica dei reati previsti nel D.Lgs. 231/2001, la generica nozione di "Risorse Umane" verrà utilizzata al solo fine di inquadrare e riunire in una stessa famiglia concettuale ipotesi delittuose il cui unico nesso derivativo tra la Società e l'ipotetico fatto criminoso è dato dalla possibile presenza

di un autore materiale del reato che operi "con" e "per" *ADR TRASPORTI SRL*, sia come dipendente che come vertice ed amministratore.

Le condotte illecite di cui si parla sono:

- *art. 583 bis c.p. - pratiche di mutilazione degli organi genitali femminili: reato presupposto dall'art. 25 quater.1;*
- *art. 600 c.p. - riduzione o mantenimento in schiavitù o in servitù: reato presupposto dall'art. 25 quinquies;*
- *art. 600 bis c.p. - prostituzione minorile: reato presupposto dall'art. 25 quinquies;*
- *art. 601 c.p. - tratta di persone: reato presupposto dall'art. 25 quinquies;*
- *art. 602 c.p. - acquisto e alienazione di schiavi: reato presupposto dall'art. 25 quinquies;*
- *art. 603 c.p. - intermediazione illecita e sfruttamento del lavoro: reato presupposto dall'art. 25 quinquies;*
- *art. 604 bis - propaganda e istigazione a delinquere per motivi di discriminazione razziale etica e religiosa;*
- *art. 609-undecies – adescamento di minorenni: reato presupposto dall'art. 25 quinquies;*
- *art. 377 bis c.p. - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria: reato presupposto dall'art. 25 decies;*
- *art. 12, commi 3, 3 bis, 3 ter, 5 del D.Lgs. 25 luglio 1998 n. 286 (Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero) - disposizioni contro le immigrazioni clandestine: reato presupposto dall'art. 25 duodecies;*
- *art. 22, comma 12 bis del D.Lgs. 25 luglio 1998 n. 286 (Testo unico delle disposizioni concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero) - impiego di cittadini di paesi terzi il cui soggiorno è irregolare: reato presupposto dall'art. 25 duodecies;*
- *art. 3, comma 3-bis, della Legge 13 ottobre 1975, n. 654 (Ratifica ed esecuzione della convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale, aperta alla firma a New York il 7 marzo 19669) - razzismo e xenofobia: reato presupposto dall'art. 25-terdecies;*
- *art. 1* (*Frode in competizioni sportive) della Legge 13 dicembre 1989, n. 401* (*Interventi nel settore del giuoco e delle scommesse clandestini e tutela della correttezza nello svolgimento di manifestazioni sportive*) - *reato presupposto dall'art. 25-quaterdecies;*
- *art. 4* (*Esercizio abusivo di attività di giuoco o di scommessa) della Legge 13 dicembre 1989, n. 401* (*Interventi nel settore del giuoco e delle scommesse clandestini e tutela della correttezza nello svolgimento di manifestazioni sportive*) - *reato presupposto dall'art. 25-quaterdecies.*

Area Gestione Risorse Informatiche

Sono idonei a rientrare in questa specifica area di rischio tutte le condotte, circostanze, situazioni ed occasioni in cui vengono utilizzati mezzi e strumenti informatici nella titolarità di *ADR TRASPORTI SRL*.

I reati inquadrabili in questa macro area sono:

A) i reati contro il patrimonio (che dunque presuppongono un evento di danno), commessi mediante l'uso del mezzo informatico

Da notare che la presupposizione operata dal D.Lgs. 231/2001 è solo in relazione alle fattispecie in danno dello Stato o di altro Ente Pubblico: v. il caso emblematico della *frode informatica*, di cui all'art. 640 ter c.p., la cui rilevanza ai fini del Modello di Organizzazione, Gestione e Controllo è unicamente in relazione al II comma (che, appunto, prevede l'alterazione di un sistema informatico o l'intervento sui relativi dati in danno dello Stato o di un altro Ente Pubblico).

I reati in questione sono:

- *art. 635 bis c.p. - danneggiamento di informazioni, dati e programmi informatici: reato presupposto dall'art. 24 bis;*
- *art. 635 ter c.p. - danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità: reato presupposto dall'art. 24 bis;*
- *art. 635 quater c.p. - danneggiamento di sistemi informatici o telematici: reato presupposto dall'art. 24 bis;*
- *art. 635 quinquies c.p.- danneggiamento di sistemi informatici o telematici di pubblica utilità: reato presupposto dall'art. 24 bis;*
- *art. 640 ter c.p. - frode informatica in danno dello Stato o di altro ente pubblico: reato presupposto dall'art. 24;*
- *art. 640 quinquies c.p. - frode informatica del soggetto che presta servizi di certificazione di firma elettronica: reato presupposto dall'art. 24 bis.*

B) i reati accorpabili "lato sensu" come informatici

- *contro l'inviolabilità del domicilio (v. i "reati presupposti" di cui agli artt. 615 ter, quater e quinquies c.p.);*
- *contro l'inviolabilità dei segreti (v. i "reati presupposti" di cui all' art. 617 quater e quinquies c.p.).*

In entrambe le richiamate tipologie normative, oggetto di tutela sono la persona fisica, il suo domicilio fisico e morale, la sua corrispondenza, la sua cerchia di beni e di valori strettamente personale.In questa ottica, l'invasione o l'attacco illecito ad una sfera web è visto come l'ideale esercizio, o prosecuzione, di una aggressione alla persona fisica.

I reati rilevanti in tal senso sono:

- *art. 491 bis c.p. - falsità in un documento informatico pubblico o avente efficacia probatoria: reato presupposto dall'art. 24 bis;*
- *art. 615 ter c.p. - accesso abusivo ad un sistema informatico o telematico: reato presupposto dall'art. 24 bis;*
- *art. 615 quater c.p. - Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici: reato presupposto dall'art. 24 bis;*
- *art. 615 quinquies - Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico: reato presupposto dall'art. 24 bis;*
- *art. 617 quater c.p. - intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche: reato presupposto dall'art. 24 bis;*

- *art. 617 quinquies c.p. - Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire od interrompere comunicazioni informatiche o telematiche: reato presupposto dall'art. 24 bis.*

C) i reati a mezzo web contro la personalità individuale

Sono reati di grande importanza ed allarme sociale, aventi ad oggetto le notorie condotte illecite pedopornografiche o di sfruttamento della prostituzione minorile.

Le ipotesi prese in considerazione dal D.Lgs. 231/2001 sono:

- *art. 600 ter c.p. - pornografia minorile: reato presupposto dall'art. 25 quinquies;*
- *art. 600 quater c.p. - detenzione o accesso di materiale pornografico: reato presupposto dall'art. 25 quinquies;*
- *art. 600 quater.1 c.p. - pornografia virtuale: reato presupposto dall'art. 25 quinquies;*
- *art. 600 quinquies c.p. - iniziative turistiche volte allo sfruttamento della prostituzione minorile: reato presupposto dall'art. 25 quinquies.*

D) i reati previsti dalla Legge 1941 n. 633, così come modificata dalla L. 18 agosto 2000 n. 248

La necessità di prevenire, attraverso specifiche azioni e procedure, tutti i reati previsti dalla Legge 1941 n. 633, così come modificata dalla L. 18 agosto 2000 n. 248, è rivolta alla tutela del "*Diritto di Autore*".

I reati direttamente rilevanti a questo fine sono quelli di cui agli artt. 171, 171-bis, 171-ter, 174-quinquies, 171-septies e 171-octies della succitata Legge 633/1941, modificata dalla L. 248/ 2000.

Le predette violazioni sono presupposte dall'art. 25 novies del D.Lgs. 231/2001.

Area Sicurezza Lavoratori

L'area in oggetto riguarda tutte le possibili condotte illecite dalle quali - attraverso la violazione della legislazione speciale in materia di sicurezza sui luoghi di lavoro (D.Lgs. 9 aprile 2008 n.81 per come integrato e corretto dal D.Lgs. 3 agosto 2009 n. 106) - scaturisca un infortunio, più o meno letale, in danno ad un lavoratore.

I reati presi in esame dal D.Lgs. 231/2001 sono:

- *art. 589 c.p. - omicidio colposo: reato presupposto dall'art. 25 septies;*
- *art. 590 c.p. - lesioni colpose: reato presupposto dall'art. 25 septies.*

Area Reati Ambientali

L'area in oggetto si riferisce:

- alla categoria dei *reati ambientali* inseriti nel D.Lgs. 231/2001 dal D.Lgs. 121/2011;
- alla categoria dei *delitti ambientali* inseriti nel D.Lgs. 231/2001 dalla Legge 68/2015.

Per incidens, il succitato Decreto Legislativo 121/2011 è quello che ha introdotto, per la prima volta nelsistema penale, la denominazione giuridica di "*reati ambientali*".

La Legge 22 maggio 2015 n. 68 ha introdotto, invece, la categoria dei nuovi "*delitti ambientali*", attraverso:

a. l'inserimento, nel codice penale, del *Titolo VI-bis* del *Libro Secondo*, con i correlati artt. 452-*bis* e ss.;
b. l'inserimento, nel D.Lgs. 3 aprile 2006 n. 152, di una nuova *Parte sesta-bis. - Disciplina sanzionatoria degli illeciti amministrativi e penali in materia di tutela ambientale*;
c. la modifica, per integrazione e per sostituzione, dell'art. 25-*undecies*, del D.Lgs. 231/2001.

I reati ambientali "presupposti" dall'art. 25 undecies sono i seguenti:

- *Inquinamento ambientale (art. 452 bis c.p.);*
- *Disastro ambientale (art.452 quater c.p.);*
- *Delitti colposi contro l'ambiente (art. 452 quinquies c.p.);*
- *Traffico e abbandono di materiale ad alta radioattività (art. 452 sexies c.p.);*
- *Circostanze aggravanti (art. 452 octies c.p.);*
- *Attività organizzate per il traffico illecito di rifiuti (art. 452 quaterdecies c.p.);*
- *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.);*
- *I reati previsti dal Decreto Legislativo 3 aprile 2006, n. 152 (Norme in materia ambientale o cd. Codice dell'Ambiente), ed in particolare quelli ex:*
  - *art. 137, commi 2, 3, 5, 11 e 13 (in materia di scarichi di acque reflue industriali);*
  - *art. 256, commi 1, 3, 5 e 6 (Attività di gestione di rifiuti non autorizzata);*
  - *art. 257, commi 1 e 2 (Bonifica dei siti);*
  - *art. 258, commi 4 seconda parte (Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari);*
  - *art. 259 (Traffico illecito di rifiuti);*
  - *art. 260 bis, commi 6, 7 e 8;*
  - *art. 279, comma 5, (in materia di gestione stabilimenti).*
- I reati previsti dalla Legge 7 febbraio 1992 n. 150 *(in materia di commercio internazionale e detenzione di specie animali),* ed in particolare quelli ex:
  - *art. 1, commi 1 e 2 (in materia di importazione ed esportazione specie animali Allegato A);*
  - *art. 2, commi 1 e 2 (in materia di importazione ed esportazione specie animali Allegati B e C);*
  - *art. 6, commi 1 e 4 (in materia di detenzione animali selvatici).*
- I reati del codice penale richiamati dall'art. 3 bis della Legge 7 febbraio 1992 n. 150 (*in materia di commercio internazionale e detenzione di specie animali*), ed in particolare quelli ex:
  - *art. 476 c.p. (Falsità materiale commessa dal pubblico ufficiale in atti pubblici);*
  - *art. 477 c.p. (Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative);*
  - *art. 478 c.p. (Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti);*
  - *art. 479 c.p. (Falsità ideologica commessa dal pubblico ufficiale in atti pubblici);*
  - *art. 480 c.p. (Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative);*

- *art. 481 c.p. (Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità);*
- *art. 482 c.p. (Falsità materiale commessa dal privato);*
- *art. 483 c.p. (Falsità ideologica commessa dal privato in atto pubblico);*
- *art. 484 c.p. (Falsità in registri e notificazioni);*
- *art. 485 c.p. (Falsità in scrittura privata);*
- *art. 486 c.p. (Falsità in foglio firmato in bianco. Atto privato);*
- *art. 487 c.p. (Falsità in foglio firmato in bianco. Atto pubblico);*
- *art. 488 c.p. (Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali);*
- *art. 489 c.p. (Uso di atto falso);*
- *art. 490 c.p. (Soppressione, distruzione e occultamento di atti veri);*
- *art. 491 c.p. (Documenti equiparati agli atti pubblici agli effetti della pena);*
- *art. 491 bis c.p. (Documenti informatici);*
- *art. 492 c.p. (Copie autentiche che tengono luogo degli originali mancanti);*
- *art. 493 (Falsità commesse da pubblici impiegati incaricati di un servizio pubblico).*

▪ I reati previsti dalla Legge 28 dicembre 1993, n. 549 ("*Misure a tutela dell'ozono stratosferico e dell'ambiente*"), ed in particolare quelli ex:

- *art. 3 (Cessazione e riduzione dell'impiego delle sostanze lesive)*

▪ I reati previsti Dlgs. 6 novembre 2007 n. 202 (*Attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni*) ed in particolare quelli ex:

- *art. 9 (Inquinamento colposo);*
- *art. 8 (Inquinamento doloso).*

Area Reati contro il Patrimonio Culturale

I reati inquadrabili in questa macro area sono quelli "presupposti" dagli artt. 25 *septiesdecies* e 25 *duodevicies.*

➢ I reati presupposti dall'art. 25 *septiesdecies (Delitti contro il patrimonio culturale)* sono:

- *Furto di beni culturali (art. 518-bis c.p.);*
- *Appropriazione indebita di beni culturali (art. 518-ter c.p.);*
- *Ricettazione di beni culturali (art. 518-quater c.p.);*
- *Falsificazione in scrittura privata relativa a beni culturali (art. 518-octies c.p.);*
- *Violazioni in materia di alienazione di beni culturali (art. 518-novies c.p.);*
- *Importazione illecita di beni culturali (art. 518-decies c.p.);*
- *Uscita o esportazione illecite di beni culturali (art. 518 -undecies c.p.);*
- *Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici (art. 518-duodecies c.p.);*
- *Contraffazione di opere d'arte (art. 518 -quaterdecies c.p.).*

➢ I reati presupposti dall'art. 25 *duodevicies ((Riciclaggio di beni culturali e devastazione e saccheggio di beni culturali paesaggistici)* sono:

- *Riciclaggio di beni culturali (art. 518-sexies c.p.);*
- *Devastazione e saccheggio di beni culturali e paesaggistici (art. 518- terdecies c.p.).*

2.2. Valutazione e stima del livello di rischio dei reati presupposti

Come già chiarito nel precedente paragrafo, la descrizione delle "*macro aree a rischio*" è stata condotta all'esclusivo scopo di pervenire alla necessaria individuazione e gestione delle *fattispecie legali astratte* di riferimento, attraverso un riordino ed una risistemazione concettuale di tutto il corredo dei *reati presupposti*; ciò, nell'ottica di giungere alla riunificazione logica di fattispecie e categorie delittuose analoghe (spesso disarticolate nell'ambito del D.Lgs. 231/2001) e, dunque, ad una loro migliore analisi, studio e gestione.

Ove, invece, si voglia spostare l'asse di attenzione alle *fattispecie concrete*, ossia alle singole e fattuali condotte aziendali "a rischio" di reati, è opportuno analizzare le singole "*fattispecie delittuose presupposte*".

Le tabelle che seguono - che riportano esclusivamente la magnitudo del rischio relativa ai *reati presupposti* reputati tecnicamente "attinenti" - sintetizzano e riepilogano i risultati ottenuti.

In Allegato 3 è riportata l'analisi dettagliata della valutazione e stima dello specifico *livello di rischio da reati* in *ADR Trasporti S.R.L.* - utilizzando i criteri della succitata UNI ISO 31000:2018 – in base ad ogni singolo *reato presupposto*.

RIEPILOGO
AREA REATI CONTRO LA PUBBLICA AMMINISTRAZIONE
Reati Attinenti

ARTICOLO C.P.	PROBABILITÀ	GRAVITÀ	RISCHIO RESIDUO
Corruzione per un atto d'ufficio - art. 318	Bassa	Alta	RILEVANTE
Corruzione per un atto contrario … - art. 319	Bassa	Alta	RILEVANTE
Corruzione in atti giudiziari - art. 319 ter	Bassa	Alta	RILEVANTE
induzione indebita … - art. 319 quater	Bassa	Alta	RILEVANTE
Istigazione alla corruzione - art. 322	Bassa	Alta	RILEVANTE
Traffico di influenze illecite - art. 346 bis	Molto Bassa	Alta	MEDIO BASSO
Turbata libertà incanti - art. 353	Molto Bassa	Alta	MEDIO BASSO
Turbata libertà proc. scelta … - art. 353 bis	Molto Bassa	Alta	MEDIO BASSO

RIEPILOGO
AREA REATI CONTRO IL PATRIMONIO DELLA PUBBLICA AMMINISTRAZIONE
Reati Attinenti

ARTICOLO C.P.	PROBABILITÀ	GRAVITÀ	RISCHIO RESIDUO
640, comma 2, n. 1 - truffa in danno dello Stato	Bassa	Alta	RILEVANTE

RIEPILOGO
AREA RAPPORTI CON IL MERCATO PRIVATO
Reati Attinenti

ARTICOLO C.P.	PROBABILITÀ	GRAVITÀ	RISCHIO RESIDUO
Turbata libertà dell'industria .. – art. 513	Molto Bassa	Alta	MEDIO BASSO
Illecita concorrenza … - art. 513 bis	Molto Bassa	Alta	MEDIO BASSO

RIEPILOGO
AREA A RISCHIO DI COMMISSIONE REATI CONTRO LA FEDE PUBBLICA, L'ORDINE PUBBLICO, L'ORDINE DEMOCRATICO, GLI INTERESSI DELLO STATO
Reati Attinenti

ARTICOLO C.P.	PROBABILITÀ	GRAVITÀ	RISCHIO RESIDUO
Associazione per delinquere art. 416 c.p.	Molto Bassa	Alta	MEDIO BASSO
Associazioni di tipo mafioso art. 416 bis c.p.	Molto Bassa	Alta	MEDIO BASSO
Scambio elettorale politico … art. 416 ter c.p.	Molto Bassa	Alta	MEDIO BASSO

RIEPILOGO
AREA A RISCHIO DI COMMISSIONE REATI CONTRO LA FEDE PUBBLICA, L'ORDINE PUBBLICO, L'ORDINE DEMOCRATICO, GLI INTERESSI DELLO STATO
Reati Attinenti

ARTICOLO C.P.	PROBABILITÀ	GRAVITÀ	RISCHIO RESIDUO
Associazione per delinquere art. 416 c.p.	Molto Bassa	Alta	MEDIO BASSO
Associazioni di tipo mafioso art. 416 bis c.p.	Molto Bassa	Alta	MEDIO BASSO
Scambio elettorale politico … art. 416 ter c.p.	Molto Bassa	Alta	MEDIO BASSO

RIEPILOGO
AREA FINANZA E CONTABILITÀ
Reati Attinenti

ARTICOLO C.C. - C.P. – D.lgs. 74/2000	PROBABILITÀ	GRAVITÀ	RISCHIO RESIDUO
False comunicazioni sociali - art. 2621 c.c.	Molto Bassa	Alta	MEDIO BASSO
Impedito controllo - art. 2625 c.c.	Molto Bassa	Alta	MEDIO BASSO
Illegale ripartizione utili … – art. 2627 c.c.	Molto Bassa	Alta	MEDIO BASSO
Operazioni in pregiudizio cred. – art. 2629 c.c.	Molto Bassa	Alta	MEDIO BASSO
Formazione fittizia del capitale – art. 2632 c.c.	Molto Bassa	Alta	MEDIO BASSO
Corruzione tra privati - art. 2635 c.c.	Molto Bassa	Alta	MEDIO BASSO

Istigazione alla corruzione - art. 2635 bis c.c.	Molto Bassa	Alta	MEDIO BASSO
Illecita influenza sull'assemblea - art. 2636 c.c.	Molto Bassa	Bassa	TRASCURAB. +
Ostacolo all'esercizio delle ….. - art. 2638 c.c.	Molto Bassa	Molto Alta	MEDIO BASSO +
Ricettazione – art. 648 c.p.	Molto Bassa	Alta	MEDIO BASSO
Riciclaggio – art. 648 bis c.p.	Molto Bassa	Alta	MEDIO BASSO
Impiego di denaro, beni o …. – art. 648 ter c.p.	Molto Bassa	Alta	MEDIO BASSO
Autoriciclaggio – art. 648 ter 1 c.p.	Molto Bassa	Alta	MEDIO BASSO
Indebito utilizzo e falsificaz. … - art. 493 c.p.	Molto Bassa	Bassa	TRASCURAB. +
Reati Tributari ex D.Lgs. 74/2000 ag. al D.L. 124/2019, come modif. e conv. in L.157/2019:	Bassa	Alta	RILEVANTE
Art. 2. Dichiarazione fraudolenta …..			
Art. 3. Dichiarazione fraudolenta ….			
Art. 8. Emissione di fatture ….			
Art. 10. Occultamento o distruzione …			
Art. 11. Sottrazione fraudolenta ….			

