MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

ex D.Lgs. 231/2001
esteso alla normativa anticorruzione

Gennaio 2025

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 avviato su scala internazionale a partire dagli anni '90.

Tra le ideali fonti di questo importante percorso si inseriscono:

- la Convenzione OCSE «*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), 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, adottate dal Comitato dei Ministri del Consiglio d'Europa il 6 novembre 1997.

Anche in Italia, la Legge Delega n. 300/2000[1] - da cui scaturisce il Decreto Legislativo 231/2001 – nasce dalla necessità di controllare, prevendere, monitorare e auspicabilmente diminuire/azzerare il sempre più crescente rischio legato alle disfuznioni delle strutture societarie, anche e soprattutto a carattere privatistico.

Il Decreto Legislativo 8 giugno 2001 n. 231 (*Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*, dunque, introduce, per la prima volta in Italia, 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

[1] 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».*

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*.

Tale *responsabilità indiretta* è azionabile, ex 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.

Sul piano squisitamente sostanziale e processuale, 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'architettura normativa all'impianto normativo 231 è piuttosto complessa in quanto, unitamente all'introduzione di uno specifico sistema punitivo per gli enti, viene prevista una serie di apposite regole di prevenzione delittuosa, eminentemente basate sullo strumento dell'organizzazione a carattere preventivo.

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).

Di assoluta centralità il principio secondo cui: ove si sia provveduto a strutturare un idoneo (v. in base ai canoni ed elementi essenziali previsti per legge) Modello di Organizzazione, Gestione e Controllo, l'ente «*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 un doppio e convergente livello di responsabilità, sia a carico della persona fisica che ha commesso il reato che dell'ente "in" o "con" cui la persona fisica opera, 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 – vengono 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[2].

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);
- 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.

Attraverso tale dimostrazione, l'ente potrà "difendersi" ed affermare 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[3].

---

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

[3] 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*

1.2. Il sistema anticorruzione spontaneamente integrante un MOGC 231

La legislazione general-preventiva varata per gli *enti privati* con il D.Lgs. 231/2001 è sbarcata nel sistema delle *pubbliche amministrazioni* nell'anno 2012, con la Legge 6 novembre 2012 n. 190 (*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione*).

Anche questa legge, come il D.Lgs. 231/2001, è "figlia" della richiesta, da parte della Comunità Internazionale, di predisporre una normativa statuale a carattere general-preventivo.

L'intervento strutturale operato dalla Legge 190/2012 – in parte come regolazione legislativa diretta, in parte come legislazione di delega – è stato particolarmente vasto e si è mosso razionalmente su diversi piani, tra cui (a titolo meramente esemplificativo e non esaustivo), quelli aventi ad oggetto:

I. La nuova distribuzione di organi, soggetti, funzioni e poteri (centrali e decentrati), per l'approntamento di misure preventive "anti illiceità" nell'ambito delle pubbliche amministrazioni;

II. L'introduzione di strategie e azioni preventive a carattere centrale e decentrato;

III. La definizione di nuove norme ed istituti giuridici finalizzati alla regolazione ed al monitoraggio, diretto ed indiretto, dell'azione amministrativa;

IV. L'aggiornamento di strumenti di regolazione etica e comportamentale;

V. L'irrigidimento della repressione.

Il quadro programmatico della Riforma Anticorruzione è stato basato su tre livelli di intervento:

- ❒ *Piano Legislativo;*
- ❒ *Piano della Programmazione Organizzativa;*
- ❒ *Piano della Strategia Preventiva.*

Per ciò che concerne il *Piano delle Riforme Legislative,* la Legge 6.11.2012 n. 190 (*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione*): in parte, ha disciplinato direttamente e per intero il sistema di prevenzione e repressione della "corruzione ed illegalità nella Pubblica Amministrazione"; in parte, si è mossa alla stregua di Legislatore Delegante, ossia rimandando la disciplina attuativa di determinati settori ad altri e successivi provvedimenti legislativi.

I provvedimenti legislativi delegati dalla Legge 190/2012 sono stati:

- il D.Lgs. 235/2012 in materia di *incandidabilità* (di rilievo accessorio ai fini dei Modelli 231 e dei Piani Anticorruzione avendo prevalentemente ad oggetto situazioni legati alla incandidabilità di natura politica);
- il D.Lgs. 14 marzo 2013 n. 33 (*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*), poi modificato e aggiornato dal D.Lgs. 25 maggio 2016 n. 97 (*Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del Decreto Legislativo 14 marzo 2013, n. 33);*
- il D.P.R. 16 aprile 2013 n. 62 (*Regolamento recante Codice di Comportamento dei dipendenti pubblici, a norma dell'articolo 54 del Decreto Legislativo 30 marzo 2001, n. 165);*

---

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»

- il D.Lgs. 18 aprile 2013 n. 39 (*Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico,*
- il Decreto del Presidente del Consiglio dei Ministri del 18 aprile 2013 (istitutivo del sistema delle *white list* in materia di appalti e forniture), successivamente modificato e aggiornato dal Decreto del Presidente del Consiglio dei Ministri 24 novembre 2016

Nel corso degli anni a seguire, il corredo dei provvedimenti "anticorruzione" delegati dalla Legge 190/2012 è stato parzialmente modificato ed aggiornato – soprattutto nella strutturazione delle funzioni e dei poteri a livello istituzionale - ad opera del D.L. 24.6.2014 n. 90, convertito in Legge 11.8.2014 n. 114 (*Misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari).*

Attraverso tale provvedimento legislativo è stata effettuata la redistribuzione dei poteri e delle funzioni anticorruzione a livello centrale, nei seguenti termini:

❒ Nella Legge 190/2012, l'assetto anticorruzione era stato costruito come un sistema dualistico ripartito tra due Organismi Centrali: il Dipartimento della Funzione Pubblica; l'Autorità Nazionale Anticorruzione.

❒ A seguito della ristrutturazione operata dall'art. 19 del D.L. 90/2014, l'Autorità Nazionale Anticorruzione è rimasta vertice assoluto di tutta la "macchina anticorruzione".

Con lo stesso D.L. 90/2014, all'Autorità Nazionale Anticorruzione è stata espressamente devoluta anche la *materia degli appalti,* già devoluta all'A.V.C.P. (organo soppresso dallo stesso Decreto Legge a seguito dei noti scandali MOSE ed EXPO).

La *macro programmazione centrale e decentrata* prevista dalla Legge 190/2012 si fonda sulle seguenti linee portanti:

A) Redazione e pubblicazione di un *Piano Nazionale Anticorruzione* (per brevità PNA), a durata triennale e a cadenza annuale, quale Atto di Indirizzo (*rectius* Atto di Alta Amministrazione) di livello centrale e parametro di riferimento di tutte le pubbliche amministrazioni italiane, con il quale vengono stabiliti principi direttivi e linee guida dell'azione preventiva anti-illiceità da adottare a livello decentrato.

B) Redazione e relativo invio all'Autorità Nazionale Anticorruzione dei *Piani Triennali della Prevenzione della Corruzione e della Trasparenza* (per brevità PTPCT), quali atti emessi dalle singole pubbliche amministrazioni centrali e decentrate, parimenti a durata triennale e a cadenza annuale, con i quali ogni pubblica amministrazione decentrata prevede ed implementa, nell'ambito della propria struttura, specifiche azioni di gestione del rischio-illiceità, anche sulla base delle direttive del PNA e dell'ANAC.

C) Inserimento nei predetti Piani (in coordinamento con il Sistema preventivo della corruzione) del *sistema trasparenza,* con il quale viene illustrato il piano obbligatorio relativo alla pubblicazione dei dati ed informazioni delle singole pubbliche amministrazioni.

C) Accorpamento, nel Piano Triennale della Prevenzione della Corruzione, del *Piano della Performance* (a cadenza annuale) già previsto dal D.Lgs. 27 ottobre 2009 n. 159 (cd. Riforma Brunetta). Nel caso degli enti privati in controllo pubblico, tale Piano si riduce alla rappresentazione delle premialità distribuite ai dipendenti.

Avuto infine riguardo alla *micro strategia preventiva decentrata*, i Piani Triennali della Prevenzione della Corruzione e della Trasparenza adottati da ogni singola pubblica amministrazione dovranno:

► *Gestire razionalmente il rischio* di corruzione ed illegalità in relazione alle peculiarità della propria, specifica, struttura amministrativa;

► *Supportare la gestione del rischio attraverso l'applicazione delle inderogabili misure preventive* - esattamente n. 13 - indicate nel Piano Nazionale Anticorruzione

Le predette 13 misure preventive anticorruzione sono:

- ✓ *Trasparenza*;
- ✓ *Codice di Comportamento*;
- ✓ *Rotazione del Personale*;
- ✓ *Obbligo di astensione in caso di conflitto di interesse*;
- ✓ *Svolgimento di incarichi d'ufficio – attività ed incarichi extra-istituzionali*;
- ✓ *Conferimento di incarichi dirigenziali*;
- ✓ *Incompatibilità specifica per posizioni dirigenziali*;
- ✓ *Attività successiva alla cessazione del rapporto di lavoro*;
- ✓ *Formazione di commissioni, assegnazione agli uffici e conferimento di incarichi in caso di condanna per i delitti contro la pubblica amministrazione*;
- ✓ *Tutela del dipendente che effettua segnalazioni di illecito (c.d. whistleblower)*;
- ✓ *Formazione*;
- ✓ *Patti di Integrità*;
- ✓ *Azioni di sensibilizzazione e rapporto con la società civile*.

1.3. Le società in house e gli obblighi anticorruzione

Le *società in house* (di derivazione inglese, letteralmente "società in casa") sono società di diritto comune (generalmente società per azioni), il cui capitale sociale appartiene interamente ad un ente pubblico che le affida uno o più lavori.

Sul piano pratico, l'ente pubblico, anziché ricorrere al modello dell'*outsourcing* (ossia chiedendo la prestazione di un servizio o di una attività ad operatori economici esterni), utilizza la logica dell'*in house providing* e dunque attribuisce ad una società di cui è integralmente titolare, l'affidamento diretto del servizio o dell'attività.

Tale orientamento giudiziale europeo è stato formalizzato nel TUSP del 2016 – in particolare negli artt. 2 (*definizioni*) e 16 (*società in house*) – attraverso l'indicazione degli specifici e fondamentali elementi distintivi della *società in house*:

A) Partecipazione totalitaria dell'ente pubblico nella società privata o, come precisato nell'art. 16, "assenza di partecipazione di capitali privati" (principio già fissato dal Consiglio di Stato[4]);

B) Controllo analogo dell'ente pubblico;

C) Prevalenza dell'attività in favore dell'ente pubblico affidante (in misura superiore all'ottanta per cento del fatturato)

Viene, dunque, confermata e stigmatizzata la natura strettamente pubblicistica delle *società in house,* che peraltro anche la Corte di Cassazione, a Sezioni Unite, aveva riconosciuto al fine di farne derivare la piena soggezione delle azioni di responsabilità alla Corte dei Conti: «Le società in house hanno della società solo la forma esteriore ma costituiscono in realtà delle articolazioni della pubblica amministrazione da cui promanano e non dei soggetti giuridici ad essa esterni e da essa autonomi. ... Gli organi delle società in house sono preposti ad una struttura corrispondente ad un'articolazione interna alla stessa pubblica amministrazione, sicché è da ritenersi che essi siano personalmente a questa legati da un vero e proprio rapporto di servizio, non altrimenti di quel che accade per i dirigenti

[4] Ad avviso del quale è anche necessario che lo Statuto non consenta cessioni di capitali a soggetti privati (Adunanza Plenaria 1/2008, ud. 10 dicembre 2007; conf. sez. V, 3 febbraio 2009, n. 591, sez. V, 30 agosto 2006, n. 5072)

preposti ai servizi erogati direttamente dall'ente pubblico» (Corte di Cassazione, Sez. Un., 25 novembre 2013, n. 26823).

Circa il *controllo pubblico*, l'art. 2 del TUSP definisce:

- *Controllo*, quello descritto dall'art. 2359 c.c. (*società controllate e società collegate*) che si estrinseca attraverso le seguenti modalità: 1) maggioranza dei voti esercitabili nell'assemblea ordinaria; 2) voti sufficienti per esercitare un'influenza dominante nell'assemblea ordinaria; 3) influenza dominante per particolari vincoli contrattuali con essa.

- *Controllo analogo,* quello caratterizzato dalla «situazione in cui l'amministrazione esercita su una società un controllo analogo a quello esercitato sui propri servizi, esercitando un'influenza determinante sia sugli obiettivi strategici che sulle decisioni significative della società controllata» (anche il Consiglio di Stato, sez. II, 24 luglio 2020, n. 4728, precisa sul punto: «la società in house agisce come un vero e proprio organo dell'Amministrazione dal punto di vista sostanziale e, proprio per questo, è richiesto il requisito del controllo analogo» (Consiglio di Stato).

Avuto specifico riguardo al problema dell'applicabilità del Sistema Anticorruzione e Trasparenza, la Legge 190/2012 aveva adottato (attraverso l'art. 1 comma 34) una formula normativa oggettivamente ambigua, cui ha fatto seguito l'art. 11, secondo comma, del D.Lgs. 33/2013 (in materia di trasparenza).

