siciltecnoplus
impianti tecnologici

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ex D.Lgs. 231/2001 esteso ai reati anticorruzione

Vers.5

31 Dicembre 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 - da cui è scaturita anche l'imposizione di un attento controllo della legalità e della prevenzione anticorruzione - avviato su scala internazionale a partire dagli anni '90.

Si inseriscono in tale processo:

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

Anche in Italia, la decisione di adottare la Legge Delega n. 300/2000[3] - con la conseguente emanazione del Decreto Legislativo 231/2001 – è scaturita dalla considerazione che, mai come nel momento attuale, si assiste ad una crescente ed inammissibile proliferazione di disfunzioni, danni e condotte illecite, derivanti dalla gestione di strutture societarie, anche e soprattutto a carattere privatistico.

Da qui la presa di coscienza: - che il *rischio di impresa* debba includere nel suo nucleo portante anche il cd. *rischio da illegalità*; - che la previsione di tale rischio (storicamente ricadente sulla collettività a causa del rigido principio di responsabilità penale personale in capo alla sola persona fisica) debba essere addossata a chi, della personalità giuridica, ne usufruisce in pieno di tutti i benefici.

Ciò premesso: il Decreto Legislativo 8 giugno 2001, n. 231, recante "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle Società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*", ha introdotto - per la prima volta nell'ordinamento italiano - la responsabilità degli enti.

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

La riprova testuale è fornita dallo stesso Decreto 231, interamente strutturato su principi, nozioni e disciplina, di diritto penale e diritto processuale penale: i *reati presupposti* richiamati dagli articoli 24 e ss.; la nozione di "*commissione del reato*" (art. 5); l'applicabilità all'ente dell'*amnistia* (art. 8);

---

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

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

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

l'applicazione delle disposizioni del codice di procedura penale (art. 34); l'estensione all'ente delle disposizioni processuali relative all'imputato (art. 35); la valutazione della responsabilità dell'ente nell'ambito di un processo penale e da parte di un Giudice Penale (art. 36); l'improcedibilità per le stesse cause di improcedibilità dell'azione penale (art. 37); l'applicazione delle misure cautelari in base alle norme processuali penali (art. 45); l'annotazione dell'illecito nel registro delle notizie di reato di cui all'art. 335 c.p.p. (art. 55); la scansione degli atti e delle fasi processuali in base al codice di procedura penale (artt. 56-81); i riti alternativi strettamente penalistici come il *patteggiamento ex* art. 444 c.p.p., il *giudizio abbreviato ex* 438 c.p.p. e il *procedimento per decreto ex* art. 459 c.p.p. (artt. 62, 63 e 64); etc. etc.

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

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

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

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

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

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

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

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

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

L'unico limite al principio di *autonomia della responsabilità dell'ente* – che, però, si è detto rimanere ferma anche nel caso in cui l'autore del reato non è stato identificato o non sia imputabile – è l'effettiva «presenza di un reato commesso nell'interesse o a vantaggio dell'ente medesimo » (Cass. pen., sez. V, 4 aprile 2013, n. 20060).

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

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

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

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

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

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

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

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

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

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

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

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

attivato un reale ed efficiente meccanismo di organizzazione e di controllo di tutte le possibili condotte illecite perpetrabili all'interno di uno dei tanti gangli della propria attività imprenditoriale.

Solo tale prova potrà consentire di "difendersi" assumendo che il reato è stato commesso non a causa di una carenza di organizzazione ma in conseguenza di una elusione fraudolenta del Modello di Organizzazione, Gestione e Controllo (art. 6, co.1, lett. c) del D.Lgs. 231/2001). Di fatto, è la stessa filosofia e politica legislativa "di tipo premiale" portata avanti dal D.Lgs. 3 agosto 2009 n. 106 (*Disposizioni integrative e correttive* al D.Lgs. 9 aprile 2008 n. 81 in materia di *tutela della salute e della sicurezza nei luoghi di lavoro*), attraverso l'introduzione del comma 3 nell'art. 16 del D.Lgs. 81/2008[6].