RIEPILOGO
AREA RISORSE UMANE
Reati Attinenti

ARTICOLO C.C. - C.P. – D.lgs. 74/2000	**PROBABILITÀ**	**GRAVITÀ**	**RISCHIO RESIDUO**
Intermediazione illecita e sfruttamento del lavoro - art. 603 bis c.p.	Molto Bassa	Alta	MEDIO BASSO
Impiego di cittadini di paesi terzi il cui soggiorno è irregolare – art. 603 bis c.3 c.p.	Molto Bassa	Alta	MEDIO BASSO

RIEPILOGO
AREA GESTIONE RISORSE INFORMATICHE
Reati Attinenti e Parzialmente Attinenti

ARTICOLO C.P. – L. 633/1944	**PROBABILITÀ**	**GRAVITÀ**	**RISCHIO RESIDUO**
635 bis c.p. - Danneggiamento di info. dati	Bassa	Bassa	MEDIO BASSO+
635 ter c.p. - Danneggiamento di info. dati e programmi informatici ….	Molto Bassa	Alta	IMEDIO BASSO
635 quater - Danneggiamento di sistemi …	Molto Bassa	Bassa	TRASCURAB. +
615 ter - Accesso abusivo ad un sistema …	Molto Bassa	Alta	MEDIO BASSO
615 quater - Detenzione, diffusione …	Molto Bassa	Alta	MEDIOBASSO

615 quinquies – Detenzione, diffusione…	Molto Bassa	Bassa	TRASCURAB.+
617 quater - Intercettazione, impedimento …	Molto Bassa	Bassa	TRASCURAB.+
Art. 171 L. 633/1944 – Diffusione…	Molto Bassa	Bassa	TRASCURAB.+
Art. 171 bis L. 633/1944 – Duplicazione…	Molto Bassa	Bassa	TRASCURAB. +
Art. 171 ter L. 633/1944 – Duplicazione …	Molto Bassa	Bassa	TRASCURAB.+

RIEPILOGO
AREA SICUREZZA SUL LAVORO
Reati Attinenti

ARTICOLO C.P.	PROBABILITÀ	GRAVITÀ	RISCHIO RESIDUO
589 - Omicidio colposo	Alta	Molto Alta	CRITICO
590 – Lesioni Colpose	Alta	Molto Alta	CRITICO

RIEPILOGO
AREA REATI AMBENTALI
Reati Attinenti

D.LGS. 152/2006 - C.P.	PROBABILITÀ	GRAVITÀ	RISCHIO RESIDUO
art. 733 bis c.p. - distruzione o deterioramento di habitat all'interno di un sito protetto	Molto Bassa	Alta	MEDIO BASSO
137 D.Lgs. 152/2006	Molto Bassa	Alta	MEDIO BASSO
256 D.Lgs. 152/2006 - gestione rifiuti …	Molto Bassa	Alta	MEDIO BASSO
257 D.Lgs. 152/2006 – bonifica dei siti	Molto Bassa	Alta	MEDIO BASSO
258 D.Lgs. 152/2006 - violazione degli obblighi …	Molto Bassa	Alta	MEDIO BASSO
259 D.Lgs. 152/2006 - traffico illecito di rifiuti	Molto Bassa	Molto Alta	MEDIO BASSO +
260 bis 152/2006 – sistema informatico….	Molto Bassa	Alta	MEDIOBASSO
452 bis c.p. – inquinamento ambientale	Bassa	Molto Alta	RILEVANTE+
452 quater - disastro ambientale	Bassa	Molto Alta	RILEVANTE +
452 quinquies c.p. – delitti colposi contro l'ambien.	Alta	Molto Alta	CRITICO
452 octies c.p. – circostanze aggravanti	Molto Bassa	Alta	MEDIO BASSO
452 quaterdecies – attività organizzata per il traffico illecito dei rifiuti	Molto Bassa	Molto Alta	MEDIO BASSO+

2.3. Gestione dei Rischi: Protocolli e sistemi di controllo

Si è più volte ricordato che, nello specifico ambito di un Modello 231, per protocollo[17] si intende "*un sistema strutturato ed organico di procedure e regole, che include anche le attività di controllo preventive ed ex post, finalizzato a mitigare il rischio di commissione di reati*".

Da precisare che il protocollo non è un qualcosa di "meccanizzato" (analiticamente descrittivo dei passi che devono essere compiuti in successione, come ad esempio avviene nelle "procedure operative"), giacché è invece concepito come "*legge di principi", "proattiva", "legge che non prescrive cosa si deve fare, ma dice invece come ci si deve comportare"*.

Il "*protocollo*", insomma, non fa altro che stigmatizzare le "*euristiche*" - ovvero quelle regole organizzative e quei principi che devono essere applicati in maniera cogente nella vita lavorativa - ed indicare la strada ed i criteri alla cui stregua standardizzare il proprio modo di lavorare, aiutando anche a capire *come* è preferibile realizzarlo, ed in base a quali specifiche modalità sistematiche e organizzative. È una euristica che dice, ad esempio, "non si deve rubare", ma non specifica come farlo perché la definizione delle azioni operative per non rubare compete alla singola azienda, impresa o ente.

Dal punto di vista della loro *rilevanza giuridica nei confronti dei Destinatari* e del MOGC, i Protocolli rappresentano dei precisi "obblighi" giuridici, cui tutti i soggetti che operano "con" o "per" la Società devono sottostare al fine di consentire una corretta ed efficace azione di prevenzione dei reati presupposti. L'inottemperanza a tali "obblighi", ovvero ai *Protocolli,* è passibile di sanzione disciplinare e può dare luogo a responsabilità civile nonché, eventualmente, penale.

Rispettando questo tipo di logica ed obiettivo, nel presente MOGC si è deciso di strutturare la parte dei *Protocolli* in due grandi sotto-categorie: quella dei ***Protocolli Generali***, valevoli per tutte le ipotesi di "reato presupposto" e tutte le azioni aziendali; quella dei ***Protocolli Speciali*** - che comunque presuppongono la costante applicazione dei protocolli generali - maggiormente aderente ad alcune, piuttosto che ad altre, aree di attività.

Tale distinzione ha una sua precisa ragione d'essere nel fatto che il D.Lgs. 231/2001 richiede un'attività di protocollazione delle attività in ordine a tutti i reati presupposti (che peraltro, nel nostro specifico caso, sono stati anche integrati dai "reati presupposti speciali anticorruzione"; il che comporta la necessità di regolamentare attraverso i *protocolli* tutte le porzioni di attività idealmente prese di mira dalle fattispecie delittuose indicate dal Legislatore.

Da non dimenticare poi che il riferimento ad un'unica categoria di *Protocolli Generali* risponde, anche, all'esigenza di evitare un eccessivo "spezzettamento" e disarticolazione dei principi cogenti, e dunque delle concrete misure preventive adottabili, da applicare - si è detto - in *tutte* le fasi della vita aziendale ed in relazione a tutte le possibili condotte societarie.

In conclusione, ai fini dell'azione preventiva adottata nel presente MOGC, sono operanti e obbligatori:

---

[17] Da non confondere con i *"protocolli di legalità"* (o "*patti di integrità*" *ex* art. 1 comma 17 L. 190/2012), che sono quei documenti/accordi/intese di ordine generali usualmente stipulati e controfirmati tra le imprese/società private e le Prefetture, o gli organismi istituzionali/associativi di alta rilevanza (v. Confindustria, etc.), allo scopo di dichiarare e fissare il reciproco impegno di lotta contro la criminalità, contro la mafia locale, contro la delinquenza organizzata *tout court*, nonché stilato, sempre in via assolutamente generale, un programma di reciproci aiuti al fine di assumere tutte le necessarie iniziative atte a garantire il corretto svolgimento di una determinata attività.

- i **Protocolli Generali**, valevoli per tutte le ipotesi di "reato presupposto" e tutte le azioni aziendali;
- i **Protocolli Speciali** - che comunque presuppongono la costante applicazione dei Protocolli Generali - maggiormente aderenti ad alcune, piuttosto che ad altre, aree di attività.

Si ribadisce, quindi, che nel Modello 231 della Società i due piani dei Protocolli – Generali e Speciale - opereranno in via sinergica e complementare:

C) i *Protocolli Generali*, applicabili sempre e comunque da parte di tutti i Destinatari del MOGC in relazione a tutte le fasi di attività aziendale o le possibili ipotesi di reati presupposte;

D) i *Protocolli Speciali*, prescrittivi degli ulteriori obblighi organizzativi di dettaglio in relazione alle peculiarità di ogni determinata area di rischio (a sua volta rientrante in una delle macro e micro aree esaminate in sede di mappatura dei reati).

2.4. I Protocolli Generali

Le caratteristiche di efficacia di un sistema di prevenzione dei comportamenti a rischio di commissione dei reati sono riconducibili soprattutto alla *robustezza* (la capacità del controllo di operare in relazione alle caratteristiche dei rischi e del contesto aziendale considerato) ed i Protocolli Generali devono assicurare, anche secondo le Linee Guida di Confindustria, il rispetto dei seguenti principi di robustezza:

- **Ogni operazione o transazione deve essere: verificabile, documentata, coerente e congrua**

Con tale principio la Società intende assicurarsi che, specialmente nelle attività risultate a rischio, sussista un adeguato supporto documentale (c.d. "*tracciabilità"*) su cui si possa procedere in ogni momento all'effettuazione di controlli. A tal fine è opportuno che per ogni operazione si possa facilmente individuare chi ha autorizzato l'operazione, chi l'abbia materialmente effettuata, chi abbia provveduto alla sua registrazione e chi abbia effettuato un controllo sulla stessa. La tracciabilità delle operazioni può essere assicurata anche tramite l'utilizzo di sistemi informatici in grado di gestire l'operazione consentendo il rispetto dei requisiti sopra descritti.

- **I controlli devono essere effettivi, effettuati e documentati**

Le procedure con cui vengono effettuati i controlli devono garantire la possibilità di ripercorrere le attività di controllo effettuate, in modo tale da consentire la valutazione circa la coerenza delle metodologie adottate (self assessment, indagini a campione, ecc.), e la correttezza dei risultati emersi (es.: report degli audit). La tracciabilità, la separazione dei ruoli ed una corretta assegnazione dei poteri costituiscono un requisito fondamentale nell'ottica della prevenzione dei reati del D.Lgs. 231/2001 in quanto rendono più difficile e complessa la realizzazione di illeciti.

- **Nessuno può gestire in totale autonomia un intero processo aziendale**

Il sistema di controllo deve verificare se sussistano nella Società processi che vengano gestiti da un solo soggetto e provvedere, in tal caso, a porre in essere le necessarie modifiche in modo tale da assicurare il c.d. principio di *"separazione o segregazione delle funzioni".* Tale requisito può essere garantito provvedendo ad assegnare a soggetti diversi le varie fasi di cui si compone il processo ed, in particolare, quella dell'autorizzazione, della contabilizzazione, della esecuzione e del controllo. Inoltre, al fine di garantire il principio di separazione dei ruoli, è opportuno che i poteri autorizzativi e di firma siano correttamente definiti, assegnati e comunicati in modo tale che a nessun soggetto siano attribuiti poteri illimitati.

I tre suddetti principi di *robustezza* devono essere integrati dagli ulteriori seguenti principi (tutti insieme compongono i Protocolli Generali):

- **Chiara individualizzazione dei soggetti agenti, riparto delle responsabilità e attribuzione di deleghe e poteri di firma**

La necessità di individuare i soggetti agenti, oltre che in vista dei necessari controlli *in itinere*, è anche legata alla legittima possibilità di difesa della Società - ex artt. 5, co.2 e 6 co.1. lett. c) del D.Lgs. 231/2001 - in caso di malaugurata commissione di un fatto di reato.

Il riparto delle responsabilità è uno dei principi cardine di un corretto Modello 231, sintetizzabile nel: *deve essere sempre chiaro ed univoco "chi" fa "che cosa", in relazione e/o "con chi"*, così come il corretto rilascio di deleghe (quale attribuzione, a carattere bilaterale, di funzioni e di compiti normativamente delegabili, al fine di innalzare i livelli di efficienza e di controllo aziendale e societario) o di procure (quali atti a carattere unilaterale che conferiscono al procuratore tutto o parte dei poteri diretti ed esclusivi del titolare).

L'attribuzione dei poteri è un diretto corollario del riparto di compiti e responsabilità.

A tal fine, deve essere assicurata la conoscibilità, trasparenza e pubblicità dei poteri attribuiti.

Il protocollo è strettamente correlato al principio secondo cui: *chiunque, interno o esterno a ADR Trasporti S.R.L., ha il diritto di sapere chi è titolare di determinate potestà societarie.* I poteri autorizzativi e di firma devono essere coerenti con le responsabilità organizzative e gestionali assegnate, così come le soglie di approvazione delle spese.

È, pertanto, vietato l'affidamento di poteri-discrezionalità che consentano il controllo di un intero processo di lavoro ad un solo soggetto, al di fuori di vigilanza e/o controlli paralleli.

La *segregazione delle funzioni* - ossia la tendenziale separazione, all'interno di ciascun processo, tra il soggetto che assume la decisione (fase decisionale), il soggetto che esegue tale decisione (fase esecutiva) ed il soggetto cui è affidato il controllo del processo (c.d. "segregazione delle funzioni") - è condizione imprescindibile del Modello 231.

A fronte di cambiamenti organizzativi: deleghe e procure devono essere immediatamente aggiornate; deve esserne data tempestiva comunicazione a tutti i collaboratori e (nel caso di procure aggiornate) alla Camera di Commercio.

- **Coscienza dei ruoli funzionali apicali.**

I soggetti ai quali viene affidato un ruolo apicale - ossia di coordinamento e supervisione del settore o della funzione di cui sono a capo - devono avere piena coscienza e consapevolezza che l'operatività, l'efficacia e la correttezza gestionale, del relativo settore o funzione dipendono, anche e soprattutto, dalla loro capacità di coordinare e controllare i sottoposti, avendo anche il potere-dovere di correggerne gli errori e di avviare le eventuali azioni di riparazione/miglioramento funzionale.

- **Corretta e diligente applicazione de:**

- **La normativa di riferimento**, considerato che il primo e fondamentale presidio di una organizzazione societaria che voglia essere in linea con una gestione all'insegna della legalità e della prevenzione criminosa è la corretta applicazione di tutte le leggi e le norme di riferimento (a carattere locale, regionale, nazionale, comunitario e internazionale) che regolano l'attività sociale, sia nel suo insieme, sia in relazione alle singole mansioni e funzioni assegnate ad ognuno.
- **La prassi normativa di riferimento**.
- **Il Modello 231 adottato da *ADR Trasporti S.R.L.***, che ovviamente rappresenta il nuovo quadro di riferimento organizzativo della Società.

- **Il Codice Etico e di Comportamento** adottato da *ADR Trasporti S.R.L.* (parte integrante del Modello 231), che fotografa l'assetto morale e comportamentale che la Società richiede sia rispettato nella conduzione della propria attività.
- **Le prescrizioni dell'Organismo di Vigilanza 231**.
- **Tutti i Sistemi Gestionali** adottati dalla Società con le relative prescrizioni procedurali, tra cui, e in particolare, il **Sistema Anticorruzione 37001:2016** che, nel presente Modello, si intende del tutto integrato.
- **Le prescrizioni della Funzione di Conformità del Sistema 37001:2016**.
- **Le norme e le circolari aziendali**, quali linee direttrici cui attenersi nello svolgimento dell'attività.

➢ **Proceduralizzazione delle attività e registrazione delle fasi di processo**

Tale presidio richiede che tutte le azioni siano descritte nel loro svolgimento e che tutte le fasi del processo siano individualizzate nei compiti, incombenze e responsabilità. La descrizione organizzativa delle azioni consente, nel tempo, un affinamento e miglioramento di tutte le procedure aziendali, oltre alla loro correlata tracciabilità e replicabilità, rendendo in tal modo ricostruibile *ex post* (e dunque agevolmente controllabile) lo svolgimento delle azioni operative, delle attività e dei procedimenti.

La registrazione delle fasi di processo non è altro che la rappresentazione, tendenzialmente indelebile, di ciò che è stato concretamente posto in essere.

L'obiettivo è di rendere ricostruibili, tracciabili *ex post,* e dunque meglio controllabili, le azioni ed i processi.

L'informatizzazione è una prescrizione necessaria ed opportuna che genera efficacia ed efficienza ed agevola la corretta tracciabilità dello sviluppo del processo, di ridurre il rischio di "blocchi" non controllabili e di consentire l'emersione delle responsabilità per ciascuna fase.

➢ **Obbligo di formazione, informazione, studio e aggiornamento in capo alla Società**

La Società dovrà farsi carico di organizzare - soprattutto in relazione a materie/normative di interesse comune e/o a carattere di inderogabilità (Modello 231, Codice Etico e di Comportamento, Sicurezza sul Lavoro, Ambiente, ecc.) - una corretta politica di supporto formativo di base (comune o per distinti livelli e categorie) e/o specialistico.

La Società dovrà, altresì, attivare un sistema di coordinamento informativo/formativo al fine di consentire ai singoli Destinatari l'eventuale (e auspicabile) scambio di idee, informazioni e *best pratices*.

La formazione, l'informazione e il coinvolgimento degli attori dei processi di lavoro rendono possibile il controllo degli stessi processi in modo efficiente e trasparente.

➢ **Obbligo di formazione, informazione, studio e aggiornamento in capo ai Destinatari**

Ogni *Destinatario* del presente Modello 231 – ed in particolare ogni Responsabile di Funzione o di Unità Operativa – ha l'obbligo individuale di studiare ed aggiornarsi in merito a tutte le possibili modifiche normative (leggi speciali, regolamenti, direttive europee, circolari ministeriali, eccetera), giurisprudenziali e di prassi, afferenti alle proprie funzioni/mansioni.

- **Strutturazione e diffusione di un adeguato sistema informativo e di un sistema automatizzato di comunicazione interna**

Dovrà essere assicurato un adeguato supporto informatico al fine di consentire una corretta ed esaustiva conoscenza, diffusione e condivisione, dei dati e delle informazioni aziendali di cui ai punti precedenti.

Il suddetto presidio informatico deve rappresentare un reale e concreto ausilio per la gestione dei processi di lavoro.

La razionalizzazione dei flussi ed adeguati filtri dovranno assicurare che dati e informazioni vengano differenziati in base a specifiche esigenze o singole aree lavorative. Sempre in via di correlata conseguenzialità rispetto ai punti precedenti, la strutturazione telematica di un sistema di comunicazione interna potrà consentire la corretta circolazione di dati e informazioni da parte di tutte le persone coinvolte nei diversi processi di lavoro.

- **Strutturazione di un sistema di monitoraggio e controllo costante**

In via collaterale all'attività di auditing, è opportuna e consigliabile – anche al fine di arricchire il sistema dei controlli interni - la programmazione di un sistema di monitoraggio e di vigilanza per fasi, soggetti ed azioni, unitamente ad eventuali attività di monitoraggio occasionali e ad hoc, eventualmente affidate ad un dipendente di livello quadro/dirigente.

La strutturazione di un sistema di controllo in itinere risponde all'esigenza di controllare i processi, le procedure e le attività, prima della loro eventuale estrinsecazione illecita. La necessità di detto controllo risulta ancor più giustificata in vista della concreta possibilità per i principali organi di controllo della Società – *in primis,* l'Organismo di Vigilanza – di vigilare non solo *ex post* ma anche in fase di concreto blocco delle condotte illecite.

Il controllo *in itinere* - ad opera di tutti i partecipanti al processo di lavoro, eventualmente anche attraverso l'ausilio delle spontanee segnalazioni di illeciti – rappresenta una delle modalità più efficaci di effettuare una vigilanza anticipatoria rispetto alla malaugurata prosecuzione di eventuali azioni o condotte illecite.

La strutturazione degli specifici controlli in itinere (generali e specifici, preventivi e successivi, analitici e sintetici, contabili, gestionali, interni ed esterni) - accompagnata anche da una piena "correggibilità" delle azioni - è operazione spettante a tutta la compagine aziendale, da condurre attraverso un approccio di piena condivisione e programmazione di tutto il personale che opera "con" o "per" la Società.

Ogni Destinatario - e soprattutto i Responsabili di Funzione e/o di Unità Operative - ha l'obbligo di effettuare un monitoraggio costante su tutti i possibili rischi ex D.Lgs. 231/2001 afferenti alla propria area di azione. Tale monitoraggio si intende comprensivo dell'azione dei colleghi/dipendenti che operano nella stessa area.

- **Attività di auditing**

I Responsabili di Funzioni e/o di Unità Operative hanno l'obbligo (periodico e/o eventualmente *a sorpresa*) di utilizzare il sistema degli audit al fine di verificare e monitorare costantemente la corretta prevenzione dei rischi afferenti alla propria area di azione.

Tale attività di auditing è prevista - in via istituzionale - in capo all'Organismo di Vigilanza ed è svincolata da diversa ed eventuale attività di internal auditing.

- **Attività di reporting**

Dovrà essere sempre assicurata - da parte dei Responsabili di Funzione o di Unità Operativa - una attività di reporting, a cadenza ravvicinata e/o di razionale periodicità, analitica e sintetica, in ordine alle attività poste in essere, ai procedimenti esitati e soprattutto alle informazioni riguardanti la gestione delle situazioni "sensibili".

- **Adozione di un protocollo telematico della corrispondenza in entrata e uscita**

La misura in oggetto, oltre a consentire una doverosa controllabilità *a posteriori*, consente una razionale gestione dei dati aziendali, dei contatti con il "mondo esterno" e, quindi, del corretto svolgimento dei procedimenti.

- **Archiviazione dei dati**

La misura risponde alla intuibile necessità di custodire nel tempo quanto tracciato e raccolto, anche ai fini di possibili e futuri controlli da parte degli organismi aziendali e/o delle Autorità Istituzionali esterne.

- **Tutela di chi che effettua segnalazioni di illecito (whistleblowing)**

Come spiegato ampiamente nella Parte I, il dipendente/collaboratore ha il *diritto/dovere* di segnalare - purché in termini di sufficiente serietà, specificità e concretezza, e fermo restando la sua eventuale responsabilità in caso di calunnia o diffamazione - illeciti relativi allo svolgimento dell'attività sociale ed oggetto del Modello 231, di cui sia venuto (anche casualmente) a conoscenza durante l'espletamento delle sue mansioni/funzioni.

Dovranno essere predissequamente rispettate le regole procedurali indicate dal D.Lgs. 24/2003, adottate dalla Società e debitamente riportate nella relativa *Procedura Whistleblowing* pubblicata sul sito aziendale.

L'identità del segnalante di illeciti dovrà sempre essere tutelata, nei limiti di quanto previsto dalla legge e, in presenza di eventuali segnalazioni di illeciti per il quale il Segnalante autorizzi espressamente il disvelamento della sua identità anche all'Organismo di Vigilanza, lo stesso OdV, ove interpellato o richiesto dal Gestore del Canale di Segnalazione interna ex succitata *Procedura Whistleblowing* dovrà: intervenire immediatamente per evitare che vengano poste in essere misure ritorsive quali licenziamenti, ritorsioni, discriminazioni subite dal segnalante a seguito o per causa della succitata segnalazione; svolgere le opportune verifiche del caso; seguire lo svolgimento della vicenda e, al suo esito, a stilare un motivato report nel quale dovrà essere rappresentato e chiarito se è stato o meno realmente effettuato alcun atto di discriminazione/ritorsione nei confronti del segnalante, se è stato o meno effettivamente operato un atto di discriminazione/ritorsione, eventualmente "riparato/revocato" o ancora persistente.

L'Organismo di Vigilanza dovrà altresì intervenire, ed effettuare tutti i possibili accertamenti rientranti nel suo raggio di azione operativa, in merito ad eventuali segnalazioni di illeciti, rimanendo comunque suo diritto trasmettere gli atti alla Procura della Repubblica ove gli stessi illeciti rivestano rilevanza penale.