Il D.Lgs. 97/2016 (che ha riformato sia la Legge 190/2012 che il D.Lgs. 33/2013) ha cercato di fare chiarezza attraverso l'abrogazione del succitato articolo 11 ad opera e l'agganciamento dell'applicabilità della normativa sulla trasparenza alle *società partecipate* ad un nuovo art. 2-*bis (Ambito soggettivo di applicazione).*

In materia è altresì intervenuta l'ANAC attraverso due specifici interventi:

- Linee Guida ANAC 2015, tramite Determinazione 17 giugno 2015 n. 8;
- Linee Guida ANAC 2017, attraverso Delibera 8 novembre 2017 n. 1134.

Con le Linee Guida 2015 – emesse antecedentemente al D.Lgs. 97/2016 e al TUSP – è stata effettuata una prima importante catalogazione delle strutture collettive di riferimento, non in termini di *società partecipate* ma di *enti.*

Gli *enti* sono stati, quindi, distinti in:

- *enti di diritto privato in controllo pubblico*;
- *enti di diritto privato non in controllo pubblico* (o meramente *partecipati*).

Nelle Linee Guida 2017 – successive al D.Lgs. 97/2016 e al TUSP, dai quali si sono ricavati importanti elementi di chiarezza e di indirizzo esegetico – l'ANAC ha, quindi, cercato di ricomporre con maggiore esaustività il quadro generale delle *società partecipate.*

Questo il quadro di riferimento generale tracciato dall'Autorità:

- le *misure di integrazione anticorruzione* sono quelle obbligatorie previste dall'art. 1, comma 2-*bis*, della Legge 190/2012, ossia quelle indicate nel Piano Nazionale Anticorruzione;
- gli *enti di diritto privato in controllo pubblico* (come appunto le società in house) sono tenuti ad adottare le misure integrative anticorruzione in misura integrale (v. analogamente alle pubbliche amministrazioni) e a nominare un Responsabile della prevenzione della corruzione e della trasparenza;
- ove sia stato redatto un Modello di Organizzazione, Gestione e Controllo 231, dette misure preventive possono integrare lo stesso Modello pervenendo ad un documento unitario che riporta entrambi i sistemi di gestione preventivo (MOGC 231 e PTPCT), ma in sezioni distinte non essendovi piena sovrapponibilità di reato presupposto e di processi a rischio; oppure, operare in parallelo.

Da ultimo, il Decreto Legge 9 giugno 2021 n. 80 (*Misure urgenti per il rafforzamento della capacità amministrativa delle pubbliche amministrazioni funzionale all'attuazione del Piano nazionale di ripresa e resilienza (PNRR) e per l'efficienza della giustizia)* convertito in Legge 6 agosto 2021 n. 113, ha introdotto l'istituto del Piano Integrato Attività e Organizzazione (P.I.A.O.).

Tale Piano dovrebbe includere in sé tutti i piani programmatici oggetto di approvazione nell'ambito delle pubbliche amministrazioni (inclusi il Piano della prevenzione della corruzione, il piano della performance, etc.), attraverso un Documento Programmatico unitario.

Circa la sua obbligatorietà ed ambito di applicazione, l'art. 6 del D.L. 80/2021 conv. in Legge 113/2021 dispone che il P.I.A.O. deve essere adottato dalle pubbliche amministrazioni di cui all'art. 1, comma 2, del D.Lgs. 30 marzo 2001 n. 165.

Il predetto art. 1, comma 2, del D.Lgs. 165/2001 stabilisce che: «per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti i del Servizio sanitario nazionale, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300. Fino alla revisione organica della disciplina di settore, le disposizioni di cui al presente decreto continuano ad applicarsi anche al CONI».

Non rientrano in questo elenco gli enti in controllo pubblico.

Ne deriva che gli stessi enti – tra cui le società in house - *non* sono soggette all'obbligo di predisposizione del P.I.A.O., ma solo del Piano della prevenzione della corruzione e della trasparenza o dell'integrazione del Modello 231 con le misure preventive anticorruzione.

Tale conclusione è stata pienamente confermata dall'ANAC nel documento *Orientamenti per la Pianificazione Anticorruzione e Trasparenza* approvato dal Consiglio dell'Autorità in data 2 febbraio 2022.

1.4. I reati presupposti ordinari

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 costanti interventi legislativi di natura integrativa e/o correttiva[5] - sono quelle espressamente indicate agli artt. 24, 24-*bis*, 24-*ter*,

5 V. modifiche anno 2024: L. 6/2024 modifica art. 25 septiesdecies; D.L. 19/2024 conv. in L. 56/2024 modifica art. 512 bis c.p. presupposto da art. 25 octies.1; L. 90/2024 modifica art. 640 c.p. presupposto da art. 24 e artt. 615 ter, 615 quater, 617 quater, 617 quinquies, 635 bis, 635 ter, 635 quater, 635 quinquies c.p. presupposti da art. 24 bis, nonché introduce artt. 635 quater.1 e 629, c.3, c.p. presupposti da stesso art. 24 bis; D.L. 92/2024 conv. in L. 112/2024 modifica art. 322 bis c.p. e introduce art. 314 bis c.p., entrambi presupposti da art. 24; L. 114/2024 estrapola da art. 25 art. 323 c.p. e modifica art. 346 bis c.p.; L. 166/2024 modifica reati presupposti dall'art. 25 novies ex artt. 171 bis, 171 ter e 171 septies della L. 633/1941; l. 187/2924 modifica art. 22 del D.Lgs. 286/1998 presupposto da art. 25 duodecies; D.Lgs. 87/2024 modifica art. 10 quater del D.Lgs. 74/2000 presupposto da art. 25 quinquiesdecies; D.Lgs 141/2024 introduce e modifica plurime fattispecie di contrabbando presupposte da art. 25 sexiesdecies

25, 25-*bis*, 25 *bis.*1, 25 ter, 25-*quater*, 25-*quater*.1, 25-*quinquies*, 25-*sexies*, 25-*septies*, 25-*octies*, *25 octies.1,* 25-*novies*, 25-*decies*, 25-*undecies*, 25-*duodecies, 25-terdecies,* 25-*quaterdecies,* 25-*quinquiesdecies, 25- sexiesdecies,* 25-*septiesdecies*, 25-*duodevicies.*

Le modifiche all'impianto normativo 231 possono essere effettuate attraverso:

A) una *introduzione ex novo di un articolo 231* di natura prescrittrice e sanzionatrice [es., la Legge 9 marzo 2022 n. 22 ha introdotto nel corredo dei reati presupposti 231 il nuovo art. 25 septiesdecies (delitti contro il patrimonio culturale)];

B) una *integrazione di natura prescrittrice e sanzionattrice diretta*, come nel caso della introduzione dei reati presupposti ordinari di cui agli artt 353 e 353 bis c.p. nell'art. 24 del Decreto 231, o del reato di cui all'art. 512 bis c.p. nell'art. 25 octies.1, ad opera del D.L. 10 agosto 2023, n. 105, convertito in Legge 9 ottobre 2023, n. 137 (*Disposizioni Urgenti in materia di processo penale, di processo civile, di contrasto agli incendi boschivi, di recupero dalle tossicodipendenze, di salute e di cultura, nonché in materia di personale della magistratura e della pubblica amministrazione*)

C) una *correzione di natura indiretta*, come nel caso della modfica "interna" degli artt. 615 ter e ss. c.p. ad opera della succitata Legge 90/2024, o della presa d'atto dell'abrogazione dell'art. 323 c.p. ad opera della Legge 25 agosto 2024 n. 114.

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 soltanto questi, e non altri, potranno giuridicamente legittimare l'affermazione di una "responsabilità amministrativa" *ex* D.Lgs. 231/2001 (*«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»:* Cass. Pen., Sez. II, 29 settembre 2009, n. 41488, che ha annullato 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.

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 di erogazioni pubbliche (art. 316-*bis* c.p.);
- ✓ Indebita percezione di erogazioni pubbliche (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 o di altro ente pubblico o delle Comunità europee (art. 640, co. 2, n.1 c.p.);
- ✓ Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.);
- ✓ Frode informatica in danno dello Stato o di altro ente pubblico (art. 640-*ter*) *[*reato rilevante ex D.Lgs. 231/2001 se in danno dello Stato*]*

.

❒ **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, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 - *quater* c.p.);
- ✓ Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.);
- ✓ Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche. (art. 617-*quinquies* c.p.);
- ✓ Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.);
- ✓ Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-*ter* c.p.);
- ✓ Danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.);
- ✓ Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635 *quater.1* c.p.)
- ✓ Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-*quinquies* c.p.);
- ✓ Estorsione (art. 629, comma 3, 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 (Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione)**:

- ✓ Peculato (art. 314, I comma) [reato rilevante *ex* Decreto 231 se *"il fatto offende gli interessi finanziari dell'Unione europea"*]
- ✓ Indebita destinazione di denaro o cose mobili (art. 314 bis, c.p.) [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, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e isti-gazione 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.);
- ✓ 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.);
- ✓ Fatti di lieve entità (art. 2621 bis c.c.);
- ✓ False comunicazioni sociali delle società quotate (art. 2622 c.c.);
- ✓ [FALSO IN PROSPETTO EX ART. 2623 C.C. ABROGATO]
- ✓ [FALSITA' NELLE RELAZIONI EX ART. 2624 C.C. ABROGATO]
- ✓ 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 a esercizio funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).
- ✓ False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 D.Lgs. 19/2023).

❒ **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 ss, 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 e trasferimento fraudolento di valori):***

- ✓ 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*, 171-*septies* e 171-*octies* della Legge 22 aprile 1941 n. 633 come modificati dalla Legge 14 novembre 2024 n. 166.

❒ **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*, lett. c) del D.Lgs. 25 luglio 1998 n. 286, come modificato dalla Legge 9 dicembre 2024 n. 187

❒ **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.Lgs. 5 novembre 2024 n. 173 (*Testo unico delle sanzioni tributarie amministrative e penali*)

- ✓ 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);
- ✓ Indebita compensazione (art. 10 quater);
- ✓ 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.Lgs. 24 ottobre 2024 n. 141 (*Codice Doganale Unione – Disposizioni Nazionali Complementari*), come aggiornato al D.Lgs. 5 novembre 2024 n. 173.

❒ **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.)

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..

È infine opportuno inoltre ricordare la seguente fattispecie che, pur non integrando i reati presupposto alla responsabilità dell'ente, introduce ipotesi di responsabilità amministrativa in relazioni alle quali si applicano gli artt. 6, 7, 8 e 12 D.Lgs. 231/2001.

D.Lgs. 129/2024 Adeguamento della normativa nazionale al regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937:

"Responsabilità dell'ente (art.34 D.Lgs. 129/2024)

L'ente è punito con la sanzione amministrativa pecuniaria da euro 30.000 fino a euro 15 milioni ovvero, se superiore, fino al 15 per cento del fatturato totale annuo, nel caso in cui sia commessa nel suo interesse o a suo vantaggio una violazione del divieto di cui agli articoli 89, 90 e 91 del regolamento (UE) 2023/1114:

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria o funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

Si applicano i commi 3 e 4 dell'articolo 32.

L'ente non è responsabile se dimostra che le persone indicate al comma 1 hanno agito esclusivamente nell'interesse proprio o di terzi.

In relazione agli illeciti di cui al comma 1 si applicano, in quanto compatibili, gli articoli 6, 7, 8 e 12 del decreto legislativo 8 giugno 2001, n. 231. Il Ministero della giustizia formula le osservazioni di cui all'articolo 6 del decreto legislativo 8 giugno 2001, n. 231, sentita la Consob, con riguardo agli illeciti previsti dal presente titolo".

1.5. I reati presupposti speciali anticorruzione

Importante annotazione è quella che riguarda i *"reati presupposti speciali"*, ovvero quei reati che l'ente - spontaneamente e nell'ambito della propria discrezionalità societaria – ha il diritto-potere di prevedere all'interno del proprio Modello di Organizzazione, Gestione e Controllo 231, a fini meramente organizzativi interni (e non, dunque, a fini esterni o di possibile rilevanza amministrativa /penalistica) con l'obiettivo di innalzare ulteriormente il proprio ed autonomo raggio di azione anti-illegatà interaziendale.

L'inserimento dei reati *presupposti speciali anticorruzione* acquista una pregnanza particolare in presenza di un ente che - come certamente una società in house – sia tenuto

per legge ad adottare un Piano Triennale Prevenzione Corruzione e Trasparenza (in forma autonoma o eventualmente in via di integrazione con il MOGC 231).

Peraltro, attraverso tale spontaneo inserimento, lo stesso P.T.P.C.T. potrà "usufruire" della mappatura e della gestione dei succitati *presupposti speciali anticorruzione,* normativamente esclusi dal novero del corredo 231 e facenti parte – invece - dell'obbligatorio pacchetto preventivo anticorruzione.

Accanto, dunque, ai *reati presupposti ordinari* di cui agli artt. 24 e ss. del D.Lgs. 231/2001, potranno essere liberamente presi in considerazione - quali *reati presupposti speciali anticorruzione* - i delitti richiamati dall'art. 1 comma 75, lett. c) e lett. p) della Legge 6 novembre 2012 n. 190 (*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione)*, come integrati dalla successiva normativa tra cui quella di cui alla Legge Legge 8 agosto 2024 n. 112 (che ha introdotto l'art. 314 bis c.p.):

- il reato di *peculato* (art. 314 c.p.);
- il reato di *indebita destinazione di denaro o cose mobili* (art. 314 bis c.p.);
- il reato di *peculato mediante profitto dell'errore altrui* (art. 316 c.p.), non richiamato direttamente dalla Legge Severino ma logicamente connesso al reato di peculato.