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

1.2. 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 plurimi interventi legislativi di natura integrativa e/o correttiva[7] - sono quelle espressamente indicate agli artt. 24, 24-*bis*, 24-*ter,* 25, 25-*bis*, 25 *bis.*1, 25 ter, 25-*quarter*, 25-*quarter*.1, 25-*quinquies*, 25-*sexies*, 25-*septies*, 25-*octies*, *25 octies.1,* 25-*novies*, 25-*decies*, 25-*undecies*, 25-*duodecies, 25-terdecies,* 25-*quaterdecies,* 25-*quinquiesdecies, 25- sexiesdecies,* 25-*septiesdecies*, 25-undevicies, 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 sanzionatrice diretta*, come nel caso dell'ultima 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*).

---

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

7 V., in via esemplificativa, le principali modifiche dell'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 dallo 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. 25; 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; la Legge 9.6.2025, n.80 con la quale è stata introdotta una fattispecie di reato presupposto nell'art. 25 quater; Legge n. 82 del 6 giugno 2025 che introduce l'art. 25 undevicies in materia di maltrattamento animali; il D.L. 8.08.2025 n. 116, convertito in Legge 3 ottobre 2025, in materia di reati ambientali.

C) una *correzione di natura indiretta*, come nel caso della modifica "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. 2 L. 898 del 23 dicembre 1986

❒ **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.);

✓ Estorsione (art. 629, co. 3, 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.);

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

✓ Art. 1 c.11 D.L. n. 105 del 21 ottobre 2019

❒ **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 D.Lgs. 231/01 se "il fatto offende gli interessi finanziari dell'Unione europea"]

✓ Peculato mediante profitto dell'errore altrui (art. 316) [reato rilevante ex D.Lgs. 231/01 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 c.p.);

✓ Corruzione in atti giudiziari (art. 319-ter c.p.);

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

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

- ✓ Pene per il corruttore (art. 321 c.p.);
- ✓ Istigazione alla corruzione (art. 322 c.p.);
- ✓ Peculato, indebita destinazione di denaro o cose mobili, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.);
- ✓ Traffico di influenze illecite (art. 346-bis c.p.).

❒ **Art. 25-*bis* (*Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento*):**

- ✓ 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.);
- ✓ 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 D.Lgs. 24 febbraio 1998 n. 58 (*Testo unico delle disposizioni in materia di intermediazione finanziaria (TUF), ai sensi degli articoli 8 e 21 della legge 6 febbraio 1996, n. 52* - Ultimo aggiornamento all'atto pubblicato il 20/03/2025):

- ✓ Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate (art. 184 TUF);
- ✓ Manipolazione del mercato (art. 185 TUF)

❒ **Art. 25-septies (Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro).**

Entrambi i richiamati *reati presupposti* presuppongono la violazione della normativa sulla sicurezza sul lavoro di cui ai D.Lgs. 9 aprile 2008 n. 81/D.Lgs. 3 agosto 2009 n. 106, e sono i seguenti:

- ✓ Omicidio colposo (art. 589 c.p.);
- ✓ Lesioni colpose (art. 590 c.p.).

❒ **Art. 25-*octies* (*Ricettazione, Riciclaggio e impiego del denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*):**

✓ 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)*** *– Articolo modificato da D.L. 10 agosto 2023 n. 105 coordinato con la Legge di conversione n. 137 del 9 ottobre 2023:*

✓ 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 D.Lgs. 231/01 "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 seguenti reati sono quelli della Legge 22 aprile 1941 n. 633, come modificati dalla Legge 14 novembre 2024 n. 166:

✓ Art. 171 L. n. 633/1941

✓ Art. 171-bis L. n. 633/1941

✓ Art. 171-ter L. n. 633/1941

✓ Art. 171-septies L. n. 633/1941

✓ Art. 171-octies L. n. 633/1941

❒ 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.);

✓ Impedimento del controllo (art. 452 septies c.p.);

✓ Circostanze aggravanti (art. 452-octies c.p.);

✓ Omessa bonifica (art. 452 terdecies c.p.);

✓ Attività organizzate per il traffico illecito dei rifiuti (**a**rt. 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.);

✓ Sanzioni penali (art. 137 D.Lgs. n. 152/2006 - Codice Ambiente);

✓ Abbandono di rifiuti non pericolosi (art. 255 bis Cod. Amb.);