Del presente istituto e protocollo aziendale dovrà essere data idonea comunicazione illustrativa a tutti i Destinatari del Modello 231.

2.5. I Protocolli Speciali

❒ **Richiamo delle procedure/istruzione operative del *Sistema di Gestione Integrato Sicurezza - Ambiente - Qualità.***

Si richiamano, in termini esemplificativi e non esaustivi, le principali Procedure/Istruzioni Operative del *Sistema di Gestione Integrato Sicurezza - Ambiente - Qualità.*

Le stesse (e tutte quelle che saranno successivamente inserite nel suddetto *Sistema di Gestione Integrato*) si considerano parte integrante del presente Modello 231 e saranno eventualmente sottoposte al monitoraggio dell'Organismo di Vigilanza 231:

- **ISTRUZIONE MANUALE DELL'AUTISTA**
- **ISTRUZIONE GESTIONE SORVEGLIANZA SANITARIA**
- **PROCEDURA VALUTAZIONE DEI RISCHI DOVUTI A INTERFERENZE**
- **ISTRUZIONE GESTIONE MOVIMENTAZIONE MANUALE DEI CARICHI**
- **ISTRUZIONE GESTIONE DPI, SEGNALETICA E NORME COMPORTAMENTALI**
- **ISTRUZIONE GESTIONE EMERGENZE INCENDIO E PRIMO SOCCORSO**
- **ISTRUZIONE GESTIONE LAVORI IN QUOTA**
- **ISTRUZIONE GESTIONE ESPOSIZIONE AL RUMORE NEGLI AMBIENTI DI LAVORO**
- **ISTRUZIONE GESTIONE MODALITÀ DI EFFETTUAZIONE E DISPOSIZIONE DEI CARICHI DI PRODOTTI SUI MEZZI (ANCORAGGIO)**
- **ISTRUZIONE GESTIONE UTENSILI ELETTRICI PORTATILI**
- **ISTRUZIONE GESTIONE DELLE ATTIVITÀ DI MANUTENZIONE**
- **ISTRUZIONE DI LAVORO IN AMBIENTI CONFINATI**
- **ISTRUZIONE GESTIONE DEI PERMESSI DI LAVORO**
- **ISTRUZIONE GESTIONE "LAVORI A CALDO" E "A FREDDO" ALL'INTERNO DI AREE CLASSIFICATE ATEX**
- **GESTIONE DELLE ATTIVITA' DI SALDATURA E TAGLIO OSSIACETILENICO**
- **PROCEDURA GESTIONE HSE DEI CAMBIAMENTI**
- **PROCEDURA GESTIONE INFORTUNI, INCIDENTI E MANCATI INCIDENTI**
- **PROCEDURA GESTIONE OBIETTIVI, PROGRAMMI E RIESAME**
- **PROCEDURA COMPETENZA, ADDESTRAMENTO E CONSAPEVOLEZZA**
- **ISTRUZIONE GESTIONE SOSTANZE PERICOLOSE**
- **PROCEDURA GESTIONE EMERGENZE**
- **ISTRUZIONE GESTIONE EMERGENZE SPANDIMENTI ACCIDENTALI**
- **ISTRUZIONE GESTIONE DEI RIFIUTI**
- **DISPOSIZIONI SULLE ATTIVITÀ DI CARICO E SCARICO PRODOTTI**
- **ISTRUZIONE INFORMATIVA AMBIENTE E SICUREZZA PER OPERATORI, SUBAPPALTATORI/FORNITORI E VISITATORI**
- **DISPOSIZIONI SULLA GESTIONE DEGLI SCARICHI IDRICI PRESSO IL SITO**
- **ISTRUZIONE GESTIONE DELLE ATTIVITA' DI BONIFICA/LAVAGGIO**
- **PROCEDURA GESTIONE DELLA COMUNICAZIONE**
- **PROCEDURE GESTIONE INFORMAZIONI DOCUMENTATE**
- **PROCEDURA GESTIONE DELLE REGISTRAZIONI**
- **GESTIONE SORVEGLIANZA E MISURAZIONI**

- **PROCEDURA GESTIONE DEGLI APPROVVIGIONAMENTI**
- **PROCEDURA GESTIONE ACQUISIZIONE ORDINI**
- **PROCEDURA AUDIT INTERNI**
- **PROCEDURA GESTIONE DEL CONTROLLO OPERATIVO**
- **PROCEDURA GESTIONE NON CONFORMITÀ E AZIONI CORRETTIVE**

❒ **Richiamo delle procedure/istruzione del *Sistema 37001:2016.***

❖ **Protocolli Speciali 231**

Si indicano di seguito le principali categorie di *Protocolli Speciali*, in base alle diverse aree di rischio ex D.Lgs. 231/2001.

Rimane, tuttavia, fermo che gli stessi:

A) presuppongono la stretta osservanza dei *Protocolli Generali*;

B) presuppongono la stretta osservanza delle specifiche *Procedure e/o Istruzioni Operative* stabilite dalla Governance aziendale o previste nel *Sistema di Gestione Integrato Sicurezza - Ambiente – Qualità* adottato in *ADR*.

Area reati contro la P.A. e contro il Patrimonio della P.A.

Nella fase di valutazione dei rischi sono stati individuati come maggiormente sensibili i seguenti processi:

A) Gestione dei rapporti con funzionari pubblici
B) Gestione partecipazione a gare pubbliche
C) Gestione dei controlli delle autorità pubbliche
D) Gestione del precontenzioso e del contenzioso
E) Gestione delle attività strumentali alla commissione dei reati contro la P.A.:
   1. risorse finanziarie
   2. selezione e assunzione del personale
   3. affidamento di incarichi legali e di consulenza
   4. attività di promozione, sponsorizzazione ed erogazione di contributi
   5. beni e utilità aziendali
   6. rimborsi spese

A) Gestione dei rapporti con funzionari pubblici

- Possono intrattenere rapporti con la P.A. e gestire e firmare i relativi atti solo coloro che sono dotati di idonei poteri a loro affidati dalla Società. Essi devono osservare rigorosamente tutte le leggi, i regolamenti e le procedure che disciplinano i rapporti e i contatti con le Pubbliche Amministrazioni, con i Pubblici Ufficiali e con gli Incaricati di Pubblici Servizi.
- I rapporti con la P.A. o con altra Autorità Istituzionale – *rectius* con i relativi Rappresentanti - devono caratterizzarsi per correttezza comportamentale, gestionale, trasparenza, imparzialità e tracciabilità delle informazioni e delle operazioni, legittimità sotto il profilo sostanziale e formale, chiarezza e veridicità dei riscontri documentali contabili.

- È fatto esplicito divieto di:
  - effettuare elargizioni in denaro od offrire, direttamente o indirettamente, pagamenti indebiti a pubblici funzionari;
  - distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (eventuali regali offerti devono essere documentati in modo adeguato per consentire le verifiche da parte dell'OdV);
  - promettere o accordare vantaggi di qualsiasi natura (promesse di assunzione, etc.) in favore di rappresentanti della P.A.;
- Alle verifiche ispettive da parte della P.A. (quali, ad esempio, INPS, ASL/ASP, Ispettorato del Lavoro, GdF, NAS, soggetti certificatori, ecc.) o dell'Autorità Giudiziaria devono partecipare i soggetti la cui funzione è coinvolta; gli stessi devono informare i superiori gerarchici, i quali, in ordine ad eventuali criticità emerse, devono darne tempestiva comunicazione all'Organismo di Vigilanza.
- È fatto divieto, in sede di ispezioni e accertamenti da parte dei soggetti pubblici, di porre in essere comportamenti in violazione di leggi, norme o regolamenti finalizzati a influenzare, anche nell'interesse della Società, giudizi e pareri o ad ostacolare in qualsiasi modo le funzioni di controllo e/o vigilanza.

B) Gestione partecipazione a gare pubbliche.

Nella eventuale partecipazione alle gare pubbliche, ADR dovrà rispettare le seguenti norme comportamentali:

- applicare correttamente le procedure di partecipazione ai bandi di gara, sia con riferimento alla fase di raccolta delle informazioni sul bando, sia alla valutazione del bando stesso, alla sua approvazione e alla predisposizione e invio della documentazione di gara.
- effettuare controlli sull'esistenza di condizioni essenziali per partecipare ai bandi, sulle delibere autorizzative alla partecipazione alla gara e sull'integrità della busta accompagnatoria della documentazione necessaria per partecipare al bando;
- verificare l'esistenza di eventuali conflitti d'interesse e rimuoverne le cause;
- procedere alla tracciabilità e verificabilità ex post delle transazioni fatte dalla P.A. tramite adeguati supporti documentali/informativi;
- verificare le modalità autorizzative e di monitoraggio sui bandi;
- monitorare i poteri anche con riferimento alla verifica delle firme autorizzative.

C) Gestione dei controlli delle Autorità pubbliche

- Nel caso di ispezioni giudiziarie, tributarie e amministrative (ad esempio verifiche tributarie, INPS, NAS, ASL, Guardia di Finanza, Vigili del Fuoco, etc.), i rapporti con gli organi ispettivi devono essere tenuti solo dai responsabili di Funzione o da soggetti esplicitamente delegati, all'insegna di azioni e comporti improntati alla massima collaborazione, nel rispetto della legge, allo svolgimento delle attività ispettive.
- Il Responsabile della Funzione o il soggetto da questi delegato dovrà verificare che gli organi ispettivi redigano il verbale delle operazioni compiute e richiederne una copia (nei casi in cui ve ne sia il diritto) che dovrà essere adeguatamente conservata. Laddove non sia stato possibile ottenere il rilascio di copia del verbale ispettivo, il soggetto che ha partecipato all'ispezione dovrà provvedere a redigere un verbale/report ad uso interno.

D) Gestione del precontenzioso e del contenzioso

Tra le situazioni di frequente verificazione societaria, vi è quella dei *precontenziosi amministrativi*, ovvero di quelle possibili occasioni in cui - tramite verbali di accertamento o di contestazione/constatazione, visite ispettive con accertamento di violazioni amministrative oblabili, diffide o atti amministrativi analoghi - la Società acquisisce la ragionevole certezza di dover subire un probabile provvedimento di natura sanzionatoria (eventualmente anche di rilevante danno economico e/o di immagine), a seguito di un determinato iter amministrativo.

In presenza di questo tipo di evenienze, diventano di estrema "*sensibilità a rischio di illiceità"* sia i comportamenti dei rappresentanti della Società, sia la gestione della corrispondenza sensibile[18].

In relazione ai **comportamenti dei rappresentanti della Società**:

- sono da scongiurare in modo assoluto ed incondizionato eventuali proposte o azioni di tipo corruttivo al fine di evitare o attenuare l'irrogazione di provvedimenti sanzionatori.

In relazione alla **gestione della corrispondenza sensibile**, la Società è tenuta ad adottare i seguenti presidi:

- tutta la posta sensibile in entrata e in uscita deve essere protocollata con l'apposizione di data e numero progressivo da parte dell'addetto al protocollo;
- le missive in partenza devono essere compilate su carta intestata della Società con l'indicazione della funzione emittente, la qualifica e il nome per esteso del firmatario;
- la posta sensibile deve sempre essere firmata secondo i poteri e le competenze definite dalla Società;
- tutta la corrispondenza gestita per e-mail che impegna la Società verso terzi deve essere seguita da una conferma scritta.

Rimane comunque fermo che, nella **gestione di contenziosi, amministrativi, civili o penali**:

A) tutti i Destinatari dovranno astenersi da:

- dare o promettere denaro o altre utilità a pubblici funzionari o a incaricati di un pubblico servizio o a persone dagli stessi indicati in modo da influenzare l'imparzialità del loro giudizio;
- inviare documenti falsi, attestare requisiti inesistenti o fornire garanzie non rispondenti al vero;
- porre in essere qualsiasi tipo di condotta illecita idonea a favorire o danneggiare una parte nel processo;
- promuovere, assecondare o tacere l'esistenza di un accordo illecito o di una qualsiasi irregolarità o distorsione nelle fasi processuali.

B) la Funzione Legale dovrà:

- protocollare/archiviare correttamente gli atti pervenuti alla società tramite l'ufficiale giudiziario o a mezzo posta;

[18] Qualunque comunicazione in arrivo dalla Pubblica Amministrazione che implichi un comportamento attivo da parte della Società in termini informativi, operativi, attestativi che, ove non messo in atto, può innescare l'insorgere di provvedimenti, diffide ad adempiere o precontenziosi. Qualunque comunicazione in uscita che impegna la Società in quanto controparte inadempiente (o presunta tale) a norme istituzionali (Inps, Inpdai, Ministero delle Finanze, ecc.) e/o a adempimenti commerciali con controparti pubbliche e in ogni caso qualunque risposta alla posta sensibile ricevuta.

- curare l'istruttoria generale del contenzioso redigendo un report contenente i seguenti dati informativi: attore del giudizio, oggetto del contendere, data di notifica dell'atto, funzioni coinvolte, autorità adita, tutta la documentazione necessaria per predisporre gli atti difensivi;
- conservare e custodire tutta la documentazione;
- mantenere un file di tutte le informazioni acquisite dalla Società relative alla nuova posizione di contenzioso (data di udienza di comparizione, data di costituzione, udienza successiva, natura del giudizio, data dei provvedimenti successivi, provvedimenti adottati, data di deposito degli atti, termini di decadenza, notifica del provvedimento, termine di prescrizione, data di chiusura, grado del giudizio);
- aggiornare periodicamente l' Organo Amministrativo sullo status dei contenziosi e sulla loro eventuale chiusura.

E) Gestione delle attività strumentali alla commissione dei reati contro la P.A.

Sono considerate sensibili, in quanto strumentali alla commissione dei reati contro la P.A. le seguenti attività di gestione:

1. Risorse finanziarie

La gestione delle risorse finanziarie è tra quelle maggiormente sensibili rispetto ad una eventuale attività illecita/corruttiva nei confronti di soggetti appartenenti alla P.A., nella misura in cui la stessa attività potrebbe essere verosimilmente alimentata da denaro proveniente dalle casse sociali. A tal fine, vanno rigorosamente osservati i seguenti principi:

- devono essere stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative. Il superamento dei limiti quantitativi di spesa assegnati deve avvenire solo ed esclusivamente per comprovati motivi di urgenza e in casi eccezionali: in tali casi deve essere previsto che si proceda alla sanatoria dell'evento eccezionale attraverso il rilascio delle debite autorizzazioni;
- l'Organo Amministrativo o il soggetto da esso delegato, deve stabilire o modificare, se necessario, la procedura di firma congiunta per determinate tipologie di operazioni o per operazioni che superino una determinata soglia quantitativa;
- le operazioni che comportano l'utilizzo o l'impiego di risorse economiche o finanziarie devono avere una causale espressa ed essere documentate e registrate in conformità ai principi di correttezza professionale e contabile;
- l'impiego di risorse finanziarie deve essere motivato dal soggetto richiedente, anche attraverso la mera indicazione della tipologia di spesa alla quale appartiene l'operazione;
- devono essere monitorati i flussi, in entrata e in uscita, delle risorse finanziarie;
- la Società deve avvalersi di istituti finanziari e bancari sottoposti a una regolamentazione di trasparenza e di correttezza conforme alla disciplina dell'Unione Europea;
- devono essere preventivamente stabiliti, in funzione della natura della prestazione svolta, limiti quantitativi all'erogazione di anticipi di cassa e al rimborso di spese sostenute da parte del personale della Società.

2. Selezione e assunzione del personale

L'assunzione del "personale" potrebbe concretamente celare accordi o promesse di tipo corruttivo. Il processo dovrà, pertanto, essere uniformato ai seguenti princìpi:

- formulazione richiesta di nuovo personale da parte del Responsabile di Funzione che ne manifesta l'esigenza, corredata da dettagliata documentazione presentata nel rispetto delle procedure interne;
- accettazione della richiesta coerentemente con il budget e le piante organiche approvate (se presenti. Le richieste extra budget devono essere sempre motivate e autorizzate in accordo con le procedure interne);
- tracciabilità delle fonti di reperimento dei *curricula vitae;*
- richiesta e rilascio di una dichiarazione del candidato relativa all'eventuale esistenza di particolari vincoli di parentela o affinità con eventuali soggetti pubblici con i quali *ADR Trasporti S.R.L.* intrattiene rapporti contrattuali;
- verifica valutazione reputazionale, anche di ordine giudiziario.
- rispetto del criterio della separazione organizzativa per le attività di valutazione delle candidature nel cui ambito è necessario:
  - definire criteri di controllo nel caso in cui la Società faccia ricorso al lavoro interinale mediante le agenzie specializzate;
  - prevedere distinte modalità di valutazione, "attitudinale" e "tecnica", del candidato;
  - assegnare la responsabilità delle valutazioni attitudinali e tecniche a soggetti distinti (la valutazione a cura della funzione "tecnica" deve essere sempre accompagnata da quella delle Risorse Umane);
  - formalizzare l'esito del processo di valutazione e selezione del candidato.
- scelta sulla base di requisiti di professionalità specifica rispetto all'incarico;
- uguaglianza di trattamento, indipendenza, competenza e, in riferimento a tali criteri, adozione di una motivata e tracciabile attività.
- nella fase di formulazione dell'offerta e assunzione:
  - verifica del rispetto dei requisiti di legge ai fini dell'assunzione, compresa la regolarità in termini di permessi di soggiorno in caso di persone straniere;
  - verifica dell'esistenza della documentazione accertante il corretto svolgimento delle fasi precedenti in sede di sottoscrizione della lettera di assunzione;
  - valutazione dei requisiti personali e professionali, eventualmente anche tramite debita documentazione o autocertificazioni riguardanti l'affidabilità di ordine reputazionale;
  - corretta e tracciabile archiviazione della documentazione;
  - applicazione delle norme prescritte in materia di sicurezza e igiene nei luoghi di lavoro e divieto di sottoporre il lavoratore a condizioni di lavoro ed a metodi di sorveglianza degradanti (con conseguente rigorosa applicazione della normativa relativa all'orario di lavoro, ai periodi di riposo, al riposo settimanale, all'aspettativa obbligatoria, alle ferie);
  - corresponsione di retribuzioni conformi ai contratti collettivi nazionali o territoriali stipulati dalle organizzazioni sindacali più rappresentative a livello nazionale, o comunque retribuzioni proporzionate alla quantità e qualità del lavoro prestato;
  - reclutamento di soggetti solo in età e condizione lavorativa;

- consegna al neo assunto, al momento dell'assunzione, di un kit contenente il Modello 231 e il Codice Etico e di Comportamento che il lavoratore dovrà sottoscrivere con l'accettazione delle regole e dei comportamenti previsti nei suddetti documenti.

▪ l'acquisizione dei dati personali dovrà essere effettuata nel rispetto dei criteri di riservatezza e delle disposizioni di cui al D.Lgs. 196/2003 ss.mm.ii. in materia di dati sensibili e comuni.

3. Affidamento di incarichi legali e di consulenza

La funzione richiedente la consulenza è tenuta ad indicare le ragioni che giustificano il ricorso all'esterno, la tempistica, il profilo professionale richiesto e i criteri di scelta del soggetto individuato.

4. Attività di promozione, sponsorizzazione ed erogazione di contributi

▪ Le attività di gestione delle erogazioni liberali e dei contributi devono essere esclusivamente connesse all'attività aziendale e/o dirette ad accrescere ed a promuovere l'immagine e la cultura della Società.

▪ Deve esistere una autorizzazione formalizzata a conferire utilità.

▪ Devono esistere documenti giustificativi delle spese effettuate per la concessione di utilità con motivazione e attestazione di inerenza e congruità.

▪ Devono essere predisposti controlli di monitoraggio sulle suddette operazioni al fine di individuare quelle ritenute anomale per controparte, tipologia, oggetto, frequenza o entità sospette.

▪ Deve essere verificata la regolarità dei pagamenti per donazioni, sponsorizzazioni o liberalità con riferimento alla piena coincidenza dei destinatari dei pagamenti e le controparti effettivamente coinvolte.

▪ Devono esistere report periodici sulle spese per la concessione di utilità, con motivazioni e nominativi beneficiari, e archiviati.

5. Beni e utilità aziendali

Il riferimento - a titolo meramente esemplificativo e non esaustivo – è ai seguenti beni: autovetture, cellulari, personal computer, carte di credito aziendali, etc.

In relazione a tali beni - il cui abuso potrebbe essere costituito da una illecita distrazione in favore di soggetti appartenenti alla P.A. o a pubblici poteri, eventualmente corruttibili - l'affidamento dovrà essere:

▪ corredato da assegnazione del bene motivata in ragione del ruolo e della mansione del personale beneficiario e accompagnato da modalità che consentano la costante tracciabilità di quanto consegnato all'interessato;

▪ debitamente autorizzato, nonché registrato, aggiornato e archiviato;

▪ revocato in caso di violazione delle procedure e dei regolamenti aziendali durante l'utilizzo;

▪ restituito in caso di dimissioni o pensionamento del dipendente.

6. Rimborsi spese

I rimborsi spese, al pari dei beni e delle utilità aziendali di cui al punto precedente, potrebbero essere abusati in favore di soggetti appartenenti alla P.A. ad intuibili fini di "*favor*" o proposte corruttive. Ne deriva la necessità di rispettare le seguenti prescrizioni:

- la gestione dei rimborsi spese deve avvenire in accordo con la normativa, anche fiscale, applicabile;
- possono essere ammessi anticipi o rimborsi delle spese sostenute direttamente dai soggetti esterni con evidenza documentale delle spese da sostenere/sostenute;
- devono essere definite responsabilità e limiti alla concessione di anticipi ai lavoratori;
- deve essere individuato, secondo i livelli gerarchici presenti in azienda, il Responsabile che autorizza *ex ante* o *ex post* (a seconda delle tipologie di trasferte, missioni o viaggi al di fuori dei consueti luoghi di lavoro) le note spese ai soggetti richiedenti;
- le note spese devono essere gestite secondo le modalità comunicate a tutto il personale, in termini di rispetto dei limiti indicati dalle *policy aziendali*, delle finalità delle spese sostenute, della modulistica, dei livelli autorizzativi richiesti e della liquidazione delle somme a rimborso;
- i processi di autorizzazione e controllo delle trasferte devono essere sempre ispirati a criteri di massima trasparenza, sia nei confronti della regolamentazione aziendale interna che nei confronti delle leggi e delle normative fiscali vigenti;
- deve essere assicurata l'evidenza dell'avvenuta approvazione della missione;
- devono essere previsti formali controlli circa l'inerenza e la documentazione delle spese per le quali si richiede il rimborso.