A questo riguardo va chiarito che la spontanea collocazione di tali reati nel raggio di azione del MOGC 231 è integrale e non solo – come stabilito nello stesso art. art. 25 del D.Lgs. 231/2001 - «*quando il fatto offende gli interessi finanziari dell'Unione europea*» (secondo la dicitura della Direttiva PIF 2017/1371).

Per incidens, l'offesa agli *interessi finanziari dell'Unione Europea* è di oggettivo remoto accadimento nella stragande maggioranza della piccole e medie imprese italiane.

Tale spontanea integrazione nel Modello 231 ha anche lo scopo di consentire una vigilanza preventiva integrale da parte dell' Organismo di Vigilanza.

1.6. 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)*[6]*,* 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.
- *Principi e Linee Guida ANAC* (soprattutto nel caso in cui si tratti di società in house, integralmente soggetta al Sistema Anticorruzione e Trasparenza), ovvero tutti i *principi di gestione del rischio* suggeriti dall'Autorità Nazionale Anticorruzione nei *Piani Nazionale Anticorruzione* adottati con cadenza annuale a partire dall'anno 2013, unitamente alle *Linee Guida ANAC - Ministero dell'Interno* 15 luglio 2014 e 27 gennaio 2015.

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 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

[6] 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.

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 prfesenza 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.

Dal che deriva:

- che è 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.

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 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 degli usuali rischi da commissione di reati presupposti ex Decreto 231).

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.

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 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;

Lo stesso sistema dovrà, dunque, 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.

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 ordinaramente inserite nello *Statuto OdV* dell'ente. (*infra,* 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 [7];
- 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[8], 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[9] 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* art. 2 della Legge 179/2017.

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.

---

[7] 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».

[8] «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).

[9] 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».

2.5 Il Whistleblowing

L'istituto, di origini anglosassoni, del *whistleblowing* - tra i più importanti cardini della nuova filosofia anticorruzione - è stato inserito nel D.Lgs. 231/2001 (esattamente all'art. 6) dalla 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*).

Storicamente, l'istituto è nato allo scopo di 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 ingiustamente discriminati o abbiano subito ritorsioni.

La prima *tutela da whistleblowing* è stata introdotta in ambito pubblicistico dalla Legge Severino 190/2012 e dal successivo D.L. 90/2014 convertito in Legge 114/2014.

Con il D.Lgs. 10 marzo 2023 n. 24 (recante "*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*"), la disciplina pubblicistica e quella privatistica sono state poi unificate.

Avuto specifico riguardo al Sistema 231, il D.Lgs. 24/2023 ha abrogato gli ex commi 2 ter[10] e 2 quater[11] dell'art. 6 del D.Lgs. 231/2001 (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:
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».

Preso atto che il D.Lgs. 24/2023 ha rivisto in via unitaria la regolamentazione del *whistleblowing* (frutto, si ribadisce, della duplice normativa, di tipo pubblicistico ex Legge

[10] «*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».*

[11] «*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».*

190/2012 e di tipo privatistico ex Legge 179/2017), i nuovi principi e norme regolatrici sono:

A) I cd. *"segnalanti",* ai sensi del succitato Decreto Legislativo, possono essere non solo dipendenti, ma anche collaboratori, azionisti, persone che esercitano (anche in via di mero fatto) funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza della società e altri soggetti terzi che interagiscano con la società (ad esempio, i consulenti), nonché stagisti o lavoratori in prova, candidati a rapporti di lavoro ed ex dipendenti. A differenza, dunque, della precedente disciplina, il D.Lgs. 24/2013 ha ampliato la platea dei soggetti che - in ragione del coinvolgimento in una segnalazione – necessitino protezione. Le misure di tutela previste per i *segnalanti* trovano, altresì, applicazione con riferimento a: facilitatori; persone del medesimo contesto lavorativo della persona segnalante e che sono legati a essa da uno stabile legame affettivo o di parentela entro il quarto grado; colleghi di lavoro della persona segnalante che lavorano nel medesimo contesto lavorativo e che hanno con il segnalante un rapporto abituale e corrente; enti di proprietà della persona segnalante o che operano nel medesimo contesto lavorativo della stessa.

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

C) 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).

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

E) 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"*.

F) Le informazioni sulle "*segnalazioni*" dovranno essere esposte e rese facilmente visibili nei luoghi di lavoro, nonché 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, anche del settore privato, pubblicano dette informazioni in una sezione dedicata del suddetto sito.

G) 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 dalla violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

H) Le disposizioni del whistleblowing <u>non</u> si applicano (ai sensi di quanto espressamente disposto dall'art. 1, comma, del D.Lgs. 23/2024) *«alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che*

attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate»;

I) L'organo deputato alle "*segnalazioni esterne*" è l'Autorità Nazionale Anticorruzione (ANAC), la quale ha previsto 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, salvo esplicita richiesta contraria della persona segnalante ovvero salvo il caso in cui l'ANAC ritenga che l'avviso pregiudicherebbe la protezione della riservatezza dell'identità della persona segnalante; 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.

J) 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 della persona segnalante alla rivelazione della propria identità.

K) 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.

L) 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.

M) 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.

N) Avuto riguardo alle *sanzioni* eventualmente 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, nonché 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).

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

Va, altresì, ricordato che le violazioni che possono essere oggetto di *segnalazione* sono quelle che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e - secondo quanto chiarito dall'Autorità Nazionale Anticorruzione - consistono in:

1) illeciti amministrativi, contabili, civili o penali;

2) condotte illecite rilevanti ai sensi del Decreto Legislativo 231/2001, 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;

5) atti od omissioni riguardanti il mercato interno;

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

ATM SpA Trapani – che già aveva previsto nella precedente versione del Modello 231 la *tutela da whistleblowing,* ai sensi dell'art. 6 del D.Lgs. 231/2001 - si è oggi pienamente adeguata alla novella legislativa ex D.Lgs. 24/2023, attraverso l'acquisto di una piattaforma informatica, appositamente conformata in base ai crismi di legge, utile alla gestione del *canale interno delle segnalazioni.*

Sul sito, sarà debitamente illustrata la procedura di accesso e di inserimento delle segnalazioni.

La concreta *gestione del canale interno* viene affidata – in via congiunta – all'Organismo di Vigilanza 231 e al Reponsabile della prevenzione della corruzione e della trasparenza.

2.6 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.

In chiave operativa, le norme di un *Codice Etico e/o di Codice 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/o 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/o 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.

PARTE II – Il Modello 231 di ATM SpA Trapani

1. STORIA E ATTUALE STRUTTURA SOCIETARIA DI ATM SPA TRAPANI

Costituita il 28 dicembre 1995 come Azienda Speciale - S.A.U. (Servizi Autofiloviari Urbani) del Comune di Trapani, per l'esercizio di trasporto pubblico con mezzi di linea, la Società è stata trasformata in Società per Azioni, ai sensi dell'art. 115 del D.Lgs. 267/2000, con Delibera del Consiglio Comunale n. 4 del 22 gennaio 2007.

Socio Unico: Comune di Trapani.

Lo Statuto Sociale è stato poi modificato - al fine di adeguarsi al D.Lgs. 175/2006 (T.U. Società Partecipate), di ampliare l'oggetto sociale e di ammettere la possibile ammissione come soci di ulteriori enti local - con Verbale di Assemblea del 27 giugno 2019.

❒ **Sedi operative**

Il contratto di servizio tra il Comune di Trapani e ATM, siglato in data 19/03/2007, nell'art. 3 riportava che per i primi sei anni ATM avrebbe avuto pieno utilizzo degli immobili destinati o impiegati per i servizi di trasporto pubblico urbano.

Allo stato attuale, ATM continua ad utilizzare gli uffici amministrativi, gli immobili destinati alla riparazione, lavaggio e ricovero degli autobus a titolo gratuito, che richiedono una profonda ristrutturazione.

Con l'accordo di collaborazione / protocollo d'intesa siglato il 20/05/2008 tra il Comune di Trapani e ATM veniva concesso in uso alla stessa Società l'immobile (Terminal City) sito nell'odierna Piazzale Papa Giovanni Paolo II per la durata di anni 8.

Sono ancora in corso interlocuzioni con il Socio Unico nella definizione di un contratto di locazione e relativo canone annuo per i suddetti immobili

❒ L'**oggetto sociale** previsto in Statuto è:

a) La gestione del trasporto pubblico collettivo attuato in ogni forma e con qualsiasi mezzo, e di ogni altra attività, anche strumentale, connessa e/o complementare alla mobilità ed al traffico ivi compresi anche i servizi di manutenzione e riparazione di parchi rotabili di qualsiasi tipologia, per conto proprio e di terzi e la gestione e la vendita di ricambi.

b) L'organizzazione e la gestione dei servizi relativi alla viabilità ed al traffico quali la rimozione coatta dei veicoli, i parcheggi, la sosta tariffata, i semafori, la segnaletica stradale, i sistemi di controllo degli accessi e dei transiti, il *road pricing* ed ogni altra attività connessa.

c) L'apposizione di cartellonistica pubblicitaria e la rimozione di cartellonistica abusiva.

d) Le eventuali funzioni di agenzia del Comune per la mobilità, anche al fine di pianificare, regolare e controllare l'esercizio del trasporto nel territorio comunale.

e) La produzione di servizi di interesse generale, ivi inclusa la realizzazione e la gestione delle reti e degli impianti funzionali ai servizi medesimi, mediante prestazioni di servizi energetici nei confronti di tutti i componenti ed i soggetti della catena di produzione e/o utilizzo di energia e l'offerta di servizi integrati per la realizzazione e la gestione di interventi di efficienza energetica (tra i quali, a titolo meramente esemplificativo e non esaustivo, l'analisi dei propri consumi energetici e/o di terzi, la valorizzazione economica degli interventi di efficienza energetica anche mediante la gestione efficiente degli impianti esistenti, la realizzazione di attività per il contenimento dell'inquinamento ambientale, la ricerca di fonti di finanziamento, direttamente e/o tramite terzi, anche mediante forme condivise di investimento e/o di risparmio, degli interventi di cui sopra, etc.).

Sempre secondo quanto previsto nello Statuto, la Società può:

✓ realizzare e gestire le attività di cui sopra, anche al di fuori dell'ambito territoriale di Trapani, direttamente, in concessione, in appalto o in qualsiasi altra forma, anche a seguito di richiesta di terzi non soci, purché essi siano enti pubblici;

✓ operare direttamente ed avvalersi di terzi;

✓ effettuare studi, progettazioni ricerche tecnologiche e consulenze e attività amministrative, tecniche, organizzative, finanziarie e gestionali ad Enti Pubblici e privati;

✓ provvedere alla progettazione ed alla costruzione degli impianti destinati all'esercizio dell'attività propria, direttamente o tramite affidamento a terzi nel rispetto delle norme di legge;

✓ compiere, nell'ambito dell'oggetto sociale e delle attività comunque ad esso connesse, qualsiasi operazione immobiliare, mobiliare, commerciale, bancaria, industriale e tecnica, necessaria ed utile ai propri scopi, compresa l'assunzione di finanziamenti e mutui passivi, anche ipotecari;

✓ richiedere contributi e prestare garanzie ipotecarie in favore proprio ed anche di terzi.

✓ assumere - sempre in via strumentale al compimento dell'oggetto sociale e delle attività comunque ad esso connesse, ed in eventuale associazioni di imprese - appalti, nonchè affidare lavori e servizi, gestire beni, complessi di beni e strutture di terzi e compiere ogni altra operazione di carattere tecnico, commerciale, industriale, immobiliare e finanziario.

✓ raccogliere presso i propri soci e nel rispetto delle leggi e dei regolamenti vigenti, i fondi necessari per il conseguimento dell'oggetto sociale.

❒ Tutte le **operazioni che riguardano il capitale sociale** (variazioni, versamenti, gestione azioni, cessioni, opzioni e prelazioni, recessi etc.) possono essere compiute esclusivamente dal Socio Unico.

❒ Sono **organi della Società**:

- L'Assemblea dei Soci;
- L'Organo amministrativo (attualmente composto da un Consiglio di Amministrazione a tre membri, compreso il Presidente);
- Il Collegio Sindacale (composto da tre membri effettivi, compreso il Presidente);
- il Direttore Generale (nominato dall'Organo Amministrativo e responsabile della gestione operativa della società e dell'attuazione delle linee strategiche e delle disposizioni impartite dallo stesso Organo amministrativo.
- Il Revisore Legale dei conti (in forma individuale o societaria).

❒ Tra le peculiarità della struttura istituzionale e societaria di ATM Trapani – in termini assolutamente analoghi a tutte le società in house – vi è la soggezione al **controllo analogo** da parte del Socio Unico.