✓ Abbandono di rifiuti non pericolosi in casi particolari (art. 255 ter Cod. Amb.);

- ✓ Attività di gestione di rifiuti non autorizzata (art. 256 Cod. Amb.);
- ✓ Combustione illecita di rifiuti (art. 256 bis Cod. Amb);
- ✓ Bonifica dei siti (art. 257 Cod. Amb.);
- ✓ Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (art. 258 Cod. Amb.);
- ✓ Traffico illecito di rifiuti (art. 259 Cod. Amb.);
- ✓ Sistema informatico di controllo della tracciabilità di rifiuti (art. 260 bis Cod. Amb.);
- ✓ Sanzioni (art. 279 Cod. Amb);
- ✓ Art. 8 D.Lgs. n. 202/2007;
- ✓ Art. 9 D.Lgs. n. 202/2007;
- ✓ Art. 3 L. n. 549/93;
- ✓ 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 Legge 150/1992 n. 150 (artt. 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 491-bis, 492, 493);
- ✓ Reati previsti dalla Legge 28 dicembre 1993, n. 549 (Misure a tutela dell'ozono stratosferico e dell'ambiente) – (art. 3 "Cessazione e riduzione dell'impiego delle sostanze lesive");
- ✓ Reati previsti dal D.Lgs. 6 novembre 2007 n. 202 (15) – artt. 8 (inquinamento doloso) e 9 (inquinamento colposo).

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

- ✓ Artt. 12, comma 3, 3-*bis*, 3-*ter*, 5 e 22, comma 12-*bis*, del D.Lgs. 25 luglio 1998 n. 286.
- ✓ Art. 22 c. 12-bis del D.Lgs. n. 286/1998 (modificato dal D.L. n. 145 dell'11 ottobre 2024 e dalla L. n. 187 del 9 dicembre 2024)

❒ **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. 74/2000, aggiornato al D.Lgs. 5 novembre 2024 n. 173 (Testo unico delle sanzioni tributarie amministrative e penali), la cui formale operatività è prevista per il 1° gennaio 2026.

- ✓ Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2);
- ✓ Dichiarazione fraudolenta mediante altri artifici (art. 3);
- ✓ Emissione di fatture o altri documenti per operazioni inesistenti (art. 8);
- ✓ Occultamento o distruzione di documenti contabili (art. 10);
- ✓ Sottrazione fraudolenta al pagamento di imposte (art. 11).

Ai succitati articoli, 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 e paesaggistici):

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

❒ ***Art. 25- undevicies (Delitti contro gli animali):***

- ✓ Uccisione di animali (art. 544 bis c.p.);
- ✓ Maltrattamento di animali (art. 544 ter);
- ✓ Spettacoli o manifestazioni vietate (art. 544 quater);
- ✓ Divieto di combattimento tra animali (art. 544 quinquies);
- ✓ Uccisione o danneggiamento di animali altrui (art. 638 c.p.).

❒ L. 146/2006 (Reati transnazionali):

- ✓ Art. 377-bis c.p.
- ✓ Art. 378 c.p.
- ✓ Art. 416 c.p.
- ✓ Art. 416-bis c.p.
- ✓ Art. 416-bis.1 c.p.
- ✓ Art. 12 co. 3, 3-bis, 3-ter e 5 D.Lgs. 286/1998
- ✓ Art. 74 D.P.R. 309/1990
- ✓ Art. 86 D.Lgs. 141/2024

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".

1.3. 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 231, a fini meramente organizzativi interni (e non, dunque, a fini esterni o di rilevanza amministrativa/penalistica) con l'obiettivo di innalzare ulteriormente il proprio ed autonomo raggio di azione anti-illegalità interaziendale.

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 stragrande 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.