Area Rapporti con il Mercato Privato

Devono essere rigorosamente applicati i Protocolli Generali, intesi come *standard precauzionali/preventivi generali* a presidio dei rischi e le Procedure/Istruzioni Operative del succitato *Sistema di Gestione Integrato*.

Area a Rischio di commissione Reati contro la Fede Pubblica, l'Ordine Pubblico, l'Ordine Democratico, gli interessi dello Stato

Al fine di prevenire i rischi di infiltrazione della criminalità organizzata nell'attività aziendale e di controllarne i relativi e possibili reati, è cogente l'applicazione dei Protocolli Generali, intesi come *standard precauzionali/preventivi generali* a presidio dei rischi.

Entrando nel merito (e preso altresì atto che i delitti iscrivibili in questa area non sembrano potersi ricollegare a singole e specifiche attività svolte dalla Società), va considerato che:

- tali delitti hanno, per ampia parte, natura di reati associativi (associazione per delinquere) o comunque, fortemente collegati ai reati associativi (v., ad esempio, lo scambio elettorale politico-mafioso avvalendosi delle modalità di cui all'art. 416-bis c.p.), che puniscono anche solamente l'accordo tra più persone volto alla commissione di qualunque delitto.
- i reati associativi, essendo per definizione costituiti dall'accordo volto alla commissione di qualunque tipo di delitto, estendono il novero dei reati presupposto ad un numero indeterminato di figure criminose. Pertanto, qualsiasi attività svolta dalla Società potrebbe

comportare la commissione di un delitto - e la conseguente responsabilità ex D.Lgs. 231/2001 - "tramite" un'associazione per delinquere.

Sebbene, come detto, tali reati risultino essere non riconducibili a specifiche attività, gli stessi possono essere astrattamente commessi sia da soggetti apicali che da subordinati, nonché da eventuali partners o fornitori, soprattutto sub vettori A questo fine, assume rilevanza il Sistema di Controllo Interno già in essere nella Società e il rispetto dei Protocolli Generali.

In via meramente esemplificativa, va comunque ricordato che le attività potenzialmente più esposte agli interessi di associazioni criminose, nell'ambito delle quali potrebbero essere commessi i delitti di criminalità organizzata previsti dall'art. 24-ter del Decreto, sono:

A) Gestione delle risorse finanziarie (trattato *supra* e ripreso *infra* nell'*Area Finanza e Contabilità*).

B) Selezione, assunzione e gestione del personale (trattato *supra*).

C) Approvvigionamento di beni e servizi e controllo dei fornitori

Avuto specifico riguardo al controllo e vigilanza su tale specifica attività - ovvero, lato sensu, sull'*approvvigionamento di beni e servizi* e sul *controllo fornitori* - i Protocolli prevedono che:

- tutti i beni acquistati devono essere procurati da fornitori ufficiali, conosciuti sul mercato e provvisti di correlata documentazione di acquisto e trasporto. La documentazione di acquisto e trasporto deve essere regolarmente registrata nella contabilità sociale;
- l'approvvigionamento di beni o servizi deve essere disciplinata da documentazione scritta nel quale sia chiaramente indicato il prezzo del bene o della prestazione o i criteri per determinarlo;
- i contratti di approvvigionamento di valore significativo devono sempre essere preventivamente valutati e autorizzati dal Responsabile della funzione che richiede il bene o il servizio e dal Responsabile Amministrativo/Acquisti;
- nei contratti che regolano i rapporti con i fornitori, gli appaltatori, i subappaltatori, i vettori e i sub vettori, devono essere inserite apposite clausole che richiamano gli adempimenti e le responsabilità derivanti dal Modello 231 e dal relativo Codice Etico e di Comportamento e deve essere sottoscritta una specifica ed idonea clausola di manleva sulla loro osservanza;
- devono essere preventivamente valutate la reputazione e l'affidabilità del fornitore, o del sub vettore, dal punto professionale e personale;
- non devono essere corrisposti pagamenti ai fornitori in misura non congrua rispetto alla natura ed al valore dei beni o servizi forniti, o non conformi alle condizioni commerciali o alla prassi esistenti sul mercato;
- il Responsabile della funzione interessata deve segnalare immediatamente all'Organismo di Vigilanza eventuali anomalie nelle prestazioni rese dal fornitore o altri ed eventuali indici di alert;
- devono essere specificamente adottati dei controlli antimafia al fine di prevenire ed evitare i reati di cui all'art. 24 ter, ovvero possibili ingressi di personale malavitoso o qualunque eventuale rischio di infiltrazione mafiosa e/o di infiltrazione lato sensu illecita (sotto qualsiasi forma e modalità), anche attraverso:

- monitoraggio di qualsiasi indice di alert, da qualsiasi parte provenga ed attraverso qualsiasi forma si presenti;
- valutazione di indici attestanti l'affidabilità personale e professionale;
- controllo di iscrizione alla *white list* dei fornitori (soprattutto di servizi, come ad esempio i sub vettori) o dei partners che appartengano alle categorie per le quali è prevista la relativa iscrizione, o richiesta di analoga autocertificazione da parte di coloro appartenenti alle categorie escluse;
- richiesta di iscrizione alla succitata *white list* per i fornitori non ancora iscritti;
- veto ad intrattenere rapporti di committenza con fornitori che non intendano iscriversi alla *white list*:
- richiesta di un un'autocertificazione dalla quale risulti l'indicazione nominativa del personale utilizzato nei lavori;
- richiesta di un'autocertificazione con la quale il fornitore attesti, sotto la propria responsabilità, che agisce in nome proprio, se del caso fornendo la specifica documentazione richiesta dalla Società;
- divieto di intrattenere rapporti di lavoro o di partenariato o di fornitura con imprese che possano essere ritenute, anche sulla base di elementi di fatto o valutazioni di ordine indiziario, costituite al solo scopo di occultare o favorire soggetti appartenenti a gruppi criminali, o di eludere divieti nello svolgimento di attività imprenditoriali, nonchè prive di rapporti con aziende di credito o rappresentate da persone o soggetti privi di legittimazione ad agire o ad interloquire;
- richiesta di documenti comprovanti l'iscrizione ad albi, ordini, elenchi, qualora l'iscrizione sia requisito necessario per lo svolgimento dell'attività;

Infine, **qualsiasi condotta genericamente anomala o sospetta** deve essere monitorata con attenzione, in primis dalla funzione Risorse Umane.

Si ricordi, del resto, che il D.Lgs. 231/2001 enuclea tra i suoi reati presupposti ordinari, alcune fattispecie delittuose molto "particolari" (oltre che non concretamente prevedibili o evitabili), quali ad esempio:

- tutti i reati contro l'Ordine Pubblico di cui all'art. 24 ter;
- tutti i reati contro l'Ordine Democratico di cui all'art. 25 quater;
- le ipotesi di reato di cui all'art. 25 quinquies (tra cui, la riduzione o il mantenimento in schiavitù o in servitù ex art. 600 c.p.) e 25 quater.1 (pratiche di mutilazione dei genitali);
- i reati di razzismo e xenofobia richiamati dall'art. 25 terdecies.

Tali delitti non sono concretamente collegabili a specifici processi/mansioni della Società e, dunque, potranno risultare evincibili solo da condotte genericamente anomale, o da comportamenti inusuali, o da segnalazioni più o meno esplicite, o da indistinti elementi di sospetto.

Anche per queste ipotesi delittuose la Funzione Risorse Umane dovrà garantire un'azione di costante monitoraggio e vigilanza, con correlativo obbligo di relazionare all'Organismo di Vigilanza in presenza di circostanze rappresentative di possibili *alert* da verificare o da tenere sotto controllo.

Area Finanza e Contabilità

I protocolli logicamente accorpabili in quest'area di rischio sono quelli afferenti a:

A) i reati societari (presupposti dall'art. 25 ter del D.Lgs 231/2001);

B) i delitti contro il patrimonio ex artt. 648, 648-bis, 648-ter, 648-ter.1 del codice penale (presupposti dall'art. 25 octies del D.Lgs. 231/2001) ed ex art. 493 ter c.p. (presupposto dall'art. 25 octies.1 del Decreto 231);

C) i reati tributari ex artt. 2, 3, 8, 10 e 11 del D.Lgs. 74/2000 e succ. modifiche (presupposti dal neo art. 25 quinquiesdecies introdotto dall'art. 39 del D.L. 26 ottobre 2019 n. 124, a sua volta convertito con modificazioni in Legge 19 dicembre 2019, n. 157).

❖ Si ricorda, invece, la *non pertinenza* - analiticamente illustrata nell'Allegato 3 (*Mappatura e Gestione dei Rischi)* dei reati tributari introdotti dal D.Lgs. 75/2020 nell'art. 25 quinquiesdecies e dei reati di contrabbando inseriti dallo stesso D.Lgs. 75/2020 nell'art. 25 sexiesdecies.

A) Reati Societari

Il sistema protocollare da attivare e vigilare in ordine ai reati societari di cui all'art. 25 ter del D.Lgs 231/2001 è basato su "specifici" standard di controllo interno anche in relazione alla vastità, articolazione e delicatezza dei processi e attività aziendali coinvolte:

- Ciclo Passivo (registrazione fatture e pagamenti di fornitori; gestione note di credito/debito; altre registrazioni contabili pertinenti alla contabilità fornitori) e Ciclo Attivo (emissione di fatture attive e loro registrazione in contabilità; gestione incassi crediti verso clienti e loro registrazione contabile; altre registrazioni contabili pertinenti alla contabilità clienti); Gestione Cespiti (tenuta e aggiornamento libro cespiti, registrazione ammortamenti, rilevazione contabile di plusvalenze/minusvalenze); Tasse (registrazioni contabili e pagamenti dichiarazioni IVA, tasse e altre imposte); Finanziario (movimentazione flussi bancari - tramite bonifici, prelievi e depositi, assegni, ecc. - e finanziari - mutui, interessi, etc.); Controllo e Verifica (predisposizione e verifica riconciliazioni bancarie, reportistica e rendicontazione, determinazione e controllo del budget); Amministrazione del personale (tenuta dei libri obbligatori, registrazione contabile e pagamenti di buste paga, registrazione contabile e pagamento di contributi INPS, INAIL, ecc. e ritenute d'acconto);
- Attività in conformità a quanto deliberato dal Organo Amministrativo: redazione della bozza di bilancio e della relazione sulla gestione; predisposizione ed approvazione di comunicazioni sociali rilevanti; supporto alle attività di controllo svolte dai competenti organismi (autorità pubbliche di vigilanza, collegio sindacale, ecc.); operazioni in materia di ripartizione di utili o riserve, nonché su azioni o quote sociali; attività riguardanti la riduzione o la formazione del capitale sociale, nonché operazioni di fusione, scissione e di finanza straordinaria; gestione rapporti e ispezioni svolte da organi pubblici di vigilanza e controllo; gestione delle informazioni, anche tramite attività di rendicontazione amministrativa e contabile; gestione dei dati ai fini della redazione della bozza del bilancio d'esercizio e delle comunicazioni sociali della Società).

Conseguentemente, attraverso l'attività di *risk assessment*, sono state individuate le principali attività sensibili, di seguito elencate, nell'ambito delle quali potrebbero potenzialmente essere commessi i reati societari previsti dall'art. 25-ter del Decreto.

A.1 Attività propedeutiche e relative alla redazione dei bilanci, delle scritture contabili e di altri documenti societari.
A.2 Gestione dei rapporti con i Soci e con gli Organi di Controllo (Organismo di Vigilanza e Organismo di Controllo contabile ex art. 379, comma 1 lett.c) del D.Lgs. 12 gennaio 2019, n. 14 (Codice della crisi d'impresa e dell'insolvenza in attuazione della legge 19 ottobre 2017, n. 155).

A.1 Attività propedeutiche e relative alla redazione dei bilanci, delle scritture contabili e di altri documenti societari

- La gestione della finanza e del denaro aziendale deve essere assegnata alla relativa Funzione societaria e non è delegabile, se non in casi di eccezionale, motivata e comprovata necessità aziendale. Tutte le eventuali attività delegate devono essere formalizzate al fine di consentire la precisa individuazione dei soggetti agenti.
- Devono essere stabiliti limiti all'autonomo impiego delle risorse finanziarie, mediante la definizione di soglie quantitative di spesa, coerenti con le competenze gestionali e le responsabilità organizzative. Il superamento dei limiti quantitativi di spesa assegnati può avvenire solo ed esclusivamente per comprovati motivi di urgenza e in casi eccezionali. In tali casi è previsto che si proceda alla sanatoria dell'evento eccezionale attraverso il rilascio delle debite autorizzazioni da parte delle funzioni aziendali competenti.
- L'Organo Amministrativo, o il soggetto da esso delegato, stabilisce e modifica, se necessario, la procedura di firma congiunta per determinate tipologie di operazioni o per operazioni che superino una determinata soglia quantitativa.
- Per la gestione dei flussi in entrata e in uscita sopra i limiti previsti dalla normativa vigente, devono essere utilizzati esclusivamente i canali bancari e di altri intermediari finanziari accreditati e sottoposti alla disciplina dell'Unione Europea e agli obblighi previsti dalle leggi sul riciclaggio.
- I pagamenti in contanti sono vietati, salvo che via sia espressa autorizzazione da parte del vertice societario e comunque per importi che non superino somme gestite nei limiti previsti dalla normativa vigente.
- I rapporti intrattenuti con gli Istituti bancari, con i clienti e con i fornitori, devono essere costantemente verificati attraverso lo svolgimento di periodiche riconciliazioni.
- Per il consolidamento dei dati di bilancio, deve essere adottato un manuale contabile o delle procedure contabili in cui ove siano indicati con chiarezza i dati e le informazioni contabili, i criteri contabili per l'elaborazione dei dati e la tempistica per la loro trasmissione alla funzione responsabile, nonché i criteri e le modalità per il consolidamento dei dati di bilancio.
- Devono essere rispettati i tempi e le modalità di predisposizione ed invio dei dati alla Funzione Amministrazione e Finanza, affinché ciò avvenga in modo corretto, completo e tempestivo, specificando chiaramente le fonti originarie dalle quali sono tratte ed elaborate le informazioni trasmesse.
- La rilevazione, trasmissione e aggregazione delle informazioni contabili finalizzate alla predisposizione delle comunicazioni sociali deve avvenire in modo tale da garantire la tracciabilità dei singoli passaggi del processo di formazione dei dati e l'identificazione dei soggetti che inseriscono i dati nel sistema, nel rispetto della separazione delle funzioni e della coerenza dei livelli autorizzativi.

- Le bozze del bilancio e degli altri documenti contabili devono essere messi a disposizione degli amministratori con ragionevole anticipo rispetto alla riunione dell'Assemblea chiamata a deliberare sull'approvazione del bilancio.
- È vietato modificare o alterare, anche in concorso di colpa con altri, i dati contabili e/o di bilancio, fornendo una rappresentazione della situazione patrimoniale, economica e finanziaria della Società difforme dalla realtà al fine di indurre i soci o i terzi in errore per trarne un ingiusto profitto.
- È vietato occultare risorse e fondi liquidi o di riserve al fine di indurre in errore i soci o i creditori per trarne un ingiusto profitto o vantaggio o esposizione di dati idonea a pregiudicare i diritti dei creditori al fine di ottenere un indebito vantaggio.
- È vietato violare l'obbligo di astensione a prendere decisioni in conflitto d'interessi al fine di procurare un vantaggio o un profitto alla Società.

A.2 Gestione dei rapporti con i Soci e con gli Organi di Controllo

- Deve essere garantito ai soci e agli Organi di Controllo il libero accesso alla contabilità aziendale, alla gestione sociale e a quanto altro richiesto per un corretto svolgimento dell'incarico.
- Le richieste e le trasmissioni di dati e informazioni devono essere documentate e conservate.
- È vietato qualsiasi comportamento (anche sotto forma di opposizione, rifiuti pretestuosi, comportamenti ostruzionistici, mancata collaborazione, ritardi nelle comunicazioni o nella messa a disposizione di documenti) che sia di ostacolo all'esercizio delle funzioni di vigilanza.
- Devono essere effettuate con tempestività, correttezza e buona fede, tutte le comunicazioni e le segnalazioni previste dalla legge e dai regolamenti nei confronti degli organismi di controllo e delle Autorità di vigilanza.

B) Delitti contro il patrimonio (Ricettazione, Riciclaggio, impiego di denaro, beni o utilità di provenienza illecita e autoriciclaggio)

Per ciò che afferisce ai presupposti *Delitti contro il Patrimonio* - v., in particolare, i reati di *ricettazione*, *riciclaggio*, *impiego di denaro, beni e altre utilità di provenienza illecita* e auto riciclaggio - la prevenzione ed il controllo riguardano due diverse tipologie di oggetti:

- il denaro illecito, eventualmente introitato e nascosto tra quello lecito;
- i beni, le cose o le altre utilità, provenienti da delitto e illecitamente acquistati, ricevuti, occultati, reimpiegati, o trasferiti per celarne la provenienza illecita.

I protocolli di prevenzione che seguono devono trovare specifica attuazione nelle procedure aziendali.

B.1 Gestione dei flussi monetari e finanziari in uscita

Tali flussi si distinguono in: *flussi ordinari*, connessi ad attività/operazioni correnti (ad es., acquisti di beni, servizi e licenze, oneri finanziari, fiscali e previdenziali, stipendi e salari); *flussi straordinari*, connessi alle operazioni di tipo finanziario (ad es. sottoscrizioni, aumenti di capitale sociale, finanziamenti a società collegate, cessioni di credito, ecc.). Sul presupposto che i flussi in oggetto costituiscono una delle modalità strumentali attraverso cui, in linea di principio, potrebbero essere commessi i reati che presuppongono la *datio* illecita di denaro, la Società deve:

- assicurare una corretta separazione di ruolo ed una piena tracciabilità degli atti per le operazioni di: a) richiesta dell'ordine di pagamento o di messa a disposizione dei fondi; b) approvazione della richiesta; c) effettuazione del pagamento; d) controllo a consuntivo;
- prevedere un flusso informativo sistematico che garantisca il costante allineamento fra procure, deleghe operative e profili autorizzativi;
- prevedere idonei ed espliciti livelli autorizzativi, sia per la richiesta che per l'ordine di pagamento o di messa a disposizione dei fondi, in funzione della natura dell'operazione (ordinaria o straordinaria) e dell'importo. Eventuali modalità non standard (v. ad esempio i pagamenti c.d. manuali) devono essere considerate "in deroga" e soggette, pertanto, a criteri di autorizzazione e controllo specificamente definiti e riconducibili a: a) individuazione del soggetto che richiede l'operazione; b) individuazione del soggetto che autorizza l'operazione; c) indicazione, a cura del richiedente, della motivazione; d) designazione (eventuale) della persona abilitata all'effettuazione dell'operazione attraverso autorizzazione/procura ad hoc;
- assicurare la ricostruzione delle operazioni e la registrazione dei dati in appositi archivi da mettere a disposizione delle funzioni o Autorità di Controllo;
- verificare sempre la regolarità dei pagamenti, con riferimento alla piena coincidenza dei destinatari/ordinanti e le controparti coinvolte nella transazione (in particolare dovrà essere puntualmente verificato che vi sia coincidenza tra il soggetto a cui è intestato l'ordine e il soggetto che incassa le relative somme) e deve essere previsto il divieto di accettazione ed esecuzione di ordini di pagamento provenienti da soggetti non identificabili.

B.2 Gestione acquisti di beni e servizi

Vale quanto prescritto *supra* nell'*Area a Rischio di commissione Reati contro la Fede Pubblica, l'Ordine Pubblico, l'Ordine Democratico, gli interessi dello Stato, lettera C) approvvigionamento di beni e servizi e controllo fornitori*.

C) Reati Tributari

Come rilevato in sede di *crime risk assessment*, i reati tributari di cui agli artt. 2, 3, 8, 10 e 11, previsti e puniti dal D.Lgs. 10 marzo 2000, n. 74 (recante "*Nuova disciplina dei reati in materia di imposte sui redditi e sul valore aggiunto, a norma dell'articolo 9 della legge 25 giugno 1999, n. 205"*, aggiornato al D.L. 26 ottobre 2019 n. 124 e per come modificato in sede di conversione dalla Legge 19 dicembre 2019, n. 157), hanno un minimo comune denominatore: l'obiettivo (che dal punto di vista penalistico si traduce in "*dolo specifico*") di eludere i propri obblighi fiscali attraverso azioni ed operazioni di natura sostanzialmente fraudolenta.

Tale obiettivo e fraudolenza sono oggettivamente agevolati dal disordine contabile e dalla mancanza di: idonea e razionale formalizzazione degli atti e delle operazioni; fedele conservazione ed archiviazione di atti e documenti; proceduralizzazione delle attività; controlli interni ed esterni; individuazione delle specifiche funzioni e compiti assegnati a più soggetti distinti; segregazione di funzioni, azioni ed attività.

Ciò comporta che, mai come in questo specifico ambito, è necessario ed indispensabile il rigoroso rispetto dei *Protocolli Generali* previsti nel presente Modello 231. Accanto a tali presidi di ordine generale vanno parimenti rispettati e monitorati i *Protocolli Speciali* richiamati *supra* e *infra*.

Una attenzione particolare deve essere rivolta all'attività di **gestione degli acquisti di beni e servizi**, che potrebbe diventare rilevante sopratutto ai fini del reato di cui all'art. 2 del D.Lgs. 74/2000, ovvero alla fraudolenta attività di inserimento o manipolazione/falsificazione dei documenti di costo (certificazioni fiscali o fatture) al fine di pervenire ad un innalzamento delle componenti negativo di reddito con conseguente abbassamento dell'imponibile e fraudolento risparmio di imposta.

Anche in questo caso, vale quanto prescritto *supra* nell'*Area a Rischio di commissione Reati contro la Fede Pubblica, l'Ordine Pubblico, l'Ordine Democratico, gli interessi dello Stato, lettera C) approvvigionamento di beni e servizi e controllo fornitori.*

Area Risorse Umane

Si ricorda che la macro area in oggetto non si sovrappone perfettamente alle attività istituzionali della Funzione Risorse Umane. Infatti, la generica nozione di Risorse Umane inquadra e riunisce in una stessa famiglia concettuale ipotesi delittuose il cui nesso derivativo tra la Società e l'ipotetico fatto criminoso è dato dalla possibile presenza di un autore materiale del reato che operi "con" e "per" *ADR Trasporti S.R.L.*, sia come dipendente che come vertice ed amministratore.

Al fine di prevenire i rischi di commissione dei reati inseriti in questa area, è cogente l'applicazione dei *Protocolli Generali*, intesi come *standard precauzionali/preventivi generali* a presidio dei rischi, rivolti a tutti i destinatari del Modello 231.