Stabilisce, al riguardo, l'art. 32 bis dello Statuto:

«*1. L'Ente Pubblico socio, in conformità all'art. 5, comma 5, del D.Lgs. 18 aprile 2016, n. 50, agli artt. 2, comma 1, e 16 del D.Lgs. 19 agosto 2016, n. 175, esercita sulla società e sui servizi pubblici ad essa affidati un controllo analogo a quello svolto sui propri servizi.*

2. A tal fine, se la società ha un solo Ente pubblico socio esso è titolare di specifici poteri di ispezione e supervisione che esercita, secondo modalità specificate negli atti negoziali che disciplinano l'affidamento dei servizi, attraverso un responsabile individuato al suo interno per ciascun servizio affidato. Il socio affidante ha diritto di esercitare controlli diretti sulla qualità del servizio affidato; inoltre, ha diritto di esercitare sul bilancio societario, oltre al potere ed ai diritti derivanti dalla partecipazione alla compagine societaria, verifiche specifiche per gli effetti che sullo stesso derivano dal servizio affidato in house e sulla coerenza delle scelte aziendali di programmazione e tecnica con gli obbiettivi da raggiungere con il servizio affidato; esso, ancora, attraverso il proprio rappresentante legale, può proporre alla

società specifiche iniziative per la migliore attuazione del servizio affidato e questa dovrà comunicare senza indugio al socio le deliberazioni assunte sulle predette proposte».

Attualmente il Socio è Unico (Comune di Trapani); pertanto, *non* è operativo il controllo analogo congiunto.

❒ L'attuale **fotografia gestionale** è quella riportata nella Relazione sulla Gestione al Bilancio di esercizio al 31.12.2023.

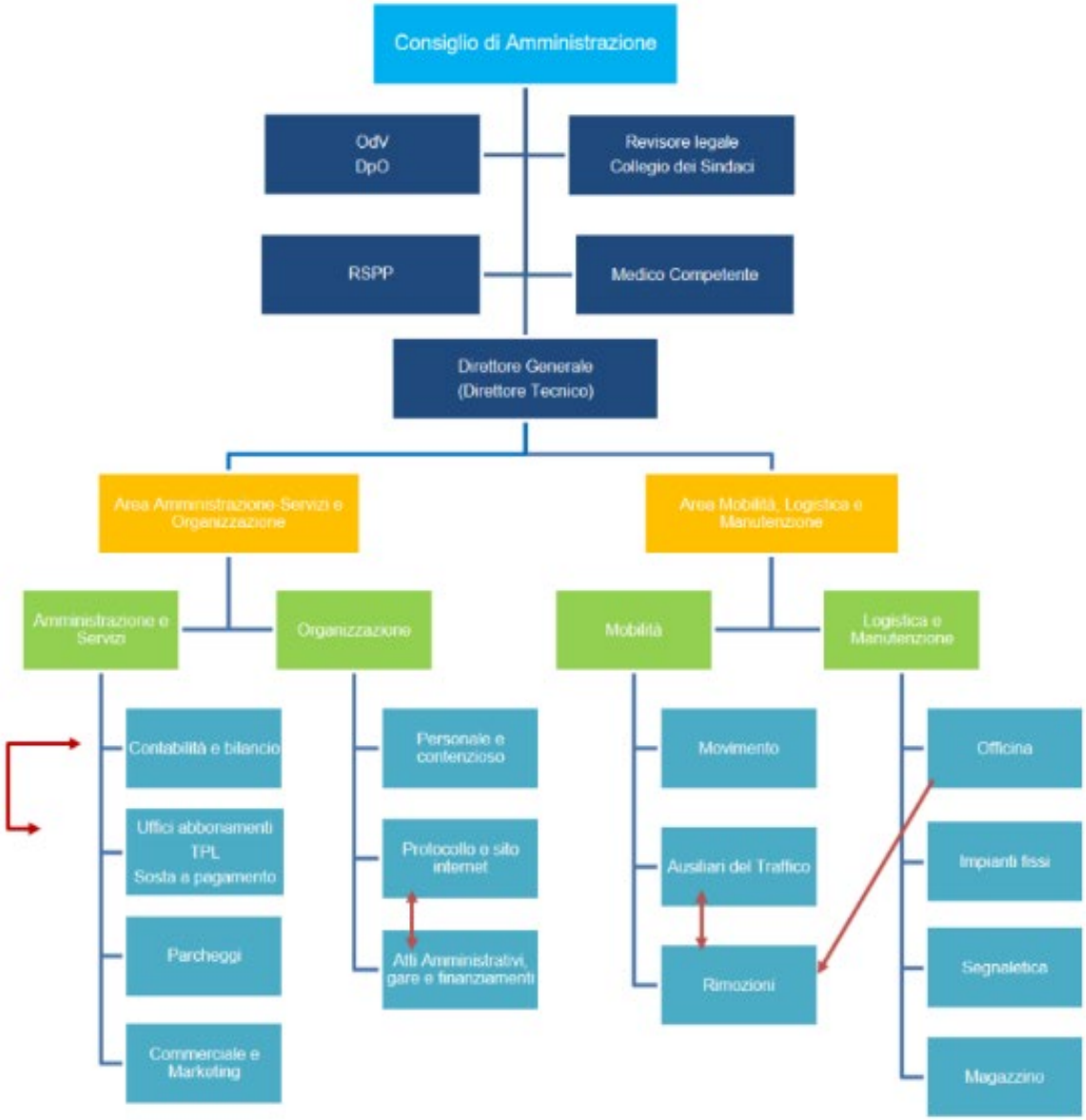
✓ **Campo di attività** svolte attualmente (su concessione e per conto del Comune di Trapani):

- **Trasporto Pubblico Locale**: ATM opera nel territorio del Comune di Trapani sulla base di un contratto di servizio stipulato con l'Ente proprietario e all'interno del contiguo territorio del Comune di Erice - sulla base di un'apposita convenzione stipulata il 14/03/1978, fra il Comune di Trapani ed il Comune di Erice, successivamente modificata in data 13/02/1995. Il contratto di servizio, identificato dal Repertorio Generale n. 22604 del 2021, redatto secondo lo schema stabilito dalla Regione Siciliana è stato prorogato lo scorso 22/03/2023 e avrà scadenza il prossimo 02/12/2024, contratto tuttavia che non avrà termine operativo prima del 02/12/2026

- **Gestione aree di sosta a pagamento (strisce blu)**: il Consiglio Comunale di Trapani con propria Delibera n. 70 del 24/06/2019 ha stabilito il rinnovo dell'affidamento con scadenza per il prossimo 31/12/2028, rinnovabile per ulteriori anni 9.
- **Gestione dei parcheggi "Egadi" e "Multipiano":** il Consiglio Comunale di Trapani con propria Delibera n. 70 del 24/06/2019 ha stabilito il rinnovo dell'affidamento con scadenza per il prossimo 31/12/2028, rinnovabile per ulteriori anni 9.
- **Gestione servizio di ripristino e manutenzione della segnaletica stradale**: Con la Delibera Dirigenziale n. 2240 del 24/08/2018 il V Settore, Comando di Polizia Locale, ha proceduto all'affidamento in house del servizio in oggetto ad ATM. In data 30/08/2018 veniva siglato il relativo contratto di servizio tra il Comune di Trapani ed ATM con scadenza fissata per il prossimo 31/12/2020. Il Consiglio Comunale di Trapani con propria Delibera n. 53 del 28/06/2021 ha stabilito il rinnovo dell'affidamento con scadenza per il prossimo 31/12/2029.

Gli affidamenti "in house" delle aree di sosta a pagamento, del parcheggio "Multipiano", del parcheggio "Egadi" e in ultimo la gestione della "manutenzione della segnaletica stradale" hanno rappresentato, delle iniziative molto importanti per lo sviluppo e la crescita di ATM come azienda impegnata attivamente nell'area mobilità, che di fatto si sono aggiunte alla gestione del "Trasporto Pubblico Locale" che da sempre è stato il fulcro operativo di questa Azienda che già dal lontano 2007 periodicamente, e secondo i dettami della Regione Siciliana, ha sempre visto prorogare il suddetto Contratto di Servizio.

✓ **Organigramma della Società:**



✓ **Descrizione andamento della gestione**

ATM ha chiuso il 2023 con un utile di esercizio, al netto delle imposte, di € 48.736 con un Valore della Produzione superiore in termini relativi di circa il 9,7% rispetto al dato del 2022.

✓ **Informazioni D.lgs. n. 14/2019 e sue modifiche ed integrazioni.**

ATM Spa Trapani, come previsto dal D.lgs. n. 14/2019 (Codice della crisi e dell'insolvenza d'impresa), ha adottato un assetto organizzativo, amministrativo e contabile adeguato alla natura dell'impresa anche in funzione della rilevazione tempestiva della crisi d'impresa e dell'assunzione di idonee iniziative, il tutto anche ai sensi dell'art. 3 e dell'art. 25-*nonies* del CCII.

Inoltre, alla data di chiusura del bilancio, ATM:

- non possiede alcuna azione propria, né ha realizzato operazioni di compravendita nel corso dell'esercizio di azioni proprie o altrui;

- non ha fatto uso di strumenti finanziari e non è esposta a particolari rischi di variazione di flussi finanziari;
- il suo rischio di credito, connesso al normale svolgimento delle attività operativa, è costantemente monitorato;
- non è esposta al rischio di liquidità in quanto ritiene di avere accesso a fonti di finanziamento sufficienti a soddisfare le prevedibili necessità finanziarie, come ampiamente dimostrato nella parte relativa agli indici finanziari.
- non ha posto in essere operazioni con parti correlate ex art. 2427, primo comma, n. 22 bis c.c.

2. MAPPATURA RISCHIO DA ILLICEITÀ EX DECRETO 231

2.1. Mappatura rischi e approccio metodologio

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 - *a fortiori* di un Modello "*rinforzato ex Legge 190/2012 e correlato Sistema Anticorruzione",* come nello specifico caso di ATM SpA Trapani - sono:

a) la **"*mappatura dei rischi di reato*"** (***Crime Risk Assessment***);

b) la "*gestione del rischio di reati"* (C*rime Risk Management*).

Una 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 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*, *ordinari* o *speciali anticorruzione*).

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

Sia il Decreto Legislativo 231/2001 che la Legge 190/2012 (entrambi presupposti logico-normativi del Modello 231 di ATM SpA Trapani) sono, del resto, provvedimenti legislativi emessi allo specifico scopo di prevenire *reati* e *condotte illecite.*

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.

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*.

Preliminare, al riguardo, chiarire che *non* esiste una metodologia "obbligata", potendo la stessa analisi essere effettuata:

- per *reati,* ossia partendo dall'analisi e valutazione dei *reati presupposti,* di cui lo stesso Legislatore 231 chiede espressamente la previsione e l'evitabilità;
- per *processi,* sul presupposto che qualunque attività aziendale è costituita da un insieme di processi[12] tra di loro correlati;

[12] 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.

- per *funzioni,* atteso che le condotte illecite non sono altro che azioni umane poste in essere da soggetti fisici, quali partecipanti ad un determinato processo di lavoro e quindi potenzialmente in grado di commettere reati o illiceità di rilevanza penale.

La metodologia di analisi e di approccio è – per consolidata ed unanime opinione – assolutamente libera, purchè si raggiunga 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» (Linee Guida Confindustria).

Lo stesso art. 6, comma 2, lett. a), del Decreto 231 si limita a dire: «individuare le attività nel cui ambito possono essere commessi reati».

Anche nella legislazione anticorruzione si parla - genericamente - di *"uffici esposti al rischio corruzione*" o di *"attività",* come ad esempio nelle ipotesi esemplificative individuate dall'art. 1 comma 53 della Legge 190/2012, in cui si indicano quali "*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»;

Il dato certo è che, qualunque sia la denominazione utilizzata, 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 *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*.

Ove correttamente svolte: l'analisi dei reati a rischio di verificazione e l'analisi dei processi o delle funzioni a rischio di deviazione illecita dovrebbero combaciare.

2.2. Mappatura rischi da reati presuppposti 231

Il dato da cui partire ai fini di una corretta mappatura dei "rischi da reato" all'interno di una struttura aziendale, è rappresentato – per preciso volere del Legislatore 231 – dai *reati presupposti* (oggetto di doverosa previsione ed evitabilità), nel loro possibile e concreto estrinsecarsi all'interno di una specifica realtà aziendale.

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

Considerato, poi, 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".

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*".

O si pensi, altresì, agli specifici *reati presupposti* di "natura informatica", in numero 23, tutti disordinatamente distribuiti tra gli artt. 24-*bis*, 25-*quinquies*, 25-*novies* del D.Lgs. 231/2001; tutto ciò, nonostante gli stessi reati siano 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), cui viene affidato il "processo" sensibile sottostante all'"area" risorse informatiche.

Ne deriva quindi – avuto riguardo al predetto esempio dei reati informatici ex Decreto 231 – la necessità di mappare, valutare e gestire: i r*eati contro il patrimonio commessi mediante l'uso del mezzo informatico* presupposti dall'art. 24-*bis;* i *reati lato sensu informatici,* presupposti dallo stesso art. 24-*bis* ma facenti parte di altra famiglia penalistica; i *reati a mezzo web contro la personalità individuale,* presupposti dall'art. 25-*quinquies;* i reati che derivano dalla *violazione del diritto di autore* (presupposti dall'art. 25-*novies*).

Quanto sin qui detto - in via generale - dimostra la necessità di *riordinare* 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; il che conduce ad un accorpamento in aree comuni di tutti i "reati presupposti" connessi per raggio di azione e similitudini giuridiche, 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.

Tale quadro normativo - che, alla fine, è la risistemazione 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;

B) *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 1**).