1.4. 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 conseguenza che il Modello 231 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 il Modello 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 operative»;
- *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 il Modelli organizzativo in piena autonomia, oppure utilizzare i modelli redatti dalle associazioni di categoria a condizione però che venga specificatamente pensato e progettato, secondo un approccio "sartoriale", per quel determinato ente nel quale dovrà trovare applicazione»;
- *Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'Organismo di Vigilanza e prospettive di revisione del D.Lgs. 8 giugno 2001, n. 231,* a cura del Gruppo di Lavoro Multidisciplinare costituito da rappresentanti del Consiglio Nazionale Dottori Commercialisti ed Esperti contabili, Associazione Bancaria Italiana, Consiglio Nazionale Forense e Confindustria, del dicembre 2018;

- *Norma ISO 31000.2018* (in italiano *UNI ISO 31000)*[8]*,* di marca internazionale, che: fornisce principi e linee guida generali per la gestione del rischio utilizzabili per qualsiasi organizzazione e struttura (pubblica o privata); non è specifica per alcuna industria o settore (né è formalmente certificabile trattandosi di Linee Guida); è stata pubblicata per la prima volta nel mondo nel novembre del 2009, aggiornata nel febbraio 2018, pubblicata in Italia il 25 novembre 2010.

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

Ove poi - come appunto Sicil Tecno Plus srl - l'ente voglia spontaneamente adottare un Modello 231 integrato con il Sistema Anticorruzione: sono di estrema importanza 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 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

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

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.

Il che comporta:

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

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

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

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

- avere piena consapevolezza della contemporaneità di più rischi da dovere affrontare e superare;
- valutare quale sia il rischio minore e decidere di intraprenderlo sulla base di un modello di priorità condiviso e debitamente motivato;
- dare formalmente atto di come, e perché, si sia deciso di affrontare il rischio minore rispetto ad uno maggiore;
- essere in grado di controllare a posteriori - anche attraverso la succitata motivazione della decisione – l'effettuazione dell'avvenuta ponderazione del rischio;
- controllare e vigilare il successivo "rientro a regime" delle procedure ordinarie rispetto, ad esempio, all'adozione di quelle eccezionali assunte in situazioni di emergenza.

Nel Modello 231 di Sicil Tecno Plus srl, la fase di mappatura sarà affrontata attraverso l'applicazione della metodologia ISO 31000:2018.

B) *La gestione dei rischi*

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

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

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

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

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

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

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

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

[9] Una logica di questo tipo è coerente con i consolidati riferimenti internazionali in tema di controllo interno e di corporate governance ed è alla base dei sistemi di autovalutazione dei rischi (*Control Self Assessment*) già presenti nelle più avanzate realtà aziendali italiane e, comunque, in rapida diffusione nel nostro sistema economico anche dietro l'impulso di recenti regolamentazioni. Il riferimento internazionale comunemente accettato come modello di riferimento in tema di governance e controllo interno è il "*CoSO Report*", prodotto in USA nel 1992 dalla Coopers & Lybrand (ora PricewaterhouseCoopers) su incarico del *Committee of Sponsoring Organizations of the Treadway Commission* (con l'*Institute of Internal Auditors* e l'AICPA fra le Sponsoring Organizations) che lo ha adottato e proposto quale modello di riferimento per il sistema di controllo delle imprese. Ad esso si sono ispirate le regolamentazioni nazionali di tutti i principali paesi (Regno Unito, Canada, ecc.).
Il *CoSO Report* rappresenta anche in Italia la *best practice* formalmente riconosciuta per le società quotate in Borsa (cfr. la menzione contenuta nello stesso Codice di Autodisciplina adottato dal Comitato per la Corporate Governance delle Società Quotate presso la Borsa Italiana nel 1999 ed aggiornato da ultimo nel 2006), oltre a costituire un evidente riferimento concettuale della Guida Operativa Collegio Sindacale del 2000, delle Circolari dell'ISVAP e della Banca d'Italia.

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;

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

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

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

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

2.3 L'Organismo di Vigilanza

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

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

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

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

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

Al fine di consentire una azione di vigilanza quanto più possibile efficace ed incisiva, l'art. 6 del Decreto 231 prevede che siano assicurati all'Organismo di Vigilanza precisi e specifici "*obblighi di informazione".* Si tratta dei *flussi informativi* verso l'OdV - da parte di tutte le funzioni aziendali e/o dipendenti dell'ente - che il Modello 231 dovrà necessariamente declinare e comunicare con obbligo di osservanza.

I *Flussi Informativi* di Sicil Tecno Plus sono riportati *infra,* nella Parte II.

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

Tali norme di funzionamento sono inserite nello *Statuto OdV* di Sicil Tecno Plus, *infra* nella Parte II.