Inoltre, la Società ha individuato le seguenti attività come le più esposte a rischi: A) Intermediazione illecita e sfruttamento del lavoro; B) Impiego di cittadini di paesi terzi il cui soggiorno è irregolare; C) Rilascio di dichiarazioni all'autorità giudiziaria.

A) Intermediazione illecita e sfruttamento del lavoro

Sul presupposto - chiarito in sede di *Crime Risk Analysis* - che le condotte illecite concretamente ipotizzabili in *ADR Trasporti S.R.L.* ai fini del reato di *"intermediazione illecita e sfruttamento del lavoro "ex* art. 603 bis c.p. sono "solo" quelle di cui al comma 1, lett. 2 («*utilizza, assume o impiega manodopera, anche mediante l'attività di intermediazione di cui al numero 1), sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno»)*, i protocolli preventivi prevedono e sono volti ad evitare che si possano verificare le condizioni di "sfruttamento" e di "approfittamento dello stato di bisogno" richiamati dalla norma prescrittrice.

All'uopo, la Società vieta categoricamente e sanziona sia il reclutamento della manodopera in condizioni di sfruttamento, approfittando dello stato di bisogno dei lavoratori, sia l'impiego di manodopera, anche mediante l'attività di intermediazione, sottoponendo i lavoratori a condizioni di sfruttamento ed approfittando del loro stato di bisogno.

Nell'ambito di tali comportamenti, vale quanto prescritto *supra* nell'*Area reati contro la P.A. e contro il Patrimonio della P.A., lettera G), comma 2: Gestione delle attività strumentali alla commissione dei reati contro la P.A., selezione e assunzione del personale*.

B) Impiego di cittadini di paesi terzi il cui soggiorno è irregolare

Attraverso l'attività di *crime risk assessment* la Società ha individuato le seguenti attività sensibili: 1) selezione e assunzione del personale ed in particolare, ma non esclusivamente, in caso di lavoratori stranieri; 2) conclusione di contratti con imprese che utilizzano personale d'opera non qualificato proveniente da Paesi extracomunitari. La fattispecie in esame risulta ricollegabile alla gestione dei processi di selezione e assunzione del personale ed alla gestione degli appalti in cui possono essere impiegati, a diverso titolo, lavoratori stranieri.

La Società in termini di selezione e assunzione del personale adotta i protocolli definiti *supra* nell'*Area reati contro la P.A. e contro il Patrimonio della P.A., lettera G), comma 2: Gestione delle attività strumentali alla commissione dei reati contro la P.A., selezione e assunzione del personale*, mentre per la gestione del processo di affidamento di incarichi di consulenza o prestazioni occasionali, valgono le prescrizioni definite *supra* nell'*Area reati contro la P.A. e contro il Patrimonio della P.A., lettera G), comma 3: Gestione delle attività strumentali alla commissione dei reati contro la P.A., affidamento di incarichi legali e di consulenza*.

Inoltre, vigono i seguenti obblighi e precetti:

- divieto di assumere lavoratori stranieri privi del permesso di soggiorno o comunque in stato irregolare, con obbligo di acquisire la relativa documentazione e monitorare i conseguenti termini di scadenza. Le competenti strutture aziendali, nel compiere la selezione delle controparti destinate a fornire particolari servizi (quali, ma non solo, imprese con alta incidenza di manodopera non qualificata), devono svolgere tali attività valutando anche l'affidabilità di tali controparti ai fini della prevenzione dei reati di cui alla presente parte speciale, anche attraverso specifiche indagini *ex ante*;
- richiesta esplicita di impegno ai fornitori del rispetto degli obblighi di legge in tema di occupazione di lavoratori stranieri, tutela del lavoro minorile e delle donne, ed in generale ai sensi del D.Lgs. 231/2001;
- definizione di meccanismi di monitoraggio che consentano di evitare l'impiego e o l'ingresso di professionisti con permesso di soggiorno non regolare o per cui non sia stata inoltrata la relativa domanda di rinnovo entro i tempi o con permesso di soggiorno scaduto o revocato o con permesso di soggiorno per motivi differenti dal lavoro;
- applicazione di specifiche misure sanzionatorie ove le previste attività di verifica non siano state rispettate;
- documentazione ed archiviazione del processo di ricerca, selezione e assunzione di personale.

C) Rilascio di dichiarazioni all'Autorità Giudiziaria

La situazione in oggetto è quella presa di mira dall'art. 377 bis c.p. (reato presupposto dall'art. 25 decies), che punisce «*chiunque, con violenza o minaccia, o con offerta o promessa di denaro o di altra utilità, induce a non rendere dichiarazioni o a rendere dichiarazioni mendaci la persona chiamata a rendere davanti alla autorità giudiziaria dichiarazioni utilizzabili in un procedimento penale, quando questa ha la facoltà di non rispondere*».

A tale riguardo, la Società richiede e vigila affinché vi sia una fattiva collaborazione a non rendere dichiarazioni mendaci, reticenti, o non esaustivamente rappresentative dei fatti e della verità. Quindi:

- è vietato coartare o indurre, in qualsiasi forma e con qualsiasi modalità (anche nel malinteso interesse di "agevolare" la Società), i soggetti chiamati dall'Autorità Giudiziaria a rendere dichiarazioni non veritiere o ad avvalersi (ove indagati) della facoltà di non rispondere;
- è vietato porre in essere o dare causa a comportamenti che, individualmente o collettivamente, integrino direttamente o indirettamente la fattispecie di reato di cui all'art. 377 bis del Codice Penale;

A fronte del rischio di tali possibili comportamenti illeciti, corrisponde il preciso dovere delle funzioni apicali (ove messe a conoscenza della situazione *de qua*) di vigilare affinché i soggetti chiamati a rendere dichiarazioni dinanzi all'Autorità Giudiziaria:

- comprendano l'importanza del loro obbligo di testimoniare (nel caso in cui siano chiamati come testimoni e non come indagati);
- decidano liberamente se avvalersi o meno della facoltà di non rispondere (nel caso in cui rivestano la qualifica di indagati);
- siano messi nella condizione psicologica di riferire all'Autorità Giudiziaria quanto a loro conoscenza in assoluta libertà e senza correre il rischio di alcun condizionamento (esterno, interno, o di natura lato sensu "gerarchica");
- possano esprimere liberamente le proprie rappresentazioni dei fatti o di esercitare la facoltà di non rispondere accordata dalla legge, in particolare per coloro i quali dovessero risultare indagati o imputati in un procedimento penale, anche connesso, inerente l'attività lavorativa prestata nella Società;
- possano avvertire tempestivamente l'Organismo di Vigilanza: a) di ogni atto, citazione a testimoniare e procedimento giudiziario (civile, penale o amministrativo) che li veda coinvolti, sotto qualsiasi profilo, in rapporto all'attività lavorativa prestata o comunque ad essa attinente; b) di ogni violenza o minaccia, pressione, offerta o promessa di danaro o altra utilità, ricevuta al fine di avvalersi della facoltà di non rispondere o di rendere dichiarazioni non veritiere all'Autorità Giudiziaria.

Il Responsabile della funzione Risorse Umane - pur senza entrare nel merito della eventuale dichiarazione resa o da rendere (si ricordi, infatti, che le dichiarazioni in oggetto, soprattutto nella fase delle Indagini Preliminari, sono rigorosamente coperte dal segreto istruttorio) - dovrà cautamente verificare che la stessa dichiarazione sarà, o sia stata, resa serenamente e senza alcun tipo di induzione o pressione da parte di alcuno ed informare tempestivamente l'OdV.

Area Gestione Risorse Informatiche

La premessa da cui partire ai fini di meglio comprendere la sensibilità dell'area in oggetto è che i lavoratori e i collaboratori della società possono essere dotati di postazioni di lavoro personali, attraverso le quali accedono ai sistemi e ai servizi informatici aziendali per lo svolgimento delle attività di propria competenza. Tra i servizi aziendali di base a cui hanno accesso tutti i dipendenti e collaboratori ci sono, in particolare, la posta elettronica ed il web.

L'utilizzo di strumenti e tecnologie informatiche è, quindi, estremamente diffuso e trasversale alle diverse aree funzionali e operative dell'Azienda. Questa elevata diffusione e

trasversalità, determinata dalle esigenze di business, fa nascere la necessità di analizzare e controllare i rischi connessi agli utilizzi non ammessi o illeciti degli stessi strumenti informatici.

In particolare, devono essere analizzate e controllate le casistiche e gli scenari in cui un illecito informatico commesso da un dipendente o da un collaboratore può determinare un interesse o vantaggio per l'Azienda, configurando la responsabilità della Società secondo quanto disposto dal D.lgs. 231/01. Fondamentale è l'indicazione delle modalità di trattamento ed i requisiti dei dati trattati, individuati i necessari presupposti di liceità.

Il presente Modello 231 richiede che tutte le attività svolte dalla Società debbano essere compiute secondo i *principi di sicurezza delle informazioni* e la cogente l'applicazione dei *Protocolli Generali*, intesi come *standard precauzionali/preventivi generali*.

Più in generale, non devono essere adottati comportamenti illeciti o non conformi nell'elaborazione delle informazioni che possano procurare un profitto illecito all'Azienda nell'ambito dell'utilizzo e nell'esercizio dei sistemi a supporto dei processi di gestione aziendale, nella gestione dei rapporti con la P.A. e nell'utilizzo degli strumenti informatici aziendali che consentono l'accesso ai siti internet e di pubblica utilità.

Per ciò che poi, specificamente, concerne il corretto e legittimo uso di macchine (computer, smart phone, tablet, etc.) da parte del personale della Società, nonché di tutti coloro che collaborano con la stessa ed hanno la materiale disponibilità di computer o postazioni internet messe a loro disposizione, il Codice Etico e di Comportamento detta precise regole di condotta, sia ai fini di una legittima, corretta e morale, utilizzazione del mezzo informatico *per soli ed esclusivi motivi di lavoro e necessità aziendali*, sia in relazione alla protezione dello stesso mezzo informatico quale bene materiale aziendale da proteggere e non danneggiare.

Qualunque tipo di inosservanza o di inottemperanza a tali obblighi – di natura etica e/o più strettamente contrattuale (v. contratto di lavoro) - comporterà sanzioni di natura disciplinare nonché, nei casi più gravi, l'immediato licenziamento per giusta causa.

Accanto all'adozione di accorgimenti tecnici atti ad evitare azioni di danneggiamento, interpolazione, alterazione dati, installazione fraudolenta di programmi o apparecchiature di natura illecita, devono comunque essere previsti periodici controlli e verifiche da parte del personale addetto.

I sistemi informatici devono, infine, tutelare la riservatezza dei dati personali e garantire ad essi la protezione necessaria da ogni evento che possa metterli a rischio di violazione, nel pieno rispetto del Regolamento dell'Unione Europea n. 2016/679 ("GDPR") ed in particolare del suo art. 13.

Tra le attività maggiormente esposte a rischi di reato sono state individuate: A) Politiche di gestione della risorsa informatica; B) Gestione strategica dei Sistemi Informativi (accessi, account, profili e sistemi software); C) Gestione dei sistemi informativi (servizi di rete, sistemi hardware, accessi fisici); D) Gestione dell'hardware per la firma digitale (es. le smart card); E) Gestione e sicurezza della documentazione in formato digitale; F) Gestione degli acquisti e utilizzo di programmi s/w; G) Gestione degli accessi fisici ai locali ove risiedono le infrastrutture IT; H) Violazione dei diritti d'autore.

A) Politiche di gestione della risorsa informatica

È buona prassi definire le Politiche di Gestione della risorsa informatica e della sua sicurezza, che deve essere redatta, formalmente approvata, aggiornata periodicamente e comunicata a tutto il personale aziendale. nell'ambito delle suddette Politiche:

- la funzione "amministratore macchina" deve essere in capo solo ed esclusivamente al Responsabile dei Servizi Informatici;
- la gestione del *back up* deve essere disciplinata da una procedura in cui siano definite le attività di *back up* per ogni rete di telecomunicazione, la frequenza dell'attività, le modalità, il numero di copie, il periodo di conservazione dei dati;
- devono essere previsti, a fronte di eventi disastrosi, piani di *Business Continuity* e di *Disaster Recovery*, al fine di garantire la continuità dei sistemi informativi e dei processi ritenuti critici;
- devono esser disciplinate da apposite formali procedure la generazione e la protezione dei *log* delle attività sui sistemi, almeno nel contesto delle attività relative a dati sensibili;
- deve essere regolamentata da procedure la rilevazione e risoluzione degli incidenti di sicurezza logica deve esser regolamentata. Nelle procedure devono essere: a) definiti i criteri di classificazione degli incidenti ed i livelli di *escalation* (a seconda della tipologia dell'anomalia segnalata); b) previste le comunicazioni degli stessi ai soggetti interessati; c) condotte attività di *reporting* sui risultati ottenuti;
- devono essere previste direttive aziendali per favorire la segnalazione di fattispecie a rischio di reati informatici rilevati da dipendenti e collaboratori durante l'utilizzo dei servizi informatici aziendali.

B) Gestione strategica dei sistemi informativi (accessi, account, profili e sistemi software)

- Osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informativi e per il corretto utilizzo delle risorse informatiche aziendali.
- Osservare ogni altra norma o procedura specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati, applicazioni e sistemi dell'azienda.
- Utilizzare unicamente applicazioni/software preventivamente approvate dalla funzione Sistemi Informativi e impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa.
- Astenersi dall'effettuare copie non specificamente autorizzate di dati e software.
- Evitare di lasciare incustodito e/o accessibile ad altri il proprio computer e non prestare o cedere a terzi qualsiasi apparecchiatura informatica senza la preventiva autorizzazione del Responsabile dei Sistemi Informativi. In caso di smarrimento o furto, informare tempestivamente la funzione Sistemi Informativi e l'ufficio Amministrativo e presentare denuncia all'Autorità Giudiziaria preposta.
- Definire formalmente i requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori.
- Individuare univocamente i codici identificativi (user-id) per l'accesso alle applicazioni ed alla rete.

- Definire i criteri e le modalità per la creazione e gestione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (es. lunghezza minima della password, regole di complessità, scadenza).
- Verificare periodicamente gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete.
- Tenere traccia delle modifiche ai dati e alle applicazioni compiute dagli utenti.
- Evitare l'utilizzo di password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile dei Sistemi Informativi; qualora si venisse incolpevolmente a conoscenza della password di altro utente, darne immediata notizia alla funzione Sistemi Informativi.
- Evitare di detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di colleghi, soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate.
- Evitare di trasferire all'esterno della Società e/o trasmettere file, documenti, o qualsiasi altra documentazione riservata di proprietà dell'azienda stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio Responsabile.
- Evitare di svolgere attività di modifica e/o cancellazione/distruzione di dati, informazioni o programmi di pubblica utilità e alterare documenti informatici, pubblici o privati, aventi efficacia probatoria.
- Definire i ruoli organizzativi in una matrice autorizzativa: applicazioni/profili/richiedente.
- Definire i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente.
- Attuare verifiche periodiche dei profili utente e della coerenza degli stessi con le responsabilità assegnate.
- Archiviare la documentazione riguardante ogni singola attività allo scopo di garantire la completa tracciabilità della stessa.
- Definire i criteri e le modalità per la gestione dei sistemi software che prevedano la compilazione e manutenzione di un inventario aggiornato del software in uso presso la Società, l'utilizzo di software formalmente autorizzato e certificato e l'effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare la presenza di software proibiti e/o potenzialmente nocivi.

C) Gestione dei sistemi informativi (servizi di rete, sistemi hardware, accessi fisici)

- Prevedere, nella gestione dei sistemi hardware, la compilazione e l'aggiornamento dell'inventario dell'hw in uso presso la Società;
- Regolamentare le responsabilità e le modalità operative di intervento in caso di implementazione e/o manutenzione hardware.
- Definire le responsabilità per la gestione delle reti.
- Implementare i controlli di sicurezza al fine di garantire la riservatezza dei dati interni alla rete e in transito su reti pubbliche.
- Adottare meccanismi di segregazione delle reti e di monitoraggio del traffico di rete.

- Implementare e manutenereregolarmente le reti telematiche, mediante la definizione delle responsabilità e delle modalità operative di gestione. Attuare verifiche periodiche sul funzionamento delle reti e rilevare le anomalie riscontrate. Regolamentare l'esecuzione di attività periodiche di *vulnerability assessment*.
- Prevedere, per ogni rete di telecomunicazione, la frequenza dell'attività, le modalità, il numero di copie e il periodo di conservazione dei dati, per le attività di *back-up*.
- Definire le misure di sicurezza adottate, le modalità di vigilanza e la relativa frequenza, le responsabilità, il processo di reporting delle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza, e le contromisure da attivare.

D) Gestione degli strumenti per la firma digitale (es. le smart card)

- Formalizzare il processo di gestione in una procedura operativa o policy interna.
- Definire criteri e modalità per la generazione, distribuzione, revoca e archiviazione delle chiavi (smart card).
- Disciplinare formalmente l'eventuale gestione dei documenti in formato digitale da parte di soggetti terzi.
- Definire i controlli per la protezione delle chiavi da possibili modifiche, distruzioni e utilizzi non autorizzati.
- Tracciare e archiviare la documentazione di supporto alle attività effettuate con l'utilizzo dei documenti in formato digitale.

E) Gestione e sicurezza della documentazione in formato digitale

- Utilizzare tecniche di crittografia per la protezione e la trasmissione delle informazioni riservate.
- Realizzare un sistema di protezione delle "chiavi" da possibili modifiche, distruzioni, utilizzi non autorizzati.
- Realizzare un sistema di gestione delle "chiavi" a sostegno dell'uso delle tecniche crittografiche per la generazione, distribuzione, revoca ed archiviazione delle stesse.
- Formalizzare le procedure che regolamentano la gestione dell'utilizzo della firma digitale nei documenti, disciplinandone: responsabilità; livelli autorizzativi; regole di adozione di sistemi di certificazione; utilizzo e invio dei documenti; modalità di archiviazione e distruzione degli stessi.

F) Gestione degli acquisti e utilizzo di programmi s/w

- Centralizzare in un'unica funzione aziendale la gestione degli acquisti dei prodotti informatici.
- Acquistare solo software ufficiali certificati e si controlli la data di scadenza delle licenze al fine di provvedere per tempo ai singoli rinnovi.
- Predisporre l'inventario aggiornato dei software presenti in azienda e si programmino verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso.
- Definire, con procedure formalizzate, il processo di *change management*, inteso come manutenzione al software esistente o nuove implementazioni.
- Implementare e applicare un sistema di controllo per individuare i computer su cui sono stati eventualmente installati programmi non autorizzati.

G) Gestione degli accessi fisici ai locali ove risiedono le infrastrutture IT

- Prevedere, per la gestione della sicurezza fisica dei siti ove risiedono le infrastrutture, una apposita procedura formalizzata con le misure di sicurezza adottate, le modalità di vigilanza, la frequenza, le responsabilità, il processo di reporting delle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza, le contromisure da attivare;
- Proteggere e regolamentare l'accesso fisico ai locali riservati in cui risiedono le infrastrutture ICT mediante l'utilizzo di codici di accesso, *token authenticator*, *pin*, *badge*, etc.;
- Effettuare controlli periodici sulla corrispondenza delle abilitazioni concesse ed il ruolo ricoperto dall'utente autorizzato.

H) Violazione dei diritti d'autore

- Approntare idonei sistemi di controllo al fine di evitare l'abusiva riproduzione e/o utilizzo di software per il quale è prescritta, ai sensi della Legge sul Diritto D'Autore, l'apposizione di contrassegno da parte della S.I.A.E.
- Non riprodurre o duplicare i supporti in cui sono contenute le opere tutelate dal diritto di autore, senza averne acquisito i relativi diritti.
- Adottare adeguati processi di controllo per verificare che il software e ogni altro eventuale elemento digitale tutelato da proprietà intellettuale siano utilizzati nel rispetto delle condizioni di licenza prescritte dall'autore.
- Richiedere le necessarie informazioni al Responsabile Sistemi Informatici in caso di dubbi circa l'esistenza del diritto di sfruttamento economico del prodotto o in merito ai termini di sfruttamento. L'erroneo utilizzo di un'opera di terzi tutelata dal diritto d'autore, impropriamente diffusa, dovrà essere immediatamente segnalato alla funzione Sistemi Informatici per le azioni di *remediation* più opportune.

Area Sicurezza Lavoratori

Come chiarito in sede di *crime risk assessment,* in *ADR Trasporti S.R.L.* il rischio di consumazione dei delitti di *omicidio colposo* e *lesioni colpose* ex art. 25 septies D.Lgs. 231/2001, in conseguenza di violazione della normativa sulla sicurezza nei luoghi di lavoro, è da considerare giuridicamente - a titolo prudenziale e di cautela avanzata - "molto alto".

La normativa di riferimento generale in materia di "sicurezza sui luoghi di lavoro" è costituita dal D.Lgs. 9 aprile 2008 n. 81, per come aggiornato e modificato dal D.Lgs. 3 agosto 2009 n. 106, nonché dalla correlata legislazione specialistica, di primo e di secondo livello.

In *ADR Trasporti S.R.L.* riveste, poi, un ruolo centrale l'Accordo Europeo relativo ai trasporti internazionali di merci pericolose su strada, siglato a Ginevra il 30 settembre 1957 sotto gli auspici della Commissione Economica per l'Europa dell'ONU - UNECE.

Quest'ultima regolamentazione è stata recepita in Italia dalla Legge 12 agosto 1962, n. 1839 (*Ratifica ed esecuzione dell'Accordo europeo relativo al trasporto internazionale di merci pericolose su strada, con annessi Protocollo ed Allegati, adottato a Ginevra il 30 settembre 1957*).

Il quadro dei soggetti e dei protocolli fondamentali a salvaguardia del *sistema di sicurezza sui luoghi di lavoro* rimane, comunque, dettato dalla "legge madre" ex D.Lgs. 91/2008, la quale individua esattamente: 1) i *soggetti* che agiscono in veste di titolari della "posizione di garanzia" nei confronti dei lavoratori; 2) le doverose *azioni preventive* da compiere.