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:

- *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. 314 bis c.p. - indebita destinazione di denaro o cose mobili: reato presupposto dall'art. 25* [reato rilevante *ex* Decreto 231 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 ……: reato presupposto dall'art. 25;*
- *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 presupposto dall'art. 24.*
- *art. 356 c.p. - frode nelle pubbliche forniture: reato presupposto dall'art. 24.*

Come chiarito nella Parte Generale, accanto ai succitati *reati presupposti ordinari,* ATM SpA Trapani ha deciso di includere nel suo MOGC anche i cd. *reati presupposti speciali*, ossia quelle fattispecie delittuose formalmente estranee al D.Lgs. 231/2001, ma spontaneamente analizzate e valutate al fine di sottoporle ad una efficace azione di monitoraggio e controllo, anche da parte dell'Organismo di Vigilanza.

Rientra in questa specifica macro area - *delitti contro la pubblica amministrazione* espressamente enucleati nella Legge 190/2012 e nel D.L. 90/2014 conv. in L. 114/2014 – i reati, nella loro massima estensione ovvero oltre il ristretto raggio di azione *"se il fatto offende gli interessi finanziari dell'Unione Europea"* di cui al D.Lgs 75/2020, di cui agli artt. 314, 314 bis e 316 c.p..

❒ 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 o di altro ente pubblico o delle Comunità europee: reato presupposto dall'art. 24;*
- *art. 640 bis c.p. - truffa aggravata per il conseguimento di erogazioni pubbliche: reato presupposto dall'art. 24.*

Anche in questo caso vale quanto prima detto a proposito dell'inserimento nella macro area in oggetto, accanto ai succitati *reati presupposti ordinari,* dei *reati presupposti speciali* richiamati dalla Legge 190/2012.

Perfettamente enucleabile nella succitata macroarea dei *Delitti contro il patrimonio in danno della P.A.* sono i reati di cui agli:

- *art. 314 c.p. – peculato - reato presupposto dall'art. 1, comma 75, lett. c) della Legge 190/2012* – considerato integralmente, ovvero anche oltre le ipotesi in cui il fatto offenda *"gli interessi finanziari dell'Unione europea*" per come invece disposto dal D.Lgs. 75/2020.
- *art. 314 bis c.p. - indebita destinazione di denaro o cose mobili – reato presupposto introdotto dalla Legge 1124 del 2024* - considerato integralmente, ovvero anche l'eventuale offesa a *"gli interessi finanziari dell'Unione europea*" prevista dal Decreto 231.
- *art. 316 c.p. – peculato mediante profitto dell'errore altrui: reato non presupposto dalla Legge 190/2012 ma logicamente connesso a quello di cui all'art. 314 c.p.* - considerato integralmente, ovvero anche oltre le ipotesi in cui il fatto offenda *"gli interessi finanziari dell'Unione europea*" per come invece disposto dal D.Lgs. 75/2020.

❒ Area rapporti con 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; nell'area afferente il cd. libero mercato dovrebbero invece inquadrarsi le attività condotte da ATM SpA Trapani in favore di privati.

Tali attività sono, in realtà, inesistenti in quanto la Società si muove solo, ed esclusivamente, nell'ambito dei servizi di natura pubblicistica.

I reati riferibili a quest'area – che si è detto essere estranea ad ATM - presuppongono l'esercizio di una attività diretta ad una produzione industriale o ad una attività commerciale.

Le ipotesi delittuose riferibili a questa macro area sono:

- *art. 513 c.p. - turbata libertà dell'industria ….: reato presupposto dall'art. 25 bis.1;*
- *art. 513 bis c.p. - Illecita concorrenza …..: 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 ….: reato presupposto dall'art. 25 bis.1;*
- *art. 517 c.p. - vendita di prodotti industriali …: reato presupposto dall'art. 25 bis.1;*
- *art. 517 ter c.p. - fabbricazione e commercio ….: reato presupposto dall'art. 25 bis.1;*
- *art. 517 quater c.p. - contraffazione di indicazioni…..: 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 ATM - 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 ATM SpA Trapani.

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

Contro la Fede Pubblica:

- *art. 453 c.p. - falsificazione di monete ….: 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…..: reato presupposto dall'art. 25 bis;*
- *art. 457 c.p. - spendita di monete falsificate….: reato presupposto dall'art. 25 bis;*
- *art. 459 c.p. - falsificazione di valori di bollo …: reato presupposto dall'art. 25 bis;*
- *art. 460 c.p. - contraffazione di carta filigranata …..: reato presupposto dall'art. 25 bis;*
- *art. 461 c.p. - fabbricazione o detenzione ….: reato presupposto dall'art. 25 bis;*
- *art. 464 c.p. - uso di valori bollati contraffatti … reato presupposto dall'art. 25 bis;*
- *art. 473 c.p. - Contraffazione, alterazione …: reato presupposto dall'art. 25 bis *;*
- *art. 474 c.p. - Introduzione nello Stato …: 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 …: 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.

❒ 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);*
- *False o omesse dichiarazioni per il rilascio del certificato preliminare (art. 54 del D.Lgs. 19/2023)*

➢ ***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 in oggetto sono quelli previsti dal D.Lgs. 2000 n. 74, aggiornato al D.L. 26 ottobre 2019 n. 124 (poi modificato e convertito in 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. 10 quater. Indebita compensazione: 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), dal D.Lgs. 14 giugno 2024, n. 87 e dal D.Lgs. 5 novembre 2024, n. 173 (tuttora in fase di implementazione e coordinamento), 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* - per come aggiornati dal ***D.Lgs. 24 ottobre 2024 n. 141*** (*Codice Doganale Unione - disposizioni nazionali complementari*)

❒ 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" ATM, sia come dipendente che come vertice ed amministratore.

Le condotte illecite di cui si parla sono:

- *art. 583 bis c.p. - pratiche di mutilazione ….: reato presupposto dall'art. 25 quater.1;*
- *art. 600 c.p. - riduzione o mantenimento …….: 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 …: reato presupposto dall'art. 25 quinquies;*
- *art. 604 bis - propaganda e istigazione….: reato presupposto dall'art. 25 quinquies;*
- *art. 609-undecies – adescamento di minorenni: reato presupposto dall'art. 25 quinquies;*
- *art. 377 bis c.p. - Induzione a non rendere …: 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 …: reato presupposto dall'art. 25 duodecies;*
- *art. 22, comma 12 bis del D.Lgs. 25 luglio 1998 n. 286 …. 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 ….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 ….: 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 …. - 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 ATM.

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 pubblici o di interesse pubblico: 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 quater.1 c.p. - 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. 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;*
- *art. 629, comma 3, c.p. – estorsione: 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. 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 e dalla Legge 14 novembre 2024, n. 166.

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, modificati dalla L. 248/ 2000 e dalla Legge 14 novembre 2024, n. 166.

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: l'inserimento, nel codice penale, del *Titolo VI-bis* del *Libro Secondo*, con i correlati artt. 452-*bis* e ss.; 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*; 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).*
- 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*).
- I reati previsti dalla Legge 28 dicembre 1993, n. 549 ("*Misure a tutela dell'ozono stratosferico e dell'ambiente*"), ed in particolare 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 ex artt. 9 *(Inquinamento colposo)* e *8 (Inquinamento doloso).*

❒ Area Reati contro il Patrimonio Culturale

- *art. 518 bis c.p. - furto di beni culturali: reato presupposto dall'art. 25 septiesdecies;*

- *art. 518 ter c.p. - appropriazione indebita di beni culturali: reato presupposto dall'art. 25 septiesdecies;*
- *art. 518 quater c.p. - ricettazione di beni culturali: reato presupposto dall'art. 25 septiesdecies;*
- *art. 518 octies c.p. - falsificazione in scrittura privata relativa a beni culturali: reato presupposto dall'art. 25 septiesdecies;*
- *art. 518 novies c.p. - violazioni in materia di alienazione di beni culturali: reato presupposto dall'art. 25 septiesdecies;*
- *art. 518 decies - importazione illecita di beni culturali: reato presupposto dall'art. 25 septiesdecies;*
- *art. 518 undecies - uscita o esportazione illecite di beni culturali: reato presupposto dall'art. 25 septiesdecies;*
- *art. 518 duodecies c.p. - distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici: reato presupposto dall'art. 25 septiesdecies;*
- *art. 518 quaterdecies c.p. - contraffazione di opere d'arte: reato presupposto dall'art. 25 septiesdecies;*
- *art. 518 sexies c.p. - Riciclaggio di beni culturali: reato presupposto dall'art. 25 duodevicies;*
- *art. 518 terdecies - Devastazione e saccheggio di beni culturali e paesaggistici: reato presupposto dall'art. 25 duodevicies.*

2.3. Mappatura principali processi/procedimenti a rischio di illiceità

Come chiarito nel superiore paragrafo 2.1., la mappatura delle aree sensibili al rischio di commissione di condotte illecite, ed in particolare di reati presupposti dal Decreto 231, può essere effettuata attraverso vari approcci metodologici.

Nel paragrafo precedente, è stata illustrata l'analitica individuazione logica delle categorie "familiari" relative a tutti i *reati presupposti* ex Decreto 231, sia "ordinari" che cd. "speciali anticorruzione".

Nel presente paragrafo, sono individuati i principali *processi di lavoro* e *procedimenti* di ATM.

Va ricordato, sul punto, che i *processi di lavoro* individuano quelle porzioni di attività lavorative basate su una concatenazione di azioni finalizzate ad uno stesso obiettivo.

I *processi di lavoro* sono ordinariamente presidiati dalle relative *funzioni* (processo acquisti = funzione acquisti; processo assunzione personale = funzione risorse umane; processo sicurezza sui luoghi di lavoro = funzione responsabile sicurezza; etc. etc.).

Processi e *funzioni* sono correlati tra di loro in un in un sistema organico, che è poi quello che dà vita alla *organizzazione aziendale*.

Nello specifico caso di una attività amministrativa pubblica, o parapubblica (come quella svolta da ATM), si utilizza anche il termine "*procedimento",* cui è correlata l'unità organizzativa affidata ad un *responsabile*[13]*.*

L' attività di una pubblica amministrazione si sviluppa, infatti, non solo sulla base dei *processi* (categoria di rilevanza organizzativa che, come prima visto, individua la successione strutturata e l'insieme di azioni/attività volte a produrre un determinato risultato, prodotto o servizio), ma anche dei *procedimenti*, quale sequenza ordinata di atti/attività finalizzati all'emanazione di un provvedimento di rilevanza giuridico-amministrativa.

Per ciò che da vicino afferisce ad ATM SpA Trapani: va preso atto, in via generale, che la presenza di *procedimenti* è ad alta frequenza non solo nelle pubbliche amministrazioni ma anche nelle società in house (valga, per tutti, l'ambito dei contratti pubblici o degli strumenti di scelta pubblicistica dei dipendenti di cui si parlerà *infra*).

Ciò comporta che la *mappatura* - nelle situazioni in cui l'attività societaria si snodi attraverso questi specifici percorsi procedimentali - dovrà opportunamente tenerne conto, individuandoli e valutandoli ai fini della conseguente regolamentazione e disciplina preventiva.

Avuto specifico riguardo ai *procedimenti* definibili "a rischio illiceità", alcuni vengono in realtà espressamente indicati dallo stesso Legislatore, come ad esempio quelli richiamati (seppur ai fini dei livelli essenziali di trasparenza) dall'art. 1, comma 16, della Legge 190/2021:

a) autorizzazione o concessione (* *che tuttavia puo riguardare solo le P.A. in senso stretto*);

b) scelta del contraente per l'affidamento di lavori, forniture e servizi (* *che rientra certamente nei percorsi operativi di una società in house*);

c) concessione ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché attribuzione di vantaggi economici di qualunque genere a persone ed enti pubblici e privati (* *solitamente riguardante le P.A. in senso stretto*);

d) concorsi e prove selettive per l'assunzione del personale e progressioni di carriera (**che afferisce anche all'attività delle società in house*).

Va da sé che i *procedimenti* di rilevanza giuridica rientrano nei relativi *processi* di rilevanza organizzativa, tra cui (ad esempio) quelli genericamente finalizzati:

- all'adozione di provvedimenti ampliativi della sfera giuridica dei destinatari con effetto economico diretto ed immediato per il destinatario;
- all'affidamento di lavori, servizi e forniture, nonché all'affidamento di ogni altro tipo di commessa o vantaggio pubblici in materia di appalti pubblici;
- all'adozione di provvedimenti ampliativi della sfera giuridica dei destinatari privi di effetto economico diretto ed immediato per il destinatario;
- all'acquisizione e alla progressione del personale.

Dal punto di vista giuridico (e non strettamente organizzativo), va segnalato che i *procedimenti* non sono direttamente sovrapponibili ai *processi* (se non in via di contiguità

[13] 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*».

dell'oggetto), atteso che tra le due categorie esiste un rapporto che potrebbe essere definito tra *genus* (il processo) e *species* (il procedimento).

Sul piano pratico ed agli specifici fini della *gestione del rischio,* ciò comporta un possibile/probabile rischio di illiceità oggettivamente diverso (pur se parimenti valevole ai fini di un *sistema di gestione del rischio da "illiceità*").

A titolo di esempio: la cattiva gestione di un *processo* potrebbe ridursi ad una semplice disfunzione di tipo organizzativo (con possibili refluenze in chiave di natura disciplinare); la cattiva gestione di un *procedimento* potrebbe comportare importanti ricadute in chiave di responsabilità, sia amministrativa che eventualmente penale.