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

2.4 Il Sistema Disciplinare

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

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

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

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

Questa regola di autonomia vale per tutti i procedimenti disciplinari.

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

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

Nonostante tale premessa, la soluzione pragmatica unanimemente condivisa in tema di sistema disciplinare 231 è – anche al fine di evitare possibili e defatiganti contenziosi di natura lavoristica – quella di strutturare la parte dei Modelli che riguarda il sistema disciplinare rinviando:

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

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

- Forma scritta;

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

Il *Sistema Disciplinare* è riportato in Allegato 1.

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.

[10] V. pubblicazione in "bacheca lavoratori", o sul sito aziendale, o diffusione con apposita circolare, o comunicato, anche se rimane sempre preferibile una consegna personale con debita sottoscrizione «per presa visione».
[11] «La contestazione deve fornire le indicazioni necessarie ed essenziali per individuare, nella sua materialità, i fatti oggetto di contestazione» (Cass. civ., sez. L., 16 ottobre 2019, n. 26199).
[12] Il principio è fissato anche dall'art. 2106 c.c. (*Sanzioni disciplinari*): «L'inosservanza delle disposizioni contenute nei due articoli precedenti può dar luogo alla applicazione di sanzioni disciplinari, secondo la gravità dell'infrazione».

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[13] e 2 quater[14] 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 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

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

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

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 non 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.

Nello specifico caso di STP la *tutela da whistleblowing* – ovvero il relativo *canale interno di segnalazione* - viene affidata all'Organismo di Vigilanza.

Allegato alla fine del presente documento, quale parte integrante del Modello 231, è riportata la relativa normativa e gestione procedurale.

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.

È, appunto, questa la scelta adottata da Sicil Tecno Plus.

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

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

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

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

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

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

- giusta causa di azione disciplinare (per i dipendenti);
- inadempimento alle obbligazioni contrattuali con ogni conseguente effetto di legge e di contratto (per i collaboratori, professionisti o fornitori esterni);

- giusta causa di revoca dei poteri e/o di estromissione societaria (per dirigenti, amministratori o organi che rivestono cariche sociali).

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

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

PARTE II – Il Modello 231 di Sicil Tecno Plus

1. CHI SIAMO

OMISSIS

Il sistema di governance adottato è quello ad Amministratore Unico, in persona del sig. Domenico Antonino Mazzeo, al quale sono affidate sia la rappresentanza che la firma sociale.

L'attività che Sicil Tecno Plus si prefigge di esercitare è:

1. edifici civili e industriali: costruzione,manutenzione o ristrutturazione di interventi puntuali di edilizia occorrenti per svolgere una qualsiasi attività umana, diretta o indiretta, completi delle necessarie strutture, impianti elettromeccanici, elettrici, telefonici ed elettronici e forniture di qualsiasi tipo nonché delle eventuali opere connesse, complementari e accessorie; comprende in via esemplificativa le residenze, le carceri, scuole, cimiteri, caserme, uffici, teatri, stadi, edifici per industrie, edifici per parcheggi, stazioni ferroviarie e metropolitane, edifici aeroportuali nonché' qualsiasi manufatto speciale in cemento armato, semplice o precompresso, gettato in opera quali volte sottili, cupole, serbatoi pensili, silos ed edifici di grande altezza con strutture di particolari caratteristiche e complessità;

2. restauro e manutenzione di beni immobili sottoposti a tutela ai sensi delle disposizioni in materia di beni culturali e ambientali: svolgimento di un insieme coordinato di lavorazioni specialistiche necessarie a recuperare, conservare, consolidare, trasformare, ripristinare, ristrutturare, sottoporre a manutenzione immobili di interesse storico soggetti a tutela a norma delle disposizioni in materia di beni culturali e ambientali; lavori inerenti restauro e manutenzione di beni culturali immobili e alla conservazione e restauro di opere d'arte; riguarda altresì la realizzazione negli immobili di impianti elettromeccanici, elettrici, telefonici ed elettronici e rifiniture tipo nonché di eventuali opere connesse, complementari e accessorie;