Nel dettaglio, l'art. 15 del D.Lgs. 81/2008, l'art. 15 detta le seguenti *"misure generali di tutela"*:

«1. Le misure generali di tutela della salute e della sicurezza dei lavoratori nei luoghi di lavoro sono:

a) la valutazione di tutti i rischi per la salute e sicurezza;

b) la programmazione della prevenzione, mirata ad un complesso che integri in modo coerente nella prevenzione le condizioni tecniche produttive dell'azienda nonché l'influenza dei fattori dell'ambiente e dell'organizzazione del lavoro;

c) l'eliminazione dei rischi e, ove ciò non sia possibile, la loro riduzione al minimo in relazione alle conoscenze acquisite in base al progresso tecnico;

d) il 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, in particolare al fine di ridurre gli effetti sulla salute del lavoro monotono e di quello ripetitivo;

e) la riduzione dei rischi alla fonte;

f) la sostituzione di ciò che è pericoloso con ciò che non lo è, o è meno pericoloso;

g) la limitazione al minimo del numero dei lavoratori che sono, o che possono essere, esposti al rischio;

h) l'utilizzo limitato degli agenti chimici, fisici e biologici sui luoghi di lavoro;

i) la priorità delle misure di protezione collettiva rispetto alle misure di protezione individuale;

l) il controllo sanitario dei lavoratori;

m) l'allontanamento del lavoratore dall'esposizione al rischio per motivi sanitari inerenti la sua persona e l'adibizione, ove possibile, ad altra mansione;

n) l'informazione e formazione adeguate per i lavoratori;

o) l'informazione e formazione adeguate per dirigenti e i preposti;

p) l'informazione e formazione adeguate per i rappresentanti dei lavoratori per la sicurezza;

q) l'istruzioni adeguate ai lavoratori;

r) la partecipazione e consultazione dei lavoratori;

s) la partecipazione e consultazione dei rappresentanti dei lavoratori per la sicurezza;

t) la 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;

u) le misure di emergenza da attuare in caso di primo soccorso, di lotta antincendio, di evacuazione dei lavoratori e di pericolo grave e immediato;

v) l'uso di segnali di avvertimento e di sicurezza;

z) la regolare manutenzione di ambienti, attrezzature, impianti, con particolare riguardo ai dispositivi di sicurezza in conformità alla indicazione dei fabbricanti».

I principali soggetti - responsabili dell'intero processo sono:

❒ Il **Datore di Lavoro**, che insieme ai dirigenti, in base a quanto disposto dall'art. 18 (*Obblighi del datore di lavoro e del dirigente*), dovrà:

«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;
b-bis) individuare il preposto o i preposti per l'effettuazione delle attività di vigilanza di cui all'articolo 19. I contratti e gli accordi collettivi di lavoro possono stabilire l'emolumento spettante al preposto per lo svolgimento delle attività di cui al precedente periodo. Il preposto non può subire pregiudizio alcuno a causa dello svolgimento della propria attività;
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, 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;
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), anche su supporto informatico come previsto dall'articolo 53, comma 5, 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, 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;

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. 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;

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.

……..

2. Il datore di lavoro fornisce al servizio di prevenzione e protezione ed al medico competente informazioni in merito a:

a) la natura dei rischi;

b) l'organizzazione del lavoro, la programmazione e l'attuazione delle misure preventive e protettive;

c) la descrizione degli impianti e dei processi produttivi;

d) i dati di cui al comma 1, lettera r), e quelli relativi alle malattie professionali;

e) i provvedimenti adottati dagli organi di vigilanza.

……..

3-bis. Il datore di lavoro e i dirigenti sono tenuti altresì a vigilare in ordine all'adempimento degli obblighi di cui agli articoli 19, 20, 22, 23, 24 e 25, ferma restando l'esclusiva responsabilità dei soggetti obbligati ai sensi dei medesimi articoli qualora la mancata attuazione dei predetti obblighi sia addebitabile unicamente agli stessi e non sia riscontrabile un difetto di vigilanza del datore di lavoro e dei dirigenti».

Il Datore di lavoro dovrà inoltre:

- Elaborare e redigere (quale attività non delegabile ad alcuno, secondo quanto disposto dall'art. 17) il *Documento di Valutazione Rischi* - da tenere costantemente aggiornato - in base ai criteri e agli elementi stabiliti dagli artt. 28 e 29, ossia in collaborazione con i Responsabile Servizio Prevenzione e Protezione e con il Medico Competente, oltre che previa consultazione del Rappresentante Lavoratore per la Sicurezza.
- Designare il Responsabile del Servizio Prevenzione e Protezione dei Rischi (a meno che, ai sensi dell'art. 34, non ricorrano i presupposti affinchè tale ruolo possa essere ricoperto dallo stesso Datore di Lavoro). Anche tale designazione, al pari della elaborazione del Documento di Valutazione Rischi, non è delegabile (art. 17).
- Effettuare tutte le azioni obbligatorie di cui all'art. 18;
- Indire, al meno una volta all'anno, la "riunione periodica" ex art. 35, a cui partecipano lui stesso o un suo rappresentante, il Responsabile del Servizio di Prevenzione e Protezione dai rischi, il Medico Competente e il Rappresentante dei Lavoratori per la Sicurezza, nella quale vengono sottoposti all'esame dei partecipanti: a) il Documento di Valutazione dei Rischi; b) l'andamento degli infortuni e delle malattie professionali e della sorveglianza sanitaria; c) i criteri di scelta, le caratteristiche tecniche e l'efficacia dei dispositivi di protezione individuale; d) i programmi di informazione e formazione dei dirigenti, dei preposti e dei lavoratori ai fini della sicurezza e della protezione della loro salute; nonché individuati si individuano i codici di condotta e le buone prassi per prevenire i rischi di infortuni e di malattie professionali e gli obiettivi di miglioramento della sicurezza complessiva.

❒ I **Preposti**, la cui individuazione e nomina è stata prevista come obbligatoria dal D.L. 21 ottobre 2021, n. 146 convertito in Legge 17 dicembre 2021, n. 215 (recante *Misure urgenti in materia economica e fiscale, a tutela del lavoro e per esigenze indifferibili*).

In base all'art. 19, i Preposti devono:

« a) sovrintendere e vigilare sull'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 rilevazione di comportamenti non conformi alle disposizioni e istruzioni impartite dal datore di lavoro e dai dirigenti ai fini della protezione collettiva e individuale, intervenire per modificare il comportamento non conforme fornendo le necessarie indicazioni di sicurezza. In caso di mancata attuazione delle disposizioni impartite o di persistenza dell'inosservanza, interrompere l'attività del lavoratore e informare i 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;
f-bis) in caso di rilevazione di deficienze dei mezzi e delle attrezzature di lavoro e di ogni condizione di pericolo rilevata durante la vigilanza, se necessario, interrompere temporaneamente l'attività e, comunque, segnalare tempestivamente al datore di lavoro e al dirigente le non conformità rilevate;
g) frequentare appositi corsi di formazione secondo quanto previsto dall'art. 37»

❒ I **Lavoratori**, i quali dovranno rispettare gli obblighi di cui all'art. 20:
«*1. Ogni lavoratore deve 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.*
2. I lavoratori 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 miscele pericolose, i mezzi di trasporto, 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 lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;
f) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo;
g) 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;
h) partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;
i) sottoporsi ai controlli sanitari previsti dal presente decreto legislativo o comunque disposti dal medico competente.

3. I lavoratori di aziende che svolgono attività in regime di appalto o subappalto, devono esporre apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro. Tale obbligo grava anche in capo ai lavoratori autonomi che esercitano direttamente la propria attività nel medesimo luogo di lavoro, i quali sono tenuti a provvedervi per proprio conto».

❒ Il **Medico Competente**, il quale dovrà rispettare gli obblighi dell'art. 25:

«a) collabora con il datore di lavoro e con il servizio di prevenzione e protezione alla valutazione dei rischi, anche ai fini della programmazione, ove necessario, della sorveglianza sanitaria, alla predisposizione della attuazione delle misure per la tutela della salute e della integrità psico-fisica dei lavoratori, all'attività di formazione e informazione nei confronti dei lavoratori, per la parte di competenza, e alla organizzazione del servizio di primo soccorso considerando i particolari tipi di lavorazione ed esposizione e le peculiari modalità organizzative del lavoro. Collabora inoltre alla attuazione e valorizzazione di programmi volontari di «promozione della salute», secondo i principi della responsabilità sociale;

b) programma ed effettua la sorveglianza sanitaria di cui all'articolo 41 attraverso protocolli sanitari definiti in funzione dei rischi specifici e tenendo in considerazione gli indirizzi scientifici più avanzati;

d) istituisce, aggiorna e custodisce, sotto la propria responsabilità, una cartella sanitaria e di rischio per ogni lavoratore sottoposto a sorveglianza sanitaria; tale cartella e' conservata con salvaguardia del segreto professionale e, salvo il tempo strettamente necessario per l'esecuzione della sorveglianza sanitaria e la trascrizione dei relativi risultati, presso il luogo di custodia concordato al momento della nomina del medico competente;

d) consegna al datore di lavoro, alla cessazione dell'incarico, la documentazione sanitaria in suo possesso, nel rispetto delle disposizioni di cui al decreto legislativo del 30 giugno 2003, n. 196, e con salvaguardia del segreto professionale;

e) consegna al lavoratore, alla cessazione del rapporto di lavoro, copia della cartella sanitaria e di rischio, e gli fornisce le informazioni necessarie relative alla conservazione della medesima; l'originale della cartella sanitaria e di rischio va conservata, nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196, da parte del datore di lavoro, per almeno dieci anni, salvo il diverso termine previsto da altre disposizioni del presente decreto;

f) (lettera soppressa)

g) fornisce informazioni ai lavoratori sul significato della sorveglianza sanitaria cui sono sottoposti e, nel caso di esposizione ad agenti con effetti a lungo termine, sulla necessità di sottoporsi ad accertamenti sanitari anche dopo la cessazione della attività che comporta l'esposizione a tali agenti. Fornisce altresì, a richiesta, informazioni analoghe ai rappresentanti dei lavoratori per la sicurezza;

h) informa ogni lavoratore interessato dei risultati della sorveglianza sanitaria di cui all'articolo 41 e, a richiesta dello stesso, gli rilascia copia della documentazione sanitaria;

i) comunica per iscritto, in occasione delle riunioni di cui all'articolo 35, al datore di lavoro, al responsabile del servizio di prevenzione protezione dai rischi, ai rappresentanti dei lavoratori per la sicurezza, i risultati anonimi collettivi della sorveglianza sanitaria effettuata e fornisce indicazioni sul significato di detti risultati ai fini della attuazione delle misure per la tutela della

salute e della integrità psico-fisica dei lavoratori;
l) visita gli ambienti di lavoro almeno una volta all'anno o a cadenza diversa che stabilisce in base alla valutazione dei rischi la indicazione di una periodicità diversa dall'annuale deve essere comunicata al datore di lavoro ai fini della sua annotazione nel documento di valutazione dei rischi;
m) partecipa alla programmazione del controllo dell'esposizione dei lavoratori i cui risultati gli sono forniti con tempestività ai fini della valutazione del rischio e della sorveglianza sanitaria;
n) comunica, mediante autocertificazione, il possesso dei titoli e requisiti di cui all'articolo 38 al Ministero del lavoro, della salute e delle politiche sociali entro il termine di sei mesi dalla data di entrata in vigore del presente decreto.

❒ Il **Responsabile del Servizio Prevenzione e Protezione**, il quale - in possesso delle capacità e dei requisiti professionali richiesti dagli artt. 31-32 - riveste i compiti fissati dall'art. 33, ossia provvede:
«a) all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
b) ad elaborare, per quanto di competenza, le misure preventive e protettive di cui all'articolo 28, comma 2, e i sistemi di controllo di tali misure;
b) ad elaborare le procedure di sicurezza per le varie attività aziendali;
c) a proporre i programmi di informazione e formazione dei lavoratori;
d) a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica di cui all'articolo 35;
f) a fornire ai lavoratori le informazioni di cui all'articolo 36[19]».

Accanto a queste figure obbligatorie, il D.Lgs. 81/2008 ne prevede altre, facoltative ed eventuali, tra cui:

A) l'**Addetto al Servizio di Prevenzione e Protezione** (il quale deve essere in possesso dei requisiti minimi di un titolo di studio non inferiore al diploma di istruzione secondaria

[19] *Art. 36 (Informazioni ai lavoratori): « Il datore di lavoro provvede affinché ciascun lavoratore riceva una adeguata informazione:*
a) sui rischi per la salute e sicurezza sul lavoro connessi alla attività della impresa in generale;
b) sulle procedure che riguardano il primo soccorso, la lotta antincendio, l'evacuazione dei luoghi di lavoro;
c) sui nominativi dei lavoratori incaricati di applicare le misure di cui agli articoli 45 e 46;
d) sui nominativi del responsabile e degli addetti del servizio di prevenzione e protezione, e del medico competente.
2. Il datore di lavoro provvede altresì affinché ciascun lavoratore riceva una adeguata informazione:
a) sui rischi specifici cui è esposto in relazione all'attività svolta, le normative di sicurezza e le disposizioni aziendali in materia;
b) sui pericoli connessi all'uso delle sostanze e dei preparati pericolosi sulla base delle schede dei dati di sicurezza previste dalla normativa vigente e dalle norme di buona tecnica;
c) sulle misure e le attività di protezione e prevenzione adottate.
3. Il datore di lavoro fornisce le informazioni di cui al comma 1, lettera a), e al comma 2, lettere a), b) e c), anche ai lavoratori di cui all'articolo 3, comma 9.
4. Il contenuto della informazione deve essere facilmente comprensibile per i lavoratori e deve consentire loro di acquisire le relative conoscenze. Ove la informazione riguardi lavoratori immigrati, essa avviene previa verifica della comprensione della lingua utilizzata nel percorso informativo».

superiore e di una formazione specifica), quale figura di ausilio/supporto del Datore di Lavoro e del RSPP;

B) il **Delegato alla Sicurezza sui luoghi di lavoro** ex art. 16.

Quest'ultima è una figura che, già applicata in via giurisprudenziale, è stata formalizzata dall'art. 16, al fine di mitigare la responsabilità del Datore di Lavoro rispetto alla complessità e ricchezza degli obblighi/doveri gravanti su di lui.

Il Sistema ha, tuttavia, limitato il margine di operatività della predetta "delega di funzione" – onde scongiurare un possibile abbassamento dei livelli di vigilanza e di controllo a scapito della salute dei lavoratori - attraverso due precise clausole:

- la non delegabilità della "*valutazione di tutti i rischi con la conseguente elaborazione del documento previsto dall'art. 28"* e della *"designazione del responsabile del servizio di prevenzione e protezione dai rischi*" (art. 17, D.Lgs. 81/2008);
- l'*"obbligo di vigilanza in capo al Datore di Lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite*" (art. 16 cit. D.Lgs. 81/2008).

La *Delega di Funzioni,* per essere valida ed efficace, deve obbligatoriamente rispettare i requisiti di forma e di sostanza richiesti dall'art.16:

«1. La delega di funzioni da parte del datore di lavoro, ove non espressamente esclusa, è ammessa con i seguenti limiti e condizioni:

a) che essa risulti da atto scritto recante data certa;

b) che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;

c) che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;

d) che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;

e) che la delega sia accettata dal delegato per iscritto.

2. Alla delega di cui al comma 1 deve essere data adeguata e tempestiva pubblicità.

3. La delega di funzioni non esclude l'obbligo di vigilanza in capo al datore di lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite. L'obbligo di cui al primo periodo si intende assolto in caso di adozione ed efficace attuazione del modello di verifica e controllo di cui all'articolo 30, comma 4[20].

3-bis. Il soggetto delegato può, a sua volta, previa intesa con il datore di lavoro delegare specifiche funzioni in materia di salute e sicurezza sul lavoro alle medesime condizioni di cui ai commi 1 e 2. La delega di funzioni di cui al primo periodo non esclude l'obbligo di vigilanza in capo al delegante in ordine al corretto espletamento delle funzioni trasferite. Il soggetto al quale sia stata conferita la delega di cui al presente comma non può, a sua volta, delegare le funzioni delegate».

[20] *Art. 30 (Modelli di Organizzazione e Gestione): «…. 4. Il modello organizzativo deve altresì prevedere un idoneo sistema di controllo sull'attuazione del medesimo modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Il riesame e l'eventuale modifica del modello organizzativo devono essere adottati, quando siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico….».*

Agli specifici fini del Modello, le attività sensibili del processo *Sicurezza sui Luoghi di Lavoro* sono:

A) attività a rischio di infortunio e malattia professionale, mutuate dal Documento di Valutazione dei Rischi aziendale di cui all'art. 28, D.Lgs. 81/2008, redatto dal Datore di Lavoro ed intese come le attività dove potenzialmente si possono materializzare gli infortuni e le malattie professionali.

B) attività a rischio di reato, intese come quelle che possono potenzialmente determinare i reati di cui all'art. *25-septies* del D.Lgs. 231/2001 - in quanto una loro omissione o un'inefficace attuazione potrebbe integrare una responsabilità colposa - e che costituiscono anche l'elemento centrale per adottare ed attuare efficacemente un sistema idoneo all'adempimento di tutti gli obblighi giuridici richiesti dalla normativa vigente sulla salute e sicurezza sul lavoro.

Nell'espletamento delle attività e delle funzioni previste dai propri ruoli, oltre a quanto previsto nei *Protocolli Generali*, tutti i Destinatari del Modello 231 sono tenuti a conoscere e a rispettare i *Protocolli Speciali* della presente area di rischio, il cui contenuto si intende sovrapponibile alle *Procedure*, *Istruzioni Operative* e *Disposizioni Aziendali*, formalizzate dalla Società e/o disposti dai Responsabili/Superiori Gerarchici nel *Sistema di Gestione Integrato*.

I documenti di valutazione dei rischi devono essere tenuti costantemente aggiornati.

Tutti i Destinatari del presente Modello, dovranno inoltre rispettare regole di condotta conformi ai principi contenuti nel Codice Etico e di Comportamento della Società, nella normativa antinfortunistica e negli strumenti di attuazione del Modello 231, al fine di prevenire il verificarsi dei reati di omicidio e lesioni colposi sopra identificati.

Area Reati Ambientali

Anche per l'*Area ambientale* vale quanto primo detto, in via generale, a proposito dei *Protocolli Speciali*: e cioè l'obbligo, costante ed incondizionato, di rispettare i *Protocolli Generali,* le *Procedure/Istruzione operative del Sistema di Gestione Integrato Sicurezza- Ambiente-Qualità,* le *Disposizioni Aziendali*, oltre ovviamente i principi del *Codice Etico e di Comportamento*.

Nell'espletamento delle attività e delle funzioni previste dai propri ruoli, tutti i Destinatari sono inoltre tenuti a conoscere e a rispettare le norme ed i principi valevoli in materia ambientale.

A quest'ultimo riguardo, ad esempio, per ciò che specificamente afferisce alla *gestione dei rifiuti*, tutti i destinatari devono avere piena consapevolezza che:

- la gestione dei rifiuti va considerata un'attività di pubblico interesse, appositamente normata per assicurare un'elevata protezione dell'ambiente, efficaci controlli, oltre a efficienza, economicità e trasparenza;
- le operazioni di recupero o smaltimento devono avvenire in condizioni di sicurezza, senza pericolo per la salute dell'uomo e senza usare procedimenti o metodi che potrebbero recare pregiudizio per l'ambiente;
- le priorità da seguire nella corretta gestione del rifiuto sono la prevenzione e riduzione della pericolosità e il loro riciclo, reimpiego e riutilizzo,

Sempre in via generale, tutti i Destinatari del Modello sono tenuti a conoscere e rispettare le *prescrizioni generali* che seguono:

- considerare sempre prevalente la necessità di tutelare l'ambiente rispetto a qualsiasi considerazione economica;
- valutare sempre gli effetti della propria condotta in relazione al rischio di danno all'ambiente;
- non adottare comportamenti imprudenti che potrebbero recare danno all'ambiente, conformemente alla normativa in vigore, alle istruzioni e ai mezzi forniti o predisposti dal Datore di Lavoro;
- utilizzare correttamente i macchinari e le attrezzature di lavoro, le sostanze e i preparati pericolosi nonché i mezzi di trasporto ed i dispositivi di sicurezza;
- astenersi dal compiere di propria iniziativa operazioni o manovre che siano suscettibili di recare danni all'ambiente;
- partecipare ai programmi di formazione e di addestramento organizzati dalla Società;
- segnalare immediatamente al datore di lavoro o a chi di dovere (in ragione delle responsabilità attribuite) le deficienze dei mezzi e dei dispositivi di protezione dell'ambiente, 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 non rimuovere o modificare i dispositivi, per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia ai responsabili competenti.

In ordine alle categorie di soggetti interessati, va ricordato che l'art. 183 del D.Lgs.152/06 definisce **Produttore** "*la persona la cui attività ha prodotto rifiuti e la persona che ha effettuato operazioni di pretrattamento o di miscuglio o altre operazioni che hanno mutato la natura o la composizione dei rifiuti*" e **Detentore** "*il produttore dei rifiuti o il soggetto che li detiene*".

Al Produttore/Detentore spettano tutte le competenze in materia di gestione dei rifiuti speciali pericolosi e non pericolosi ed in particolare:

- organizzare e sovrintendere tutte le attività relative alla gestione dei rifiuti speciali nel rispetto della normativa vigente;
- provvedere al corretto smaltimento dei rifiuti speciali controllando/predisponendo l'esatta compilazione del Formulario di Identificazione dei Rifiuti (F.I.R.);
- provvedere alla corretta identificazione e gestione dei rifiuti speciali prodotti;
- informare i propri collaboratori interessati sulle corrette procedure da adottare;
- vigilare sulla corretta gestione dei rifiuti speciali da parte dei propri collaboratori;
- curare e sovrintendere la tenuta del deposito temporaneo.

Quanto sopra premesso, ove l'Amministratore e il Responsabile del Sistema di gestione Integrata lo ritengano, potrebbe essere opportuno individuare un ***Responsabile Area Ambiente***, interno all'azienda, che - su formale delega/incarico del Legale Rappresentante - si interfacci con il Responsabile Sistema di Gestione Integrata e provveda:

- ad informarsi e vigilare su tutto ciò che riguardi, sia la materia ambientale presa legislativamente di mira dall'art. 25 undecies del D.Lgs. 231/2001, che le Procedure/Istruzioni Operative fissate dal Sistema di Gestione Integrato, anche in relazione alle specifiche condotte illecite consumabili;

- individuare tutte le possibili situazioni concrete in cui, nell'ambito dell'attività aziendale, potrebbero essere consumate le condotte delittuose e/o contravvenzionali richiamate dalla stessa legislazione;
- ricevere eventuale "delega di funzioni" rispettando i crismi dell'art. 16 D.Lgs. 81/2008 così come modificato dal D.Lgs. 106/2009;
- verificare, controllare e vigilare *in loco* affinchè le Procedure e le Istruzioni Operative del Sistema di Gestione Integrata o disposte dall'Amministratore siano rispettate e concretamente eseguite;
- verificare, controllare e vigilare affinchè la Società, ove necessario, provveda ad una corretta attività di smaltimento e/o trattamento;
- verificare, controllare e vigilare che la Società non effettui alcuna attività di trasporto dei rifiuti illecita e/o non autorizzata;
- verificare, controllare e vigilare la presenza "abusiva" di eventuali materiali e/o rifiuti di pertinenza aziendale (es. toner in relazione all'attività svolta in sede; materiale di scarto o di risulta in relazione all'attività svolta nei cantieri o nei magazzini in proprio possesso);
- verificare, controllare e vigilare che tutti i dipendenti e/o personale apicale della Società conoscano e rispettino la normativa ambientale;
- provvedere alla compilazione di specifici report sull'attività concernente il rischio di reati ambientali, o su situazioni rilevanti ai fini di una possibile commissione di condotte illecite in materia ambientale.