Fatte queste premesse di ordine generale, per ciò che specificamente attiene ad ATM SpA Trapani, si riportano di seguito le *Aree Gestionali* a maggiore rischio di illiceità di rilevanza penale (in una delle variegate qualificazioni giuridiche ipotizzate dal Decreto 231 e dal Sistema Anticorruzione), con relativa indicazione dei Regolamenti e delle Procedure applicati dalla Società:

❒ *ACQUISTI DI BENI E SERVIZI*

Per questa tipologia di processi organizzativi, il T.U. delle Società Partecipate di cui al D.Lgs. 19 agosto 2016 n. 175 dispone espressamente, all'art. 16 *(società in house*), comma 7: «*le società di cui al presente articolo sono tenute all'acquisto di lavori, beni e servizi secondo la disciplina di cui al decreto legislativo n. 50 del 2016*[14]».

Va da sé che che il Decreto Legislativo 18 aprile 2016, n. 50 – v. il Codice degli Appalti - è stato abrogato dal 1° luglio 2023, e da questo momento è entrato in vigore il Decreto legislativo 31 marzo 2023 n. 36 (*Codice dei contratti pubblici in attuazione dell'art. 1 della legge 21 giugno 2022 n. 78, recante delega al Governo in materia di contratti pubblici*)

ATM SpA Trapani rispetta pedissequamento il predetto nuovo sistema normativo.

❒ ASSUNZIONI, PROMOZIONI E CONCORSI INTERNI

In relazione a quest'area gestionale, ATM ha approvato (con Determina 281/2019) il *Regolamento per la progressione di carriera e le assunzioni del personale di ATM SpA Trapani.*

❒ AREA FINANZA E CONTABILITÀ

Avuto specifico riguardo a questa area, ATM ha approvato:

- La *Procedura gestione flussi finanziari* (Determina 449/2017);
- Le *Procedure operative ufficio amministrativo e contabile* (Delibera di Cda 15/03/2022 e Determina n. 116 del 16/03/2022);

Sono stati, poi, *esternalizzati e regolamentati* tramite appositi contratti i seguenti servizi:

- *Contratto per il servizio di gestione moneta metallica* euro, stipulato con ditta esterna, avente ad oggetto il "ritiro e la contazione della moneta metallica con servizio di smaltimento";
- *Contratti per la vendita dei titoli di viaggio* stipulati con circa 80 ricevitorie della città di Trapani;
- *Contratto per la distribuzione dei titoli di viaggio di ATM* con una Agenzia di Recapito

[14] Codice dei Contratti Pubblici

esterna;

- *Contratto per la distribuzione di titoli di sosta dematerializzati per il pagamento della sosta a raso dei veicoli all'interno delle strisce blu del Comune di Trapani,* mediante apposita Piattaforma, stipulato con ditta esterna;

- *Contratto di convenzione per la gestione del servizio di pagamento delle tariffe di sosta nel Comune di Trapani*, stipulato con ditta esterna;
- *Contratto per assistenza e manutenzione del sito istituzionale*, stipulato con ditta esterna.

Sono state, altresì, affidate a professionisti esterni – tramite sistema di selezione ad evidenza pubblicistica - alcune funzioni, come quelle di:

- ✓ D.P.O. (Data Protection Officer) e R.P.D. (Responsabile della Protezione Dati);
- ✓ R.S.P.P. (Responsabile Servizio Prevenzione e protezione);
- ✓ Medico competente;
- ✓ Professionistra per area contabile e amministrativa;
- ✓ Consulente del Lavoro.

Va da sé che la concreta esecuzione ed implementazione dei succitati Regolamenti, Procedure e Contratti, potrebbe essere soggetta a deviazioni di tipo illecito, dal che deriva la necessità che la stessa esecuzione/implementazione sia costantemente aderente ai Protocolli Generali e Protocolli Speciali (di cui *infra*), nonché sottoposta al costante monitoraggio ad opera dell'OdV e degli Organi di Controllo societario (eventualmente anche tramite audit a campione).

Rimane, altresì, ferma la necessità - già preannunciata nella succitata Relazione al Bilancio di previsione aziendale 2022/2024 - che siano colmate le lacune gestionali riguardanti la corretta suddivisione dei compiti nell'ambito degli iter procedimentali seguiti dai singoli uffici e funzioni di riferimento.

Opportuna, a quest'ultimo riguardo, la redazione/implementazione di una una *micro struttura aziendale.*

2.4. Sintesi magnitudo rischi da *reati presupposti* 231

Fermo restando che la specifica analisi e valutazione del rischio di verificazione di *tutti* i reati presupposti è stata effettuata a parte – analiticamente - utilizzando i criteri della succitata UNI ISO 31000:2018 in **Allegato 3**, si riportano di seguito le tabelle di sintesi, con i relativi risultati della "famiglia delittuosa" di appartenenza.

Si segnala che sono stati inseriti nelle predette tabelle di sintesi esclusivamente i *reati attinenti*, rimanendo i *reati non attinenti* analiticamente descritti nel succitato Allegato 1.

AREA REATI CONTRO LA PUBBLICA AMMINISTRAZIONE
Reati attinenti

CODICE PENALE	**LIVELLO RISCHIO**

316 bis - malversazione di erogazioni pubbliche	RILEVANTE
316 ter - indebita percezione di erogazioni pubbbliche	RILEVANTE
317 – concussione	CRITICO
318 - corruzione per un atto d'ufficio	CRITICO
319 - corruzione per un atto contrario ai doveri di ufficio	CRITICO
319 ter - corruzione in atti giudiziari	CRITICO
319 quater – induzione indebita a dare o promettere utilità	CRITICO
322 - istigazione alla corruzione	CRITICO
322 bis - 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 ……..	MEDIO BASSO
346 bis – traffico di influenze illecite	RILEVANTE
353 – turbata libertà d'incanto	RILEVANTE
353 bis – turbata libertà del procedimento di scelta del contraente	RILEVANTE
356 – frode nelle pubbliche forniture	RILEVANTE

AREA REATI CONTRO IL PATRIMONIO DELLA PUBBLICA AMMINISTRAZIONE
Reati attinenti

CODICE PENALE	LIVELLO RISCHIO
640, comma 2, n. 1 - truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee	RILEVANTE
640 bis - truffa aggravata per il conseguimento di erogazioni pubbliche	RILEVANTE
REATI PRESUPPOSTI SPECIALI	
314 - peculato	RILEVANTE
314 bis - Indebita destinazione di denaro o cose mobili	RILEVANTE
316 - peculato mediante profitto dell'errore altrui	RILEVANTE

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

CODICE PENALE	LIVELLO RISCHIO
464 - Uso di valori di bollo contraffatti o alterati (reato contro la fede pubblica presupposto dall'art. 25 bis D.Lgs. 231/2001)	MEDIO-BASSO
416 - associazione per delinquere	RILEVANTE
416 bis – concorso esterno in associazione a delinquere di stampo mafioso	RILEVANTE
416 ter - Scambio elettorale politico mafioso	RILEVANTE

AREA FINANZA E CONTABILITÀ
Reati attinenti

	LIVELLO RISCHIO
2621 c.c. - False comunicazioni sociali	RILEVANTE
2625 c.c. - Impedito controllo	CRITICO
2627 c.c. - Illegale ripartizione utili e riserve	MEDIO-BASSO
2635 c.c. - Corruzione tra privati	RILEVANTE
2638 c.c. - Ostacolo all'eserc. delle funzioni delle autorità pubbliche di vigilanza	CRITICO
648 c.p. – Ricettazione	RILEVANTE
648 bis c.p. - Riciclaggio	RILEVANTE
648 ter c.p. - Impiego di denaro, beni o utilità di provenienza illecita	RILEVANTE
648 ter 1 c.p. – Autoriciclaggio	RILEVANTE
Indebito utilizzo … - art. 493 ter c.p.	MEDIO-BASSO

Reati Tributari ex D.Lgs. 74/2000 aggiornati/modificati al D.L. 124/2019 (conv. in L.157/2019) al D.lgs. 87/2024 e al D.lsg. 173/2024	
art. 2 - Dichiarazione fraudolenta mediante uso di fatture	RILEVANTE
art. 3 - Dichiarazione fraudolenta mediante altri artifici	RILEVANTE
art. 8 - Emissione di fatture o altri documenti per operazioni inesistenti	RILEVANTE
art. 10 - Occultamento o distruzione di documenti contabili	RILEVANTE
art 10 quater – Indebita compensazione	RILEVANTE
Art. 11 - Sottrazione fraudolenta al pagamento di imposte	RILEVANTE

AREA RISORSE UMANE
Reati attinenti

CODICE PENALE

	LIVELLO RISCHIO
377 bis - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria	RILEVANTE
603 bis c.p. - D.Lgs. 286/998 (Intermediazione illecita/sfruttamento del lavoro/immigraz. clandestine)	MEDIO BASSO
604 bis - Propaganda e istigazione razziale terzi il cui soggiorno è irregolare	RILEVANTE

AREA GESTIONE RISORSE INFORMATICHE
Reati attinenti e parzialmente attinenti

	LIVELLO RISCHIO
635 bis c.p. - Danneggiamento di informazioni, dati e programmi informatici	MEDIO-BASSO
635 ter c.p. - Danneggiamento di informazioni, dati e programmi ….	RILEVANTE
635 quater c.p. - Danneggiamento di sistemi informatici o telematici	MEDIO-BASSO
615 ter c.p. - Accesso abusivo ad un sistema informatico o telematico	RILEVANTE

615 quater c.p. - Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire od interrompere comunicazioni informatiche o telematiche	RILEVANTE
617 quater c.p. - Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.	TRASCURABILE
Art. 171 L. 633/1944 - Diffusione, riproduzione e messa in commercio …..	MEDIO-BASSO
Art. 171 bis L. 633/1944 - Duplicazione, vendita, distribuzione ….	MEDIO-BASSO
Art. 171 ter L. 633/1944 - Duplicazione, riproduzione e diffusione …..	MEDIO-BASSO

AREA SICUREZZA LAVORO
Reati attinenti

ARTICOLO C.P.	LIVELLO RISCHIO
589 - Omicidio colposo	RILEVANTE
590 – Lesioni Colpose	RILEVANTE

REATI AMBIENTALI
Reati Attinenti

256 D.Lgs. 152/2006 - attività di gestione di rifiuti non autorizzata	RILEVANTE
258 D.Lgs. 152/2006 - violazione degli obblighi di comunicazione, …	RILEVANTE
260 bis D.Lgs. 152/2006 - sistema informatico di controllo della tracciabilità	RILEVANTE
452 bis c.p. - inquinamento ambientale	RILEVANTE
452 quinquies c.p. - delitti colposi contro l'ambiente	RILEVANTE

3. GESTIONE DEI RISCHI: PROTOCOLLI E SISTEMI DI CONTROLLO

Si è più volte ricordato che, nello specifico ambito di un Modello 231, per protocollo[15] 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:

- i **Protocolli Generali**, valevoli per tutte le ipotesi di "reato presupposto" e tutte le azioni aziendali, in qualsivoglia area, processo, procedimento o funzione.

[15] 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 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).

3.1. 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 potrà essere meglio assicurata anche tramite l'utilizzo di sistemi informatici in grado di gestire l'operazione consentendo il rispetto dei requisiti sopra descritti.

❒ I controlli effettuati devono essere 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).

Tale principio è, peraltro, espressamente richiesto dall'art. 9 (*Trasparenza e tracciabilità*) del D.P.R. 16 aprile 2013 n. 62 (*Regolamento recante codice di comportamento dei dipendenti pubblici*, formalmente adottato da ATM): «1. Il dipendente assicura l'adempimento degli obblighi di trasparenza previsti in capo alle pubbliche amministrazioni secondo le disposizioni normative vigenti, prestando la massima collaborazione nell'elaborazione, reperimento e trasmissione dei dati sottoposti all'obbligo di pubblicazione sul sito istituzionale. 2. La tracciabilità dei processi decisionali adottati dai dipendenti deve essere, in tutti i casi, garantita attraverso un adeguato supporto documentale, che consenta in ogni momento la replicabilità».

Da ricordare, al riguardo, che la tracciabilità, la separazione dei ruoli ed una corretta assegnazione dei poteri costituiscono dei requisiti fondamentali 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 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.

Ove, per ragioni di limitatezza delle risorse umane, tale principio non possa essere integralmente rispettato, sarà opportuno prevedere *protocolli aggiuntivi di rimedio* (v., a titolo esemplificativo e non esaustivo: elevare il principio di formalizzazione degli atti, o prevedere degli specifici audit a campione, o rafforzare il sistema dei controlli estrinseci ed ex post).

I tre suddetti principi di *robustezza* devono essere integrati dagli ulteriori seguenti principi (che, 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 eventuali 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 ad ATM SpA Trapani, 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.

❒ Corretta e diligente applicazione de:

- **La normativa di riferimento**, atteso 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 ATM SpA Trapani,** che ovviamente rappresenta il nuovo quadro di riferimento organizzativo della Società.
- **Il Codice Etico e di Comportamento** adottato da ATM SpA Trapani (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**, organo obbligatorio ai fini della stessa operatività e validità giuridica del Modello 231 adottato dalla Società.
- **I Regolamenti Aziendali, le Procedure Aziendali, gli Ordini di Servizio, le Norme e le Circolari Aziendali**, quali linee direttrici cui attenersi nello svolgimento dell'attività e delle mansioni e compiti attribuiti a titolo individuale.