3. strade, autostrade, ponti, viadotti, ferrovie, linee tranviarie, metropolitane, funicolari, piste aeroportuali e relative opere complementari, la costruzione, la manutenzione o la ristrutturazione di interventi a rete che siano necessari per consentire la mobilità su "gomma", "ferro" e "aerea", qualsiasi sia il loro grado di importanza, completi di ogni opera connessa, complementare o accessoria anche di tipo puntuale, del relativo armamento ferroviario, nonché di tutti gli impianti automatici, elettromeccanici, elettrici, telefonici, elettronici e per la trazione elettrica necessari a fornire un buon servizio all'utente in termini di uso, informazione, sicurezza e assistenza; le strade, qualsiasi sia il loro grado di importanza, le autostrade, le superstrade, inclusi gli interventi puntuali quali le pavimentazioni speciali, le gallerie artificiali, gli svincoli a raso o in sopraelevata, i parcheggi a raso, le opere di sostegno dei pendii, i rilevati, le ferrovie di interesse nazionale e locale, le metropolitane, le funicolari e le linee tranviarie di qualsiasi caratteristica tecnica, le piste di decollo aerei ed i piazzali di servizio di eliporti, le stazioni, le pavimentazioni realizzate con materiali particolari, naturali ed artificiali, nonché i ponti, anche di complesse caratteristiche tecniche, in ferro, cemento armato semplice o precompresso, prefabbricati o gettati in opera;

4. opere d'arte nel sottosuolo: la costruzione, la manutenzione o la ristrutturazione, mediante l'impiego di specifici mezzi tecnici speciali, di interventi in sotterraneo che siano necessari per consentire la mobilità su "gomma" e su "ferro", qualsiasi sia il loro grado di importanza, completi di ogni opera connessa, complementare o accessoria, puntuale o a rete, quali strade di accesso di qualsiasi grado di importanza, svincoli a raso o in sopraelevata, parcheggi a raso, opere di sostegno dei pendii e di tutti gli impianti elettromeccanici, elettrici, telefonici ed elettronici nonché di armamento ferroviario occorrenti per fornire un buon servizio all'utente in termini di uso, informazione, sicurezza e assistenza; comprende in via esemplificativa gallerie naturali, trafori, passaggi sotterranei, tunnel;

5. dighe: costruzione, manutenzione o ristrutturazione di interventi puntuali che siano necessari per consentire la raccolta di acqua da effettuare per qualsiasi motivo, localizzati su corsi d'acqua e bacini interni, complete di tutti gli impianti elettromeccanici, meccanici, elettrici ed elettronici necessari all'efficienza e all'efficacia degli interventi nonché delle opere o lavori a rete a servizio degli stessi; comprende dighe realizzate con qualsiasi tipo di materiale;

6. acquedotti, asdotti, oleodotti, opere di irrigazione e di evacuazione: costruzione, manutenzione o ristrutturazione di interventi a rete che siano necessari per attuare il "servizio idrico integrato" ovvero per trasportare ai punti di utilizzazione fluidi aeriformi o liquidi, completi di ogni opera connessa, complementare o accessoria anche di tipo puntuale e di tutti gli impianti elettromeccanici, meccanici, elettrici, telefonici ed elettronici, necessari a fornire un buon servizio all'utente in termini di uso, funzionamento, informazione, sicurezza e assistenza ad un normale funzionamento; comprende in via semplificativa, opere di captazione delle acque, impianti di potabilizzazione, acquedotti, torri piezometriche, impianti di sollevamento, serbatoi interrati o sopraelevati, la rete di distribuzione all'utente finale, cunicoli attrezzati, fornitura e la posa in opera delle tubazioni, fognature con qualsiasi materiale, trattamento delle acque reflue prima della loro immissione nel ciclo naturale delle stesse; manutenzione rete distribuzione gas, costruzione allacciamenti interrati ed aerei, attività ai punti di riconsegna (attivazione, chiusure, sospensioni alimentazione e sostituzione contatori, estensioni e lavori di sostituzione delle reti di distribuzione gas, pronto intervento, gasdotti, oleodotti;