A titolo di completezza, si ricordano le seguenti **prescrizioni speciali:**

A) ***Criteri organizzativi ed operativi***

- Rispettare la procedura e le istruzioni operative per la raccolta e l'eventuale trattamento dei "prodotti" che possono avere origine da diverse fasi operative;
- predisporre procedure particolari per rifiuti particolarmente pericolosi (alcuni reattivi, o instabili, o cancerogeni), per la loro raccolta e la loro conservazione;
- rendere disponibili continuamente contenitori di materiale idoneo, etichettati con la denominazione della tipologia dei rifiuti, con i simboli di rischio corrispondenti;
- allocare i contenitori in zone dedicate, separati da prodotti non compatibili e protetti contro perdite ed esalazioni;
- allontanare gli scarti con frequenza periodica in relazione dalla sostanza e alla sua quantità;
- individuare alla stregua di "rifiuto" i recipienti e gli imballaggi che li contengono.
- i depositi ubicati in un locale chiuso devono avere un'aerazione permanente adeguata. Se il deposito avviene in cumuli, questi devono essere realizzati su basamenti resistenti all'azione dei rifiuti, in modo tale da impedirne il contatto col suolo;
- i depositi esterni devono essere protetti con idonee tettoie per evitare l'irraggiamento diretto dei contenitori (con conseguenti pericoli di surriscaldamento e formazione prodotti gassosi) e l'accumulo di acqua piovana nei bacini di contenimento e verificare periodicamente e dopo piogge intense lo stato dei bacini di contenimento;
- i rifiuti stoccati in cumuli ("alla rinfusa") devono essere protetti dalle acque meteoriche e dall'azione del vento;

- i recipienti, fissi e mobili, devono essere opportunamente contrassegnati con etichette o targhe, apposte sui recipienti stessi o collocate nelle aree di stoccaggio, atti ad evidenziare la natura e la pericolosità dei rifiuti; detti contrassegni devono essere ben visibili per dimensioni e collocazioni;
- le etichette ed i cartelli di cui sopra sono realizzati in conformità a quanto previsto dalla normativa in materia di segnaletica di sicurezza, per contenitori di sostanze e preparati pericolosi. Si ricorda che, a questo proposito, la normativa prevede che:
  - i recipienti utilizzati per il magazzinaggio di sostanze o preparati pericolosi devono essere muniti dell'etichettatura (pittogramma o simbolo sul colore di fondo) corrispondente;
  - l'uso di dispositivi di protezione individuale dovrà sempre essere garantito e controllato durante i travasi.

B) ***Gestione e trattamento dei rifiuti***

- è vietato l'abbandono e il deposito incontrollato di rifiuti sul suolo e nel suolo, l'immissione di rifiuti di qualsiasi genere, allo stato solido o liquido, nelle acque superficiali e sotterranee;
- non si devono riversare i rifiuti liquidi negli scarichi fognari;
- per lo smaltimento di rifiuti speciali non devono essere usati i normali cassonetti per la raccolta dei rifiuti urbani.

C) ***Acquisto di nuove attrezzature e/o sviluppo di nuovi processi***

- l'acquisto di nuove attrezzature e/o lo sviluppo di nuovi processi sono subordinati alla verifica, da parte dei Responsabili di competenza supportati dall'RSPP, del loro impatto ambientale;
- le attrezzature, i macchinari e gli impianti devono essere conformi a quanto previsto dalla normativa vigente (a titolo esemplificativo: possesso delle dichiarazioni di conformità, marcatura UE, ecc.) e, se necessario, la loro messa in funzione ed il loro utilizzo devono essere preceduti e subordinati all'esito positivo di verifiche e collaudi.

Trattandosi di materia normativa in costante corso di revisione - la cui politica di prevenzione non ha ancora raggiunto un livello di disciplina e regolamentazione analoga a quella sulla sicurezza sui luoghi di lavoro - la Società potrà/dovrà valutare l'opportunità di rivedere alcune sue procedure in materia ambientale al fine di verificare se le stesse "coprano" adeguatamente tutte le aree di rischio derivanti dall'espletamento dell'attività sociale, soprattutto in relazione alle singole commesse in corso.

La Società potrebbe altresì valutare l'opportunità della costituzione di un *ufficio di internal auditing in materia ambientale,* al fine di predisporre e vigilare azioni di razionalizzazione della prevenzione.

In via generale, rimane comunque fermo l'assoluto divieto per tutti i Destinatari del Modello 231 di porre in essere o dare causa alla realizzazione di comportamenti che, a titolo individuale o collettivo, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle considerate all'art. 25-*undecies* del Decreto 231.

L'Organismo di Vigilanza effettua specifici controlli periodici in ordine a tali attività e processi tramite l'implementazione di appositi audit; RGSI, qualora rilevasse in sede di monitoraggio e audit interno eventuali violazioni alle normative vigenti in tema ambientale, è tenuto a darne immediata comunicazione all'OdV.

3. L'ORGANISMO DI VIGILANZA DI *ADR TRASPORTI SRL*

Volendo presidiare, monitorare e vigilare, l'efficacia del proprio Modello 231 in modo quanto più razionale e capillare possibile, *ADR Trasporti S.R.L.* ha deciso di nominare un Organismo di Vigilanza a Composizione Monocratica e di affidare il relativo compito a un professionista, specialista sia nella materia del diritto penale che nella materia della compliance organizzativa.

Tale tipologia di competenze è quella espressamente suggerita anche nelle Linee Guida di Confidustria.

Si riporta di seguito lo Statuto OdV di *ADR Trasporti S.R.L.* (il Regolamento OdV sarà predisposto dall'OdV nell'ambito della sua autonomia di azione e di regolamentazione attività).

❖ STATUTO dell'Organismo di Vigilanza

Articolo 1 - Scopo ed ambito di applicazione

1. È istituito presso *ADR Trasporti S.R.L.* un organismo - di seguito denominato anche OdV - con funzioni di vigilanza e controllo in ordine al funzionamento, all'efficacia, all'adeguatezza ed all'osservanza del Modello 231, adottato dalla Società con delibera dell'Organo Amministrativo, allo scopo di prevenire i reati dai quali possa derivare la responsabilità amministrativa ex D.Lgs. 231/2001.

Articolo 2 - Nomina e composizione

1. L'Organismo di Vigilanza di *ADR Trasporti S.R.L.* è composto da un membro nominato dall'Organo Amministrativo.
2. La nomina dell'Organismo di Vigilanza da parte dell'Organo Amministrativo, deve essere resa nota ed accettata dal professionista incaricato.

Articolo 3 - Requisiti di professionalità e di onorabilità

1. Il componente cui sono affidate le funzioni dell'Organismo di Vigilanza deve assicurare un profilo personale e professionale in grado di salvaguardare l'imparzialità di giudizio, l'autorevolezza e l'eticità della condotta.
2. Devono essere, altresì, assicurati: a) una condotta, personale e professionale, moralmente ineccepibile; b) una insussistenza di conflitti di interessi con la Società che possa pregiudicare il criterio dell'indipendenza.

Articolo 4 - Durata in carica e cessazione

1. Al fine di garantire un'efficace e razionale azione di monitoraggio del Modello, nonché una sua razionale continuità, l'Organismo di Vigilanza dura in carica tre anni decorrenti dalla data di nomina. Il mandato si rinnova automaticamente e tacitamente a meno di una specifica revoca da parte dell'Organo Amministrativo. Al fine di garantire continuità di azione, alla scadenza del mandato l'Organismo continua a svolgere *pro tempore* le proprie funzioni in regime di *prorogatio.*
2. La cessazione dall'incarico può avvenire, oltre che per cause naturali, quali morte o scadenza del mandato non tacitamente rinnovato, anche per: a) il sopraggiungere di cause di incompatibilità o la sopravvenuta carenza-assenza dei requisiti previsti per l'assunzione della

carica (autonomia, indipendenza, onorabilità, professionalità); b) le dimissioni (da trasmettere all'Organo Amministrativo tramite comunicazione scritta); c) la revoca, motivata e per giusta causa, da parte dell'Organo Amministrativo.

3. Per giusta causa di revoca deve intendersi, in via esemplificativa ma non esaustiva: a) la grave e reiterata violazione degli obblighi di riservatezza previsti dal presente Statuto e dal Regolamento dell'OdV (redatto in autonomia dall'OdV stesso); b) la prolungata ed ingiustificata inattività (per almeno 9 mesi consecutivi); c) la grave negligenza nell'espletamento dei compiti connessi all'incarico; d) il conflitto di interessi permanente; e) una sentenza di condanna per uno dei reati previsti dal D.Lgs. 231/2001 o per altro reato lesivo del prestigio professionale; f) una sentenza di condanna ad una pena che comporta l'interdizione, anche temporanea, dai pubblici uffici ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese.

4. L'Organo Amministrativo, in caso di cessazione dell'incarico di OdV, provvede, il prima possibile, alla nomina del sostituto.

5. L'Organismo di Vigilanza potrà recedere in ogni momento dall'incarico mediante preavviso di almeno 3 mesi o, senza preavviso, in presenza di gravi e motivate ragioni personali/professionali.

Articolo 5 - Collocazione societaria

1. A garanzia del principio di terzietà, l'Organismo di Vigilanza è collocato in posizione di staff al vertice della società, riportando e rispondendo direttamente all'Organo Amministrativo.

Articolo 6 - Obblighi

1. L'Organismo di Vigilanza deve adempiere alle sue funzioni con la diligenza richiesta dalla natura dell'incarico e dalle sue specifiche competenze.

2. Nell'esercizio delle proprie funzioni, l'Organismo di Vigilanza deve ispirarsi a principi di autonomia ed indipendenza e deve svolgere l'incarico con continuità.

3. L'Organismo di Vigilanza è tenuto al rispetto degli obblighi di riservatezza in ordine alle notizie ed alle informazioni acquisite nell'esercizio delle sue funzioni.

4. L'OdV svolgerà le attività necessarie per la vigilanza del Modello 231 con adeguato impegno e con i necessari poteri di indagine.

5. L'OdV dovrà assicurare non meno di 4 sessioni/riunioni all'anno.

6. La definizione degli aspetti attinenti la continuità dell'azione dell'OdV (quali, ad esempio, la calendarizzazione della sua attività o la formalizzazione delle riunioni) viene rimessa all'Organismo stesso e regolata sulla base del Regolamento OdV, predisposto dallo stesso Organismo.

Articolo 7 - Cause di incompatibilità

1. Al fine di garantire l'autonomia e l'indipendenza dell'Organismo di Vigilanza, è opportuno che siano nominati solo membri esterni. L'eventuale nomina di membri interni - in ausilio di natura tecnica/logistica - è possibile solo nei confronti di soggetti privi di compiti gestionali.

2. I componenti dell'OdV non dovranno essere legati alla Società da interessi economici o da qualsiasi altra situazione di conflitto di interesse tale da inficiarne l'obiettività di giudizio.

3. Ogni eventuale situazione di conflitto di interesse sarà valutata dall'Organo Amministrativo.
4. Non potranno essere nominati componenti dell'Organismo di Vigilanza coloro i quali abbiano riportato una condanna per uno dei reati previsti dal D.Lgs. 231/2001 o per altro reato lesivo dell'onorabilità professionale.
5. Ove l'Organismo di Vigilanza incorra in una delle suddette cause di incompatibilità, l'Organo Amministrativo, esperiti gli opportuni accertamenti e sentito l'interessato, stabilisce un termine non inferiore a 30 giorni entro il quale deve cessare la situazione di incompatibilità. Trascorso tale termine senza che la predetta situazione sia cessata, l'Organo Amministrativo deve revocare il mandato.

Articolo 8 - Funzioni e compiti

1. L'OdV vigila sull'efficacia e sull'aggiornamento del Modello 231, e deve in particolare:

ii) monitorare periodicamente l'effettiva applicazione del Modello 231 da parte dei destinatari, in relazione alle diverse tipologie di reati contemplate nel D.Lgs. 231/2001, alla struttura aziendale ed alla effettiva capacità di prevenire la commissione dei reati di cui al D.Lgs. 231/2001;

iii) verificare il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello 231;

iv) verificare l'efficienza dei sistemi di controllo e di monitoraggio tesi alla ragionevole prevenzione dei reati di cui al MOGC e delle condotte illecite di cui al Codice Etico e di Comportamento;

v) vigilare sul rispetto delle modalità e delle procedure previste dal Modello e rilevare gli eventuali scostamenti comportamentali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni cui sono tenuti i responsabili delle varie funzioni;

vi) effettuare periodicamente verifiche ed ispezioni mirate su aree aziendali, operazioni ed atti posti in essere nell'ambito delle attività sensibili, o laddove si evidenzino disfunzioni del MOGC o si sia verificata la commissione di reati oggetto dell'attività di prevenzione;

vii) segnalare all'Organo Amministrativo eventuali carenze/inadeguatezze nella prevenzione dei reati, o violazioni del MOGC e del Codice Etico;

viii) condurre, anche su eventuale richiesta dell'Organo Amministrativo, o su specifiche segnalazioni interne/esterne, indagini ai fini dell'accertamento di presunte violazioni delle prescrizioni del Modello 231 o del Codice Etico e di Comportamento;

ix) prestare, su eventuale richiesta dell'Organo Amministrativo, attività di consulenza e/o di auditing su specifiche problematiche/questioni afferenti al MOGC o al Codice Etico;

x) riferire periodicamente all'Organo Amministrativo circa lo stato di attuazione e di operatività del Modello 231;

xi) segnalare all'Organo Amministrativo, per gli opportuni provvedimenti, le violazioni accertate del Modello 231 che possono comportare l'insorgenza o il rischio di una responsabilità amministrativa in capo alla Società;

xii) segnalare all'Organo Amministrativo fatti o condotte di rilevanza disciplinare;

xiii) proporre l'adozione di eventuali sanzioni o provvedimenti disciplinari (fermo restando la competenza della Società per la conduzione del procedimento disciplinare e l'irrogazione della eventuale sanzione);

xiv) promuovere e/o sviluppare, di concerto con le funzioni aziendali preposte, programmi di formazione, informazione e comunicazione interna, con riferimento al Modello 231, al Codice Etico e di Comportamento e alle procedure aziendali.

xv) promuovere e/o sviluppare l'organizzazione, di concerto con le funzioni aziendali preposte, di corsi di formazione o la predisposizione di materiale informativo utile alla comunicazione e divulgazione dei principi etici e degli standard cui la Società si ispira nello svolgimento delle proprie attività;

xvi) formulare proposte all'Organo Amministrativo di eventuali aggiornamenti o adeguamenti del Modello 231 in conseguenza di significative violazioni delle sue prescrizioni, o modificazioni dell'assetto interno della società, o mutamento delle modalità di svolgimento dell'attività d'impresa, o modifiche normative.

2. Per l'esecuzione delle sue attività, l'Organismo di Vigilanza può avvalersi anche delle prestazioni di consulenti esterni (a questo fine dispone di un proprio budget messogli a disposizione dall'Azienda e gestito in totale autonomia dall'OdV), rimanendo sempre direttamente responsabile dell'esatto adempimento degli obblighi di vigilanza e controllo ex D.Lgs. n. 231/2001.

3. Agli eventuali consulenti di cui al precedente comma è richiesto il rispetto degli obblighi di diligenza previsti per i componenti dell'Organismo di Vigilanza.

Articolo 9 - Poteri

1. L'Organismo di vigilanza deve essere dotato di tutti i poteri necessari per assicurare una puntuale ed efficace vigilanza su funzionamento e osservanza del Modello 231, secondo quanto stabilito dall'art. 6 del decreto 231.

2. Per esercitare efficacemente le proprie funzioni, l'Organismo di Vigilanza:

a) deve avere libero accesso presso tutte le funzioni della società - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D.Lgs. 231/01;

b) ha la facoltà di avvalersi del supporto e della collaborazione delle funzioni interne, alle quali potrà essere chiesto di attivarsi per svolgere compiti strettamente collegati e funzionali alle attività di controllo;

c) può avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di consulenti esterni. Ha, pertanto, la facoltà di chiedere e/o assegnare a soggetti terzi, in possesso delle competenze specifiche necessarie, incarichi di consulenza e/o di assistenza al fine di poter svolgere le attività di propria competenza. A tal fine e nel contesto delle procedure di formazione del budget aziendale, l'Organo Amministrativo deve obbligatoriamente approvare una dotazione di risorse finanziarie per l'OdV (budget), della quale lo stesso potrà disporre in totale autonomia per ogni esigenza necessaria al corretto svolgimento dei suoi compiti;

3. L'OdV dovrà essere costantemente informato dal management societario sugli aspetti dell'attività aziendale che possono esporre la Società al rischio di commissione di uno dei reati presupposti dal D.Lgs. 231/2001.

4. Al fine di consentire il corretto svolgimento dell'attività dell'OdV, la Società e i suoi dipendenti/responsabili dovranno rispettare gli obblighi, i criteri ed i tempi, dettati in materia di flussi Informativi.

Articolo 10 - Flussi informativi

1. I flussi informativi provenienti dall'Organismo di Vigilanza nei confronti dell'Organo Amministrativo sono: a) di natura continuativa, in occasione delle sessioni OdV e dell'invio dei relativi verbali nonché in occasione dell'invio della relazione annuale, riassuntiva dell'attività svolta e delle valutazioni riportate in ordine alle eventuali criticità, ai comportamenti ed eventi societari a rischio di reato, alla maggiore o minore efficacia del MOGC; b) di natura occasionale, al fine di segnalare eventuali violazioni del Modello 231 o del Codice Etico e di Comportamento emerse durante lo svolgimento delle verifiche, nonché al fine di avanzare proposte di incontri/riunioni con una o più funzioni societarie per l'eventuale analisi di situazioni, problemi o livelli di criticità ex D.Lgs. 231/2001.
2. I flussi informativi provenienti dalla Società nei confronti dell'Organismo di Vigilanza costituiscono un'asse portante del sistema di controllo societario, una componente essenziale del Modello 231 e dell'attività di monitoraggio dello stesso OdV, un obbligo legislativamente stabilito dall'art. 6 del D.Lgs. 231/2001, in base al quale il Modello 231 deve «prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli».
3. L'Organismo di Vigilanza deve essere messo in grado di svolgere la sua corretta attività di controllo e di ausilio preventivo anti-illiceità societarie attraverso un adeguato sistema strutturato di flussi informativi proveniente da tutte le funzioni aziendali.
4. I flussi informativi nei confronti dell'Organismo di Vigilanza dovranno essere: chiari ed inequivoci nella loro rappresentazione; idonei a rappresentare compiutamente l'evento riportato; attendibili, completi e genuini, nel senso che il dato riportato dovrà essere completo e aderente a quello originale; aggiornati, nel senso che le informazioni dovranno essere il più possibile attuali rispetto al periodo di osservazione; obbligatori e tali da poterne derivare responsabilità di natura disciplinare in caso di inottemperanza, parziale o totale.
5. I flussi informativi nei confronti dell'OdV si distinguono in flussi periodici e flussi ad hoc:

a) I flussi informatici periodici, o di cd. reporting periodico, sono quelli provenienti da: Organo Amministrativo; Responsabili di Unità Operative (su attività ordinaria e straordinaria, a cadenza periodico-ordinaria eventualmente da concordare tra OdV e Organo Amministrativo); Organi di Controllo interno, su specifica e motivata richiesta dell'OdV.

b) I flussi informativi straordinari e/o ad hoc sono quelli provenienti da tutti gli organi sociali, funzioni, responsabili/dipendenti, riguardanti: gli accessi delle Autorità Istituzionali; le ispezioni o le perquisizioni o i sequestri da parte delle succitate Autorità Istituzionali; le Richieste di Rinvio a Giudizio o i Decreti di Citazione a Giudizio da parte dell'Autorità Giudiziaria Penale; gli atti di citazione in giudizio civile di particolare rilevanza sociale; le eventuali denunce/segnalazioni, anonime o non; le convocazioni da parte delle Autorità Istituzionali; le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate, ovvero i provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora gli stessi siano legati alla commissione di reati o di violazione delle regole di comportamento o

procedurali del MOGC; gli eventi a carattere straordinario e/o eccezionale (soprattutto in materia ambientale o di sicurezza sui luoghi di lavoro); tutte le situazioni fattuali a carattere straordinario o eccezionale.

c) Ulteriore flusso informativo ad hoc nei confronti dell'Organismo di Vigilanza è quello riguardante le eventuali segnalazioni di reato o di condotte illecite ex D.Lgs. 231/2001, o di comportamenti in violazione del Codice Etico, o di ritorsioni da whistleblowing, eventualmente inviate anche in forma anonima.

6. In presenza di alcuna delle segnalazioni di cui al punto 5.c (whistleblowing), l'OdV dovrà valutarle con discrezionalità e responsabilità, attivando tutti gli approfondimenti ritenuti necessari, effettuando le dovute indagini e adoperandosi affinché venga definito quanto previsto dal sistema sanzionatorio aziendale, ma, soprattutto, dovrà garantire che le informazioni acquisite saranno trattate in modo da garantire: a) la riservatezza e l'anonimato del segnalante; b) la tutela del segnalante da qualsiasi forma di ritorsione, penalizzazione, discriminazione (fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede); c) il rispetto di una specifica e strutturata procedura di trasmissione da parte del Responsabile dell'area Informatica.

7. L'Organismo di Vigilanza ha diritto di stabilire, di concerto con l'Organo Amministrativo, la tempistica e le modalità di trasmissione dei flussi informativi, da comunicare alle relative aree operative o funzioni societarie alla stregua di disposizione di servizio dal carattere di inderogabilità.