❒ 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, con 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

È opportuno sia 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 dovrebbe 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 chiarito nella Parte I, il dipendente/collaboratore/*interessato tout court* 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.

La tutela delle segnalazioni in oggetto si inserisce nella nuova disciplina del *whistleblowing* di cui al 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*).

In tema, considerato che la Società si è perfettamente adeguata alla nuova disciplina di legge, attraverso l'acquisto di una apposita piattaforma informatica, i gestori del "*canale interno delle segnalazioni*" – v., in via congiunta, l'OdV 231 e il RPCT - dovranno assicurare la piena aderenza alla procedura di legge nonché la tutela del segnalante, sia in relazione alla sua riservatezza, che in ordine a possibili azioni ritorsive nei suoi confronti.

In caso di sospetta presenza di "attività ritorsiva", lo stesso *Gestore del canale interno* - o eventualmente anche l'Organismo di Vigilanza 231 in via individuale ove il RPCT non intervenga - svolte le opportune verifiche del caso, è tenuto a seguire lo svolgimento della vicenda e, al suo esito, a stilare un motivato report (da inviare, nei limiti e condizioni sopra ricordati, ai summenzionati organismi aziendali) nel quale dovrà essere rappresentato e chiarito:

a) non essere stato realmente effettuato alcun atto di discriminazione/ritorsione nei confronti del segnalante;

b) essere stato effettivamente operato un atto di discriminazione/ritorsione che tuttavia è stato successivamente "riparato/revocato";

c) essere ancora persistente un atto di discriminazione e/o ritorsione.

Nel caso di cui al punto sub c), l'Organismo di Vigilanza potrà/ dovrà inviare gli atti alla Procura della Repubblica per le eventuali valutazioni e determinazioni del caso.

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

3.2. Protocolli Speciali

I Protocolli Speciali presuppongono la rigorosa applicazione dei Protocolli Generali.

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

In considerazione del fatto che i protocolli sono disegnati sulla logica dei processi, nella maggior parte dei casi essi attraversano l'organizzazione orizzontalmente; il che comporta il coinvolgimento di funzioni appartenenti ad entrambe le Aree.

Tutto ciò determina l'obbligo per tutti i dipendenti/collaboratori di ATM SpA Trapani di conoscerli ed applicarli pedissequamente.

Area reati contro la Pubblica Amministrazione e il suo Patrimonio

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

A) Gestione dei rapporti con funzionari pubblici
B) Gestione dei controlli delle autorità pubbliche
C) Gestione gare e contratti pubblici - procedimenti di acquisti e forniture
D) Gestione di eventuali finanziamenti e contributi extra rispetto a quelli ordinari
E) Gestione del precontenzioso e del contenzioso
F) Gestione delle attività strumentali alla commissione dei reati contro la P.A.:
    1. risorse finanziarie
    2. selezione/assunzione del personale e progressione di carriera
    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

G) Gestione beni pubblici altrui

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 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.

C) Gestione procedimenti di acquisti e forniture

- Rispettare pedissequante i regolamenti e le procedure di acquisto di beni e servizi adottate da ATM SpA Trapani, nonché quanto prescritto dal Codice dei Contratti Pubblici ex

Decreto legislativo 31 marzo 2023 n. 36 in attuazione dell'art. 1 della Legge 21 giugno 2022, n. 78, recante delega al Governo in materia di contratti pubblici;

- Verificare l'esistenza di eventuali conflitti d'interesse e rimuoverne le cause;
- Consentire la tracciabilità e verificabilità ex post delle azioni e degli atti posti in essere 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.

D) Gestione di eventuali finanziamenti e/o contributi extra

Fermo restando che i contributi concessi dal Comune di Trapani e dalla Regione Sicilia sono ordinari e senza vincolo di destinazione, ove ATM volesse accedere ad ulteriori e diversi contributi/finanziamenti vigono i seguenti **obblighi**:

- rispettare le procedure di rendicontazione previste dall'Ente erogante;
- assicurare la piena tracciabilità dei flussi documentali e finanziari e di rispetto delle procedure informatiche e di controllo manuale adottate dalla Società;
- effettuare verifiche di congruenza degli stati di avanzamento dell'eventuale progetto con il piano finanziario definito dal provvedimento di concessione;
- effettuare verifiche contabili sulla documentazione utilizzata per l'ottenimento del contributo;
- effettuare verifiche al fine di riscontrare la veridicità delle operazioni/transazioni documentate.

Inoltre, vigerebbero i seguenti **divieti**:

- destinare somme ricevute per scopi diversi da quelli cui erano destinati.
- presentare dichiarazioni non veritiere a organismi pubblici nazionali o comunitari, al fine di conseguire erogazioni, contributi o finanziamenti;
- attestare il possesso di requisiti inesistenti stabiliti dalla legge o da provvedimenti amministrativi al fine di chiedere e ottenere contributi/finanziamenti pubblici (comunitari e nazionali);
- porre in essere qualsiasi tipo di condotta idonea a indurre in errore Pubbliche Amministrazioni statali o comunitarie.

E) Gestione del precontenzioso e del contenzioso

Tra le situazioni di frequente verificazione societaria, vi è quella dei *precontenziosi amministrativi*, ovvero di quelle possibili e variegate 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[16].

[16] 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.

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 in giornata 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 o Amministrativa dovrà:

- protocollare l'atto di citazione pervenuto alla società tramite l'ufficiale giudiziario o a mezzo posta;
- 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 il Organo Amministrativo sullo status dei contenziosi e sulla loro eventuale chiusura.

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.

F) 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, a parte la stretta osservanza della *Procedura Gestione Flussi Finanziari* e delle *Procedure Operative Ufficio Amministrativo e Contaboli* adottate da ATM, 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/assunzione del personale e progressione di carriera

L'assunzione del "personale", o la sua progressione in carriera potrebbe concretamente celare accordi o promesse di tipo corruttivo.

Il processo - a parte la pedissequa osservanza del *Regolamento per la progressione di carriera e le assunzioni del personale* adottato da ATM - 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;*

- corrispondenza delle attività di selezione alle politiche aziendali (se presenti) e alle caratteristiche dei ruoli da ricoprire, nel rispetto della pari opportunità uomo-donna nel lavoro;
- preventivo accertamento e valutazione dei rapporti, diretti o indiretti, tra il candidato e la Società;
- 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 dell'affidabilità personale, morale e professionale, anche avvalendosi di certificazioni rilasciate dall'Autorità Giudiziaria Ordinaria o dalla Prefettura. A tal proposito i lavoratori al momento dell'avvio del rapporto di lavoro con la Società devono rilasciare *autodichiarazioni* attestanti l'assenza/presenza di condanne penale e di carichi pendenti con impegno ad informare la Società di eventuali fatti intervenuti;
- archiviazione della documentazione di riferimento;
- 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.

- Dovrà essere garantita l'acquisizione dei dati personali 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 economicità e 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;
- il sostenimento di spese di rappresentanza deve soddisfare il concetto di "opportunità" della spesa;
- devono essere previsti formali controlli circa l'inerenza e la documentazione delle spese per le quali si richiede il rimborso.

G) Gestione beni pubblici altrui

Come chiarito nella Parte I, la Società - in ossequio al principio di integrazione del Modello 231 con la normativa anticorruzione - ha spontaneamente inserito nell'area dei *reati presupposti speciali* (in particolare, in quella dei "*reati contro il patrimonio in danno*

della pubblica amministrazione") i delitti di peculato *ex* artt. 314 e 316 c.p., rispettivamente delitto presupposto speciale richiamato dall'art. 1, comma 75, lett. c) della Legge 190/2012 e reato ad esso collaterale.

I due richiamati delitti rappresentano una sorta di appropriazione indebita "speciale" nei confronti dei beni della Pubblica Amministrazione.

Il rischio è - soprattutto - in relazione ai possibili beni delle pubbliche amministrazioni con le quali la Società intrattiene rapporti.

Proprio al fine di evitare questo tipo di appropriazione o distrazione, la Società dovrà accuratamente discernere i *propri* beni aziendali da quelli dei terzi – soggetti pubblici - eventualmente ricevuti a titolo di comodato d'uso per un periodo di tempo limitato o per specifiche ed indicate ragioni e utilizzazioni.

Le prescrizioni protocollari minime - che hanno il precipuo obiettivo di evitare qualsiasi forma di confusione patrimoniale in tale senso - sono:

- redazione di un inventario di tutte le eventuali "cose mobili" (v. le uniche che, unitamente al "denaro", sono oggetto del delitto in esame) appartenenti agli enti pubblici o alle autorità istituzionali con cui ATM intrattiene rapporti;
- annotazione delle cose mobili appartenenti alla P.A. o ad enti pubblici in un apposito registro, con relativa descrizione del loro specifico uso e della relativa allocazione;
- individuazione di una persona che, all'interno della Società, sia nominata responsabile e custode dei beni mobili altrui;
- descrizione delle modalità d'uso dei beni mobili in oggetto;
- comunicazione a tutti i dipendenti degli specifici beni di proprietà della Società e di quelli invece appartenenti a soggetti pubblici;
- comunicazione a tutti i dipendenti dell'assoluto divieto di usare per ragioni personali i beni in oggetto;
- custodia e manutenzione dei beni in oggetto;
- divieto di qualsiasi forma di distrazione o distruzione dei beni in oggetto;
- comunicazione immediata all'Organismo di Vigilanza di eventuali inosservanze delle succitate prescrizioni.

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.

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:

- deve essere istituito un Albo Fornitori;
- deve essere prevista una procedura ad hoc di *qualificazione verifiche reputazionali e di qualità dei Fornitori*;
- 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 disciplinato da contratto scritto, nel quale sia chiaramente prestabilito il prezzo del bene o della prestazione o i criteri per determinarlo;
- i contratti di approvvigionamento di valore significativo devono essere sempre 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 o gli appaltatori/subappaltatori 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 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:
  - il monitoraggio di qualsiasi indice di alert, da qualsiasi parte provenga ed attraverso qualsiasi forma si presenti;
  - la valutazione di indici attestanti l'affidabilità personale e professionale del fornitore;
- la richiesta e valutazione di certificati penali (entro i limiti consentiti dal GDPR di cui al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016); deve essere richiesta un'autocertificazione dalla quale risulti l'indicazione nominativa del personale utilizzato nei lavori;
- deve essere richiesta 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;
- deve essere effettuato un costante controllo dei partner o subappaltatori, anche attraverso la valutazione di indici attestanti l'affidabilità personale e professionale da accertarsi in base alle modalità descritte nei precedenti punti;
- sono vietati i rapporti di lavoro o di partenariato 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;
- devono essere richiesti i documenti comprovanti l'iscrizione ad albi, ordini, elenchi, qualora l'iscrizione sia requisito necessario per lo svolgimento dell'attività;
- tutte le possibili "utilità" vanno equiparate ai "beni" dal punto di vista della loro gestione e tracciabilità.

Infine, **qualsiasi condotta genericamente anomala o sospetta** deve essere monitorata con attenzione, in primis dalla funzione Risorse Umane; considerato 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;
- i reati di razzismo e xenofobia richiamati dall'art. 25 terdecies.

Tali delitti, seppur non concretamente collegabili a specifici processi/mansioni della Società (e per tali ragioni sono stati prevalentemente considerati "non attinenti"), potranno risultare evincibili da condotte genericamente anomale, o da comportamenti inusuali, o da segnalazioni più o meno esplicite, o da indistinti elementi di sospetto.

Di tali possibili o eventuali anomalie dovrà essere sempre informato l'Organismo di Vigilanza.

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 c.p. (presupposti dall'art. 25 octies del Decreto 231) 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 il Socio Unico, con gli Organi di Controllo (Collegio Sindacale e Revisore Legale) e con l'Organismo di Vigilanza.

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 il Socio Unico, gli Organi di Controllo e l'Organismo di Vigilanza

- Deve essere garantito al Socio Unico, agli Organi di Controllo e all'Organismo di Vigilanza, 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:

- 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;
- l'utilizzo degli strumenti di pagamento diversi dal contante.

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

B.1 Gestione dei flussi monetari e finanziari in uscita

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*.

B.3 Gestione strumenti di pagamento diversi dal contante

In ATM gli strumenti di pagamento diversi dal contante sono soprattutto utilizzati ed accettati negli uffici aziendali che gestiscono gli abbonamenti (sia per il trasporto pubblico locale – TPL che per le cd. "strisce blu").

Posto che l'art. 493 ter c.p. intende elidere il rischio di possibili manipolazioni o falsificazioni dei pagamenti effettuati tramite POS - che, comunque, sono strumenti forniti ad ATM dal proprio Istituto di Credito - la Società dovrà porre particolare attenzione, (eventualmente attraverso apposita procedura) a:

- l'esatta individuazione (e registrazione) dei singoli dipendenti che gestiscono, giornalmente, le operazioni di pagamento tramite POS;
- la corretta archiviazione delle stesse operazioni;
- la tracciabilità (anche a posteriori) dei singoli pagamenti in corrispondenza agli specifici dipendenti che hanno effettuato l'operazione.

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" ATM 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 ATM 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

La fattispecie in esame risulta ricollegabile alla succitata 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/Dirigente che si occupa 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.