7. opere marittime e lavori di dragaggio: costruzione, manutenzione o ristrutturazione di interventi puntuali comunque realizzati, in acque dolci e salate, che costituiscono terminali per la mobilità su "acqua" ovvero opere di difesa del territorio delle stesse acque dolci o salate, completi di ogni opera connessa, complementare o accessoria anche di tipo puntuale e di tutti gli impianti elettromeccanici, elettrici, telefonici ed elettronici necessari a fornire un buon servizio all'utente in termini di uso, funzionamento, informazione, sicurezza e assistenza; comprende in via esemplificativa porti, moli, banchine, pennelli, piattaforme, pontili, difese costiere, scogliere, condotte sottomarine, bocche di scarico nonché lavori di dragaggio in mare o in bacino e quelli di protezione contro l'erosione delle acque dolci o salate;

8. opere fluviali, di difesa, di sistemazione idraulica e bonifica, costruzione e manutenzione o ristrutturazione di interventi, puntuali e a rete, comunque realizzati, occorrenti per la sistemazione di corsi d'acqua naturali o artificiali nonché per la difesa del territorio dai suddetti corsi d'acqua, completi di ogni opera connessa, complementare o accessoria, nonché di tutti gli impianti elettromeccanici, elettrici, telefonici ed elettronici necessari; comprende in via esemplificativa canali navigabili, bacini di espansione, sistemazioni di foci, consolidamento delle strutture degli alvei dei fiumi e dei torrenti, gli argini di qualsiasi tipo, sistemazione e regimentazione idraulica delle acque superficiali, opere di diaframmatura dei sistemi arginali, traverse per derivazioni e opere per la stabilizzazione dei pendii;

9. impianti per la produzione di energia elettrica, costruzione, manutenzione o ristrutturazione degli interventi portuali che sono necessari per la produzione di energia elettrica, completi di ogni connessa opera muraria, complementare o accessoria, puntuale o a rete, nonché di tutti gli impianti elettromeccanici, elettrici, telefonici ed elettronici, necessari in termini di funzionamento, informazione, sicurezza e assistenza; comprende le centrali idroelettriche ovvero alimentate da qualsiasi tipo di combustibile;

10. impianti per trasformazione alta/media tensione e per la distribuzione di energia elettrica in corrente alternata e continua ed impianti di pubblica illuminazione; costruzione, manutenzione o ristrutturazione degli interventi a rete che sono necessari per la distribuzione al alta e media tensione e per la trasformazione e distribuzione a bassa tensione all'utente finale di energia elettrica, completi di ogni connessa opera muraria, complementare o accessoria, puntuale o a rete e costruzione, manutenzione e ristrutturazione degli impianti di pubblica illuminazione, da realizzare all'esterno degli edifici; comprende in via esemplificativa centrali e cabine di trasformazione, tralicci necessari per trasporto e distribuzione di qualsiasi tensione, fornitura e posa in opera di cavi elettrici per qualsiasi numero di fasi su tralicci o interrati, fornitura e posa in opera di canali attrezzati e dei cavi di tensione e impianti di pubblica illuminazione su porti, viadotti, gallerie, strade, autostrade ed aree parcheggio;

11. impianti tecnologici: fornitura, installazione, gestione e manutenzione di un insieme di impianti tecnologici tra loro coordinati ed interconnessi funzionalmente, non eseguibili separatamente, di cui alle categorie di opere specializzate individuate con l'acronimo OS3, OS28 e OS30;

12. opere ed impianti di bonifica e protezione ambientale, esecuzione di opere puntuali o a rete necessarie per la realizzazione della bonifica e della protezione ambientale; comprende in via esemplificativa discariche, impermeabilizzazione con geomembrane dei terreni per la protezione delle falde acquifere, bonifica di materiali pericolosi, impianti di rilevamento e telerilevamento per il monitoraggio ambientale per qualsiasi modifica dell'equilibrio stabilito dalla vigente legislazione, nonché gli impianti necessari per il normale funzionamento delle opere o dei lavori e per fornire un buon servizio all'utente sia in termini di informazione e di sicurezza;