8. L'Organismo di Vigilanza ha diritto di chiedere e di ottenere altri e diversi flussi informativi specifici (a carattere periodico od occasionale) in presenza di ritenute emergenze di rischio o particolari criticità sociali oltre a quelli riportati nella tabella della pagina seguente.

La tabella dei *Flussi Informativi* sarà definita all'esito della conclusione e definizione dell'Organigramma Aziendale (in via di assestamento).

4. I DESTINATARI DEL MODELLO 231

Per tracciare con precisione l'area di operatività del Modello, è innanzitutto necessario individuarne i "d*estinatari",* chiarendone per ogni tipologia o categoria di riferimento la specifica potenzialità di soggezione allo stesso Modello.

In via assolutamente generale e propedeutica, possono definirsi Destinatari del Modello 231 tutti coloro che, operando *con* o *per* la Società, si trovino nella teorica condizione di commettere alcuno dei reati previsti dal D.Lgs. 231/2001; da qui il loro obbligo di conoscere e rispettare, con il massimo della diligenza e del rigore, il MOGC adottato dalla Società al fine di prevenire le specifiche condotte illecite indicate dal Legislatore.

Al di là di questa sintetica affermazione di base, va rilevato che l'individuazione dei precisi confini di responsabilità ipoteticamente attribuibili, da un lato al destinatario per fatti e reati commessi nell'esercizio di funzioni e mansioni esercitati in favore della Società, dall'altro alla Società per fatti e condotte illeciti commessi dai Destinatari nel suo interesse, presuppone un'attenta e complessa analisi delle effettive relazioni di lavoro intercorrenti tra le due entità di raffronto.

Ciò al fine di chiarire con certezza il preciso limite e discrimine - in termini di bilateralità reciproca - tra l'eventuale operato illecito dei soggetti che operano (a vario titolo o diverso periodo temporale) con la Società, e l'eventuale responsabilità della Società per i fatti illeciti eventualmente commessi da questi soggetti.

Partendo da quello che potremmo definire il corredo personale "globale" di *ADR Trasporti S.R.L.*, a prescindere cioè dalle specifiche peculiarità delle singole categorie, possiamo senz'altro inserire tra i destinatari del Modello 231 della Società i seguenti soggetti:

- L'Organo Amministrativo;
- i dirigenti ed il personale apicale in genere;
- i collaboratori, anche esterni ed a titolo occasionale (nei limiti delle funzioni svolte nell'interesse della Società);
- i dipendenti e gli operai, anche a titolo occasionale;
- i consulenti e/o i professionisti chiamati a svolgere uno o più incarichi (nei limiti delle funzioni svolte nell'interesse della Società);
- i fornitori e gli outsourcers (nei limiti delle prestazioni rese nell'interesse della Società);
- i subappaltatori e i sub fornitori (nei limiti delle prestazioni rese in regime di subappalto e subfornitura);
- le persone giuridiche che eventualmente intrattengano con la Società rapporti di lavoro in termini di collaborazione, Associazione Temporanea di Imprese, joint venture, partnership, qualunque forma di cooperazione o di co-ausilio Societario (nei limiti dei rapporti intrattenuti nell'interesse della Società).

Una annotazione di particolare importanza è che rientrano nella categoria dei Destinatari, sempre nei limiti delle funzioni svolte nell'interesse della società:

- gli appartenenti alle strutture o enti che si occupano dei controlli sulla Società;
- l'Organismo di Vigilanza ex D.lsg. 231/2001.

Giova al riguardo chiarire che i succitati organi, proprio perché espressamente chiamati dal Legislatore a svolgere una funzione di controllo superiore, potrebbero – e la casistica giudiziaria dei nostri giorni dimostra ampiamente il frequente ruolo attivo svolto dagli stessi soggetti nelle "corruzioni" o nelle operazioni illecito di "alto bordo" - contribuire a consumare, o ad occultare, illeciti di qualunque natura ed entità nell'interesse della Società[21].

Escluderli dalla categoria dei "destinatari" significherebbe introdurre nel sistema una forma di impunità priva di valida giustificazione logica e comunque nettamente anticostituzionale.

Avuto specifico riferimento ad alcuna delle succitate categorie, si reputa necessaria qualche puntualizzazione.

Per ciò che riguarda gli **amministratori, i dirigenti e il personale apicale**, l'art. 5 del D.Lgs. 231/2001, al primo comma lett. a), è chiaro nello statuire: *"L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa*

[21] V., in materia, l'interessante ricostruzione effettuata nella Circolare n. 83607/2012, emanata dal Comando Generale della Guardia di Finanza, III Reparto Operazioni, Ufficio Tutela Economia e Sicurezza.

dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso".

In definitiva, le persone che rivestono le funzioni di rappresentanza, di amministrazione, di direzione dell'ente o di una sua unità organizzativa, sono certamente responsabili in prima persona dei reati commessi nell'interesse o a vantaggio della Società (si parla, in questi casi, di "amministratori infedeli"), tanto quanto lo è la Società, per gli stessi eventuali reati, in via amministrativa e sul piano squisitamente aziendale (cioè ai fini dell'applicabilità a suo carico delle sanzioni e misure interdittive previste dal D.Lgs. 231/2001).

Altrettanto pacifico è il concetto di amministratore o di dirigente "*di fatto*" – ossia di colui che, pur non rivestendo alcuna carica o potere direzionale sul piano formale, lo eserciti in via concreta e fattuale - pienamente equiparato all'amministratore o dirigente di diritto.

I **soci** della Società, sono da considerare a tutti gli effetti Destinatari del MOGC 231.

I **dipendenti** rientrano a tutti gli effetti nel paradigma normativo dell'art. 5, co.1, lett. b) del D.Lgs. 231/2001, quali "*persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)*, ossia amministratori, dirigenti e personale apicale.

Ne deriva il loro inserimento di diritto nella categoria dei Destinatari, quali soggetti in grado di commettere reati in favore o nell'interesse della Società, nonché persone per le quali quest'ultima rimane esposta al rischio di rispondere - a titolo di "responsabilità amministrativa" - del loro eventuale operato illecito.

Da notare che, proprio nel caso dei dipendenti, la Società è soggetta ad un duplice livello di responsabilità:

a) *"amministrativa*", all'interno di un processo penale ed ai sensi del D.Lgs. 231/2001, con le note sanzioni pecuniarie e misure interdittive;

b) "*civile*", sia nell'ambito di un giudizio civile *ex* art. 2049 c.c. ("*responsabilità dei padroni e committenti"*), sia in sede di processo penale *ex* art. 83 c.p.p., quale "responsabile civile" per il fatto dell'imputato.

Entrambe le due succitate forme di responsabilità, univocamente a carico della Società, sono idonee a concorrere giuridicamente con la responsabilità strettamente personale del singolo dipendente.

Emblematico, al riguardo, il caso in cui il dipendente sia chiamato a rispondere quale responsabile di un reato colposo in materia di infortuni sul lavoro.

L'eventuale condotta illecita del dipendente comporterà a catena: la violazione dei "reati presupposti" dall'art. 25 septies del D.Lgs. 231/2001; il processo penale a suo carico per i predetti "reati presupposti"; la chiamata in causa della Società, sempre nell'ambito dello stesso processo penale, quale *padrone e committente* e dunque "responsabile civile" per il fatto del dipendente-imputato (si ricordi, peraltro, che in questi casi la responsabilità civile è di tipo oggettivo e prescinde dall'accertamento della colpa del "committente"); la chiamata della Società, ancora una volta nello stesso processo penale in cui è già presente come "responsabile civile", per l'eventuale ed ulteriore responsabilità amministrativa ai sensi del D.Lgs. 231/2001.

Tra i criteri esegetici utilizzati per meglio comprendere gli esatti confini di una eventuale duplice responsabilità "da" D.Lgs. 231/2001 – quella penale e personale dei dipendenti e

collaboratori in relazione ad un reato commesso nell'interesse della Società; quella amministrativa ed aziendale della Società, per lo stesso reato commesso nel suo interesse dai predetti soggetti – il più importante è certamente quello della "*immedesimazione organica*".

In base a questo principio e parametro giuridico, *ADR Trasporti S.R.L.* potrà essere considerata responsabile (a titolo "amministrativo" ed ai sensi del D.Lgs. 231/2001) dell'operato dei suoi dipendenti e collaboratori unicamente se, e nella misura in cui, la condotta illecita posta in essere dagli stessi soggetti sia immediatamente e direttamente *"riferibile alla Società*".

In conclusione, la Società potrà essere considerata "amministrativamente responsabile" degli eventuali reati posti in essere dai suoi collaboratori e dipendenti solo se gli stessi reati:

- siano stati commessi nell'esercizio delle specifiche funzioni assegnate dalla Società;
- siano direttamente imputabili alla Società quale espressione del principio di immedesimazione organica;
- non siano frutto di elusione fraudolenta del Modello di Organizzazione, Gestione e Controllo.

Per ciò che concerne **i fornitori e gli outsourcers** - non importa se persone fisiche o giuridiche (evenienza che potrebbe solo presupporrebbe una maggiore autonomia ed organizzazione di mezzi e di persone) – *ADR Trasporti S.R.L.* li considera *parzialmente* Destinatari del Modello di Organizzazione, Gestione e Controllo adottato. Sebbene i fornitori non esercitino in via diretta l'attività di *ADR Trasporti S.R.L.,* gli stessi possono certamente considerarsi "*sottoposti alla direzione o alla vigilanza*" di amministratori e di personale apicale della Società laddove siano chiamati a prestare una determinata attività accessoria e di ausilio, e ciò seguendo le specifiche direttive, domande e standard richiesti dalla committente. Si pensi, al riguardo, all'attività dei fornitori o tecnici chiamati a fornire e a gestire sistemi hardware e software (materia cui sono correlati molteplici reati informatici), o mezzi, materiale e strumenti di complemento per la gestione di una commessa avente ad oggetto un appalto di beni o di servizi.

Sono tutte situazioni in cui *ADR Trasporti S.R.L.* ha pieno diritto di chiedere che siano rispettate le proprie regole di natura etica e morale (interamente riportate nel Codice Etico), nonché i protocolli e gli standard di legalità specificamente indicati nel proprio Modello di Organizzazione, Gestione e Controllo.

É solo al di là di questo specifico ambito di lavoro condotto insieme che il fornitore sarà libero di muoversi liberamente in base ai propri ed autonomi assetti regolamentari, senza dovere soggiacere a nessuno Modello di Organizzazione, Gestione e Controllo che non sia quello della sua personale struttura societaria.

Tra le categorie dei destinatari di maggiore importanza, riveste senz'altro un posto di primo piano quella dei **subappaltatori, o sub vettori,** tanto più che si tratta di persone fisiche e giuridiche cui la Società affida parte delle proprie commesse.

La delicatezza dei rapporti con tali soggetti (nei cui confronti appare, dunque, opportuno muoversi in regime di *"cautela avanzata")* risiede nel fatto che - ad oggi - la valutazione giurisprudenziale in ordine alle eventuali responsabilità di natura

civile/penale/amministrativa, derivanti da una possibile non corretta esecuzione o svolgimento dei servizi appaltati, o da un infausto danno di natura extracontrattuale, è tutt'altro che unanime, pacifica e consolidata.

Una premessa di assoluta centralità è che la tematica sulle predette, specifiche, responsabilità di natura extracontrattuale opera su un piano completamente diverso rispetto a quella della eventuale *corresponsabilità solidale* di natura fiscale o contributiva-previdenziale in capo all'appaltatore.

Quest'ultimo tipo di responsabilità è regolata dall' art. 29 del D.Lgs. 276/2003 (delegato dalla Legge 30/2003), che ha introdotto un regime di responsabilità solidale dell'appaltatore verso il subappaltatore in ordine alle ritenute fiscali sui redditi di lavoro dipendente e che, a sua volta, è stato modificato dall'attuale D.Lgs. 175/2014.

Tale specifica forma di responsabilità *non* riguarda però - in alcun modo - il tema del diverso tipo di responsabilità per eventuali fatti illeciti addebitabili al subappaltatore, e quindi della eventuale posizione di correponsabilità in capo all'appaltatore.

Qui valgono regole tendenzialmente antitetiche, atteso che il regime civilistico del contratto di appalto (e quindi di subappalto) di cui agli artt. 1655-1677 c.c. si basa sul fermo principio secondo il quale l'appalto presupppone: a) l'affidamento in autonomia di una determinata opera/servizio; b) la prestazione del servizio o dell'esecuzione dell'opera subappaltati attraverso una propria organizzazione di mezzi e di risorse; c) il divieto di intromissione gestoria da parte dell'appaltatore.

Ciò comporta un duplice tipo di problema/conseguenza:

a) la necessità di individuare (e dunque prevenire ed evitare) le situazioni in cui le responsabilità del subappaltatore potrebbero estendersi anche all'appaltatore;

b) l'esigenza di predisporre un sistema organizzativo che, da un lato possa ridurre questo specifico rischio, dall'altro eviti però di produrre l'effetto opposto, e cioè di scaricare sull'appaltatore l'eventuale responsabilità del subappaltatore proprio in ragione di una asserita *"intromissione gestoria"*, v. quella che ad avviso della giurisprudenza finisce per snaturare lo stesso contratto di "subappalto", rendendo il subappaltatore una sorta di "*nudus minister*" e facendo ricadere tutte le responsabilità sull'appaltatore anziché sul subappaltatore (v. tra le tante Cass. Civ., Sez. III, 10 aprile 2014 n.8410).

Corollario dell'una o dell'altra evenienza è l'eventuale affermazione, o negazione, di una possibile, o meno, responsabilità solidale dell'appaltatore *ex* art. 2049 cc. (v. *la responsabilità dei padroni e committenti*, che peraltro è a carattere rigorosamente oggettivo).

In materia - a parte il divieto di "intromissione gestoria", in ordine al quale la giurisprudenza è assolutamente unanime nel confermare l'inderogabilità del principio di natura codicistica - il quadro giurisprudenziale di riferimento è assolutamente equivoco e non conforme.

Più da vicino, in parecchie sentenze viene affermato che: *«l'autonomia dell'appaltatore o sub-appaltatore, il quale esplica la sua attività nell'esecuzione dell'opera assunta con propria organizzazione ed apprestandone i mezzi, nonchè curandone le modalità ed obbligandosi verso il committente o subappaltante a prestargli il risultato della sua opera, esclude ogni rapporto istitutorio tra committente ed appaltatore, con la conseguenza dell'inapplicabilità dell'art. 2049 c.c.»* (Cass. Pen., Sez. 4, 14 gennaio 2010, n. 1479).

Nella stessa sentenza n. 1479 ora citata viene però affermato anche: «*l'appaltatore* (n.d.s. il subappaltatore, ai fini della nostra disamina) *deve, quindi, di regola ritenersi unico responsabile dei danni derivanti a terzi dall'esecuzione dell'opera, salva la corresponsabilità del committente* (n.d.s. dell'appaltatore, ai fini della nostra disamina) *in caso di specifiche violazioni di regole di cautela nascenti ex art. 2043 c.c.*» (Cass. Civ. 10 aprile 2014 n. 8410; Id., Sez. 3, 29 ottobre 2015, n. 286; Id., Sez. 3, 15 ottobre 2013, n. 25758; Cons. St., sez. VI, 28 ottobre 2010, n. 7635)

Per completezza, l'art. 2043 c.c. è quella di norma di salvaguardia generale che stabilisce: «*Qualunque fatto doloso o colposo che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno».*

Sempre al fine di toccare con mano l'eterogeneità di opinioni sul punto, altra importante sentenza sostiene (a specifico proposito della responsabilità per violazione della sicurezza sui luoghi di lavoro ma attraverso una proclamazione di principio assolutamente generica e generale): «è *vero che nel caso di contratto di appalto non può essere posta in dubbio la posizione di garanzia del committente* (n.d.s. dell'appaltatore nel caso di subappalto) *il quale ha l'obbligo di accertare la "idoneità tecnico professionale" dell'impresa appaltatrice, quello di fornire alla stessa dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui questa è destinata ad operare (sono i rischi derivanti dalla peculiarità dell'ambiente di lavoro, che solo il titolare può conoscere appieno) e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività, nonchè l'ulteriore obbligo di promuovere la "cooperazione" ed il "coordinamento" ai fini dell'attuazione delle misure precauzionali .... La violazione dei suindicati obblighi comportamentali può fondare una (cor)responsabilità (anche) del datore di lavoro/committente per infortuni che abbiano riguardato i lavoratori dipendenti dell'appaltatore ... Deve, pertanto, affermarsi il principio di diritto secondo il quale il committente* (n.d.s. l'appaltatore in caso di subappalto) *qualora l'evento si colleghi casualmente anche alla sua colposa omissione ed in quei casi in cui l'omessa adozione delle misure di prevenzione prescritte sia immediatamente percepibile cosicchè il committente medesimo sia in grado di accorgersi dell'inadeguatezza delle stesse senza particolari indagini ... Ne consegue che, ai fini della configurazione della responsabilità del committente, occorre verificare in concreto quale sia stata l'incidenza della sua condotta nell'eziologia dell'evento ... nonchè alla agevole ed immediata percepibilità da parte del committente di situazioni di pericolo*» (Cass. Pen., Sez. 4 18 dicembre 2014, n. 52658; conf. Cass. Sez. 4, 18 gennaio 2012, n. 3563; Id. Sez. 4, 15 dicembre 2005, n. 5977,Cimenti; Id. Sez. 3, 24 ottobre 2013, n. 50996).

Si consideri a quest'ultimo riguardo che, anche ad avviso di Corte di Cassazione, sez. VI Penale - sentenza n. 17049/11, incombe sul committente (n.d.s. sull'appaltatore in caso di subappalto) «*un dovere di controllo di origine non contrattuale al fine di evitare che dall'opera derivino lesioni del principio del "neminem ledere", idonee, queste si, ad eventualmente corresponsabilizzare il committente*(n.d.s. l'appaltatore in caso di subappalto) *in base al precetto di cui all'art. 2043 c.c.*».

Secondo questa logica, viene ad esempio considerato punibile – in materia di delega di funzioni ma il principio è assolutamente valevole ai nostri fini – il caso in cui non vi sia stata una incolpevole estraneità alle inadempienze del delegato, o vi sia stata una informazione (anche ufficiosa) di condotte censurabili, così da potersi ipotizzare un atteggiamento di inerzia

o di colpevole tolleranza in capo ai titolari delle posizioni di garanzie (Cass. pen. III, 27 giugno 2002, n. 32151; Id., III, 5 novembre 2002, n. 246).

Di avviso nettamente contrario è Cass. pen., III sez. pen, sentenza n. 11029/2015, secondo la quale, a proposito della gestione dei rifiuti: a) *«tranne nel caso di un diretto concorso nella commissione del reato, non può ravvisarsi alcuna responsabilità ai sensi dell'articolo 40, comma 2 cod. pen. per mancato intervento al fine di impedire violazioni della normativa in materia di rifiuti da parte della ditta appaltatrice* (n.d.s. subappaltatrice ai nostri fini)»; b) «*l'appaltatore* (n.d.s. il subappaltatore ai nostri fini), *in ragione della natura del rapporto contrattuale, che lo vincola al compimento di un opera o alla prestazione di un servizio con organizzazione dei mezzi necessari e con gestione a proprio rischio è, di regola, il produttore del rifiuto; su di lui gravano, quindi, i relativi oneri*».

A loro volta, di avviso esattamente antitetico a quest'ultima affermazione giurisprudenziale: Cass. 4957/2000, Cass. 24347/2003, Cass. 36963/2005, secondo le quali *«è produttore dei rifiuti colui nel cui interesse viene svolta l'attività da cui traggono origine i rifiuti*» (v. il committente o l'appaltatore nei confronti del subappaltatore).

Sulla scorta di quanto sin qui delineato è certamente opportuno che *ADR Trasporti S.R.L.*:

a) "personalizzi" il contratto con il subappaltatore o con il sub vettore integrandolo di prescrizioni e presupposti di legalità in linea con il presente Modello di Organizzione, Gestione e Controllo, nonché con eventuali ed ulteriori protocolli di legalità;

b) affidi ad un suo dipendente/funzionario una specifica *delega di funzione* avente ad oggetto:

- la valutazione preventiva dei rischi in fase esecutiva (v. soprattutto in presenza di commesse subappaltate dalla prevedibile rischiosità ambientale);
- il controllo sullo svolgimento dei lavori, ma nei limiti del richiamato art. 1622 c.c.;

c) riconsideri/ritocchi le sue procedure di controllo in materia di subappalto, cercando di trovare un giusto punto di equilibrio tra il divieto di intromissione gestoria (che, come prima detto, potrebbe far diventare il subappaltatore un semplice *nudus minister* dell'appaltatore, liberandolo in tal modo dalle sue specifiche e dirette responsabilità) e l'esigenza di un controllo ab externo in grado di abbassare il livello di rischio, soprattutto in fase esecutiva.

5. APPROVAZIONE E AGGIORNAMENTO DEL MODELLO 231

L'adozione e l'efficace attuazione del Modello costituiscono - ai sensi dell'art. 6, comma I, lett. a) del D.Lgs. 231/2001 - atti di competenza e di emanazione dell'Organo Amministrativo.

Viene, in particolare, rimesso all'Organo Amministrativo il potere di approvare e recepire, mediante apposita delibera, sia il *Modello di Organizzazione, Gestione e Controllo*, sia il *Codice Etico e di Comportamento.*

Una volta approvati, rappresentano obbligatoria attività di manutenzione, del Modello di Organizzazione, Gestione e Controllo e del Codice Etico, le attività di:

- *Verifica*;
- *Aggiornamento.*

In particolare il MOGC - anche su impulso e coordinamento dell'Organismo di Vigilanza - dovrà essere soggetto a due tipi di verifiche:

- *verifiche sull'osservanza del Modello*, e sulle principali attività poste in essere nelle aree di attività cd. "sensibili";
- *verifiche sul funzionamento del Modello,* sulla sua validità ed efficacia o sulle eventuali correzioni da effettuare sulla base: delle indicazioni dell'Organismo di Vigilanza; delle segnalazioni ricevute nel corso dell'anno da parte dell'Organismo di Vigilanza; delle proposte da parte di tutti i soggetti che operano "con" o "per" *ADR Trasporti S.R.L.*.

Il MOGC e il Codice Etico e di Comportamento dovranno essere – obbligatoriamente e costantemente - aggiornati.

L'aggiornamento del MOGC è obbligatorio soprattutto in corrispondenza di:

- mutamenti di natura aziendale;
- innovazioni di natura normativa;
- evidenziazione di punti di criticità del Modello;
- indicazioni e suggerimenti dell'Organismo di Vigilanza.