D) Propaganda e condotte a sfondo razzista

Come chiarito in sede di crime risk assessment, sebbene i *reati di razzismo e xenofobia* sono oggettivamente estranei all'attività di servizio pubblico svolta da ATM ed ai principi di rispetto della collettività perseguiti dalla stessa, si ritiene opportuno che la Società (allocata in zona geografica a discreta presenza di popolazione extracomunitaria) preveda possibili fenomeno di razzismo, soprattutto all'interno degli autobus di linea; il che potrebbe dare anche luogo a deprecabili episodi di rissa o di violenza fisica/verbale tra i passeggeri.

È, dunque, consigliabile che la Società predisponga delle apposite procedure di controllo e sanzionamento di tale possibile rischio, formando e responsabilizzando in tal senso gli operatori e gli addetti di esercizio, a cui potrebbero essere eventualmente conferiti specifici poteri di sanzionamento ed allontanamento degli utenti/passeggeri "colpevoli" delle suddette condotte.

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 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; attività affidata al DPO individuato nell'anno 2021 attraverso specifico e formalizzato incarico professionale.

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 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~~;~~
- 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 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 manutene reregolarmente 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

- 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) 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.

- Monitorare/controllare costantemente la presenza di eventuali prodotti dell'ingegno coperti dal diritto d'autore nelle aree di appartenenza aziendale (uffici, terminal, parcheggi multipiano e autobus).

Area Sicurezza Lavoratori

In ATM il rischio di consumazione dei delitti di *omicidio colposo* e *lesioni colpose* ex art. 25 septies del Decreto 231 è oggettivamente ben presidiato.

Cionostante, si tratta di un rischio che, seppur di non preoccupante probabilità, rimane di gravità "molto alta"; il che richiede un controllo ed un monitoraggio costante dei soggetti e delle azioni espressamente indicati nel D.Lgs. 81/2008 e nella correlata normativa di settore.

Di assoluta cogenza, pertanto, il **rispetto dei doveri e degli obblighi** espressamente previsti dal D.Lgs. 81/2008 in capo a:

- Il **Datore di Lavoro** e il **Dirigente**, sia in relazione alle misure generali di tutela ex art. 15 che agli obblighi ex art. 18 (tra cui, ad esempio, la riunione annuale ex art. 35 alla presenza del RSPP, del Medico Competente e del RLS);
- L'eventuale **Delegato alla sicurezza sui luoghi di lavoro** ex art. 16 (non designabile, in base al preciso divieto dell'art. 17, per la redazione del DVR ex art. 28 e per la designazione del RSPP), tenendo in debita considerazione che tale eventuale delega potrà essere efficace solo se, e nella misura in cui, rispetterà pedissequamente i requisiti di forma e di sostanza richiesti dallo stesso art. 16;
- Il **Medico Competente** ex art. 25;
- Il **Responsabile Servizio Prevenzione Protezione** (RSPP) ex art. 31;
- L'eventuale **Addetto al Servizio di Prevenzione e Protezione** ex art. 31;
- Il **Preposto** ex art. art. 19, i cui poteri-doveri sono stati ulteriormente dettagliati ed ampliati 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*).
- I **lavoratori** ex art. 20;
- Il **Rappresentante dei Lavoratori per la Sicurezza** (RLS) ex art. 2 lett. i).

Dal punto di vista delle **azioni -** che comunque sono analiticamente previste ed imposte dal D.Lgs. 81/2008 - rimane assolutamente fermo l'**obbligo** di:

✓ tenere costantemente aggiornato il Documento di Valutazione Rischi ex art. 28;

✓ applicare concretamente e senza soluzione di continuità i protocolli e le procedure previste nello stesso DVR;

✓ informare e formare costantemente i lavoratori sui rischi afferenti all'attivita lavorativa svolta;

✓ segnalare immediatamente al datore di lavoro e a chi di dovere (in ragione delle responsabilità attribuite) le deficienze dei mezzi o dei dispositivi di sicurezza antinfortunistica, nonché qualsiasi eventuale condizione di pericolo di cui si venga a conoscenza, adoperandosi anche direttamente, in caso di urgenza e nell'ambito delle proprie competenze e possibilità, per eliminare o ridurre le situazioni di pericolo grave e incombente, nonché per darne prontamente notizia ai responsabili competenti.

Area Reati Ambientali

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

A quest'ultimo riguardo, ed avuto specifico riguardo – ad esempio - alla *gestione dei rifiuti*, tutti i destinatari devono avere piena coscienza e consapevolezza che:

- la gestione dei rifiuti va considerata un'attività di pubblico interesse, appositamente disciplinata per assicurare un'elevata protezione dell'ambiente, anche attraverso un'azione di efficace e costante monitoraggio;
- 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,

In via generale, tutti i Destinatari del Modello sono, pertanto, tenuti a conoscere e rispettare le seguenti *prescrizioni generali*:

- considerare sempre prevalente la necessità di tutelare l'ambiente rispetto a qualsiasi considerazione economica;
- valutare gli effetti della propria condotta in relazione al rischio di danno all'ambiente;
- non adottare comportamenti imprudenti che potrebbero recare danno all'ambiente;
- 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;

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 predisponendo e controllando 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.

In tale contesto, la **Società dovrà assicurare**:

- la corretta informazione, ai Destinatari del MOGC, su tutto ciò che riguardi la materia ambientale presa legislativamente di mira dall'art. 25 undecies del D.Lgs. 231/2001 e dai i reati presupposti in esso richiamati;

- la costante individuazione di tutte le eventuali situazioni in cui potrebbero concretizzarsi le condotte delittuose e/o contravvenzionali richiamate dalla stessa legislazione;
- la previsione, ove necessario od opportuno, di eventuali "deleghe di funzioni" (da rilasciare rispettando i crismi formali e sostanziali dell'art. 16 D.Lgs. 81/2008);
- la costante vigilanza e controllo sui contratti stipulati dalla Società in materia di "gestione rifiuti";
- il costante controllo e monitoraggio di eventuali smaltimenti illeciti di rifiuti (in tutte le sedi aziendali e negli autobus in circolazione), o di omessa/carente tenuta dei registri F.I.R., o di qualunque situazione o azione aziendale che possa, anche indirettamente causare un danno all'ambiente;
- La predisposizione e diffusione di una o più specifica procedura aziendale finalizzata a dare istruzioni specifiche sul corretto smaltimento dei rifuti in tutte le aree aziendali, compresi gli autobus di linea.

4. L'ORGANISMO DI VIGILANZA 231 DI ATM SPA TRAPANI

Sulla base dei principi generali illustrati nella Parte I, Cap. 2, § 2.3., ATM ha provveduto a nominare l'Organismo di Vigilanza 231 a presidio del Modello di Organizzazione, Gestione e Controllo 231.

Si riporta di seguito lo **Statuto OdV di ATM** (il Regolamento OdV è stato regolarmente predisposto dall'OdV nell'ambito della sua autonomia di azione e di regolamentazione attività):

Articolo 1 - Scopo ed ambito di applicazione

1. È istituito presso ATM 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 ATM è, attualmente, a composizione monocratica.

2. La Società può, ove lo ritenga, allargare lo stesso Organismo a composizione plurisoggettiva.

Articolo 3 - Requisiti di professionalità e di onorabilità

1. L'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*, fino alla nuova nomina dei suoi componenti.

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 e agli altri membri dell'OdV tramite comunicazione scritta); c) la revoca per giusta causa da parte dell'Organo Amministrativo a maggioranza assoluta.

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 (desumibile, ad esempio, dalla mancanza di partecipazione alle riunioni dell'Organismo di Vigilanza per almeno 9 mesi consecutivi ovvero per almeno tre incontri 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 dell'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 loro funzioni con la diligenza richiesta dalla natura dell'incarico e dalle loro 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 loro 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 3 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 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:

a) 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;

b) verificare il mantenimento nel tempo dei requisiti di solidità e funzionalità del Modello 231;

c) 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;

d) 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;

e) 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;

f) segnalare all'Organo Amministrativo eventuali carenze/inadeguatezze nella prevenzione dei reati, o violazioni del MOGC e del Codice Etico;

g) 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;

h) 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;

i) riferire periodicamente all'Organo Amministrativo circa lo stato di attuazione e di operatività del Modello 231;

j) 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;

k) segnalare all'Organo Amministrativo fatti o condotte di rilevanza disciplinare;

l) 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);

m) 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.

n) 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;

o) 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 perl'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 sono quelli provenienti: A) dall'Organismo di Vigilanza nei confronti dell'Organo Amministrativo; B) dalla Società nei confronti dell'Organismo di Vigilanza.

2. I flussi informativi sub A) sono: a) di natura continuativa, in occasione di eventuali invii di Note o Verbali OdV al CdA, illustrativi di situazioni di criticità o di necessità di intervento correttivo/migliorativo, 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.

3. I flussi informativi sub B) sono quelli che consentono il corretto espletamento della funzione di vigilanza del Modello 231 all'OdV. Gli stessi rappresentano un'asse portante del sistema di controllo societario e una componente essenziale del Modello 231 e dell'attività di monitoraggio dello stesso OdV, nonché 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».

4. Sulla base di quanto confermato al punto precedente, 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.

5. 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.

6. 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 (Verbali, Delibere, Disposizioni di Servizio di particolare rilevanza, atti analoghi; 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; 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 degli stess procedimenti; gli eventi a carattere straordinario e/o eccezionale; 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.

7. In presenza di alcuna delle segnalazioni in materia di 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 siano 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.

8. 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.

9. 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.

10. L'Organismo di Vigilanza ha il diritto/potere di ricevere le segnalazioni da whistleblowing presso un indirizzo e mail estraneo a quello aziendale, che dovrà essere debitamente comunicato da tutti i Destinatari del MOGC.

5. IL CODICE ETICO E DI COMPORTAMENTO DI ATM SPA TRAPANI

Come chiarito nella Parte I, Cap. 2, § 2.6., il Codice Etico e/o Codice di Comportamento rappresenta un elemento essenziale di un Modello di Organizzazione, Gestione e Controllo 231.

Al fine di evitare possibili ridondanze o equivoci/fraintendimenti di natura applicativa, nella presente versione aggiornata del Modello: il precedente *Codice Etico* (approvato con

Determinazione 399 del 9 giugno 2017) e il precedente *Codice di Comportamento* ex D.P.R. 62/2013 (approvato con Delibera di CdA del del 23.3.2021 e successiva Determina n. 147/2021), sono stati unificati in un unico ***Codice Etico e di Comportamento***.

Il succitato *Codice Etico e di Comportamento* rappresenta **parte integrante del Modello 231 (Allegato 1).**

Qualunque violazione del suddetto Codice è, pertanto, idonea ad integrare violazione del Modello 231 con conseguente sottoposizione alle sanzioni di cui al *Sistema Disciplinare 231* (parte integrante del presente Modello 231, come Allegato 2).

Ne consegue la sottoposizione dello stesso Codice al monitoraggio e raggio di azione dell'Organismo di Vigilanza 231.

6. IL SISTEMA DISCIPLINARE 231 DI ATM SPA TRAPANI

Come chiarito nella Parte I, Cap. 2, § 2.4., il *Sistema Disciplinare 231* rappresenta un elemento essenziale e imprescindibile di un Modello di Organizzazione, Gestione e Controllo 231.

ATM ha già adottato, con Determina n. 400 del 9 giugno 2017, il *Sistema Disciplinare Sanzionatorio* aderente al R.D. 8 gennaio 1931 n. 148 (*Coordinamento delle norme sulla disciplina giuridica dei rapporti collettivi del lavoro con quelle sul trattamento giuridico-economico del personale delle ferrovie, tranvie e linee di navigazione interna in regime di concessione*).

Il predetto *Sistema Disciplinare Sanzionatorio* rimane pienamente vigente ed operativo per qualsiasi violazione che non sia strettamente derivante dalla violazione del presente Modello 231 e/o dei relativi documenti integrativi (v. Codice Etico e di Comportamento).

Con l'approvazione, invece, del presente Modello 231, il *Sistema Disciplinare 231* avente specificamente ad oggetto la sua eventuale violazione sarà interamente regolato da quello riportato nell'**Allegato 2.**

Sarà cura della Società di revisionare il succitato *Sistema Disciplinare Sanzionatorio ex R.D. 148/1931* estrapolando dallo stesso le parti afferenti alle violazioni del presente Modello 231, che a far data dalla data di approvazione dello stesso - 29 aprile 2022 - saranno regolate esclusivamente dal *Sistema Disciplinare 231* di cui al succitato Allegato 2.

7. 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 ATM SpA Trapani, ed a prescindere cioè dalle specifiche peculiarità delle singole categorie, possono definirsi Destinatari del Modello 231 adottato dalla a Società i seguenti soggetti:

- i componenti dell'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);

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[17].

Escluderli dalla categoria dei "destinatari" significherebbe introdurre nel sistema una forma di impunità priva di valida giustificazione logica e comunque nettamente anticostituzionale.

8. 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 il *Modello di Organizzazione, Gestione e Controllo* 231.

Una volta approvati, rappresentano obbligatoria attività di manutenzione, del Modello di Organizzazione, Gestione e Controllo e del Codice Etico, le attività di:

- *Verifica*;

[17] 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.

- *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" ATM Spa Trapani.

Il MOGC e i richiamati Codice Etico e Codice di Comportamento dovranno essere tenuti – 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.