13. opere di ingegneria naturalistica: costruzione, manutenzione o ristrutturazione di opere o lavori puntuali, di opere o di lavori diffusi, necessari alla difesa del territorio ed al ripristino della compatibilità fra "sviluppo sostenibile" ed ecosistema, comprese tutte le opere ed i lavori necessari per attività botaniche e zoologiche; comprende in via esemplificativa i processi di recupero naturalistico, botanico e faunistico, conservazione e recupero del suolo utilizzato per cave e torbiere e dei bacini idrografici, eliminazione del dissesto idrogeologico per mezzo di piantumazione,opere necessarie per la stabilità dei pendii, riforestazione, lavori di sistemazione agraria e opere per rivegetazione di scarpate stradali, ferroviarie, cave e discariche; lavori inerenti verde storico, parchi e giardini;
14. lavori in terra: scavo, ripristino e modifica di volumi di terra, realizzati con qualsiasi mezzo e qualunque sia la natura del terreno da scavare o ripristinare: vegetale, argilla, sabbia, roccia;
15. superfici decorate di beni immobili del patrimonio culturale e beni culturali mobili di interesse storico, artistico, archeologico ed etnoantropologico intervento diretto di restauro, esecuzione della manutenzione ordinaria e straordinaria di: superfici decorate di beni immobili del patrimonio culturale, manufatti lapidei, dipinti murali, dipinti su tela, dipinti su tavola o su altri supporti materici, stucchi, mosaici, intonaci dipinti e non dipinti, manufatti polimaterici, manufatti in legno policromi e non policromi, manufatti in osso, in avorio, in cera, manufatti ceramici e vitrei, manufatti in metallo e leghe, materiali e manufatti in fibre naturali e artificiali, manufatti in pelle e cuoio, strumenti musicali, strumentazioni e strumenti scientifici e tecnici; lavori inerenti alla manutenzione e al restauro dei beni culturali mobili e di superfici decorate di beni architettonici e materiali storicizzati di beni immobili culturali, a conservazione e restauro di opere d'arte;
16. beni culturali mobili di interesse archivistico e librario, l'intervento diretto di restauro, esecuzione di manutenzione ordinaria e straordinaria di manufatti cartacei e pergamenacei, di materiale fotografico e di supporti digitali;
17. impianti idricosanitari, cucine, lavanderie fornitura, montaggio e manutenzione o ristrutturazione di impianti idrosanitari, cucine, lavanderie, gas ed antincendio, qualsiasi sia il loro grado di importanza, completi di ogni connessa opera muraria, complementare o accessoria, da realizzarsi in opere generali che siano state già realizzate o siano in corso di costruzione;
18. impianti elettromeccanici trasportatori fornitura, montaggio e manutenzione o ristrutturazione d'impianti trasportatori, ascensori, scale mobili, di sollevamento e di trasporto completi di ogni connessa opera muraria, complementare o accessoria, da realizzarsi in opere generali che siano state già realizzate o siano in corso di costruzione;
19. impianti pneumatici e antintrusione fornitura, montaggio e manutenzione o ristrutturazione di impianti pneumatici e di impianti antintrusione, completi di ogni connessa opera muraria, complementare o accessoria, da realizzarsi in opere generali che siano state già realizzate o siano in corso di costruzione;
20. finiture di opere generali in materiali lignei, plastici, metallici e vetrosi fornitura e posa in opera, la manutenzione e ristrutturazione di carpenteria e falegnameria in legno, di infissi interni ed esterni, di rivestimenti interni ed esterni, di pavimentazioni di qualsiasi tipo e materiale e di altri manufatti in metallo, legno, materie plastiche e materiali vetrosi e simili;
21. finiture di opere generali di natura edile e tecnica costruzione, manutenzione o ristrutturazione di murature e tramezzature di qualsiasi tipo, comprensive di intonacatura, rasatura, tinteggiatura, verniciatura e simili nonché fornitura e posa in opera, manutenzione di opere delle finiture di opere generali quali isolamenti termici e acustici, controsoffittatura e barriere al fuoco;
22. opere di impermeabilizzazione fornitura, posa in opera e ristrutturazione di opere di impermeabilizzazione con qualsiasi materiale e simili;
23. impianti per segnaletica luminosa e sicurezza del traffico fornitura e posa in opera, manutenzione sistematica o ristrutturazione di impianti automatici per segnaletica luminosa e la sicurezza del traffico stradale, ferroviario, metropolitano o tranviario compreso il rilevamento delle informazioni ed elaborazione delle medesime;
24. segnaletica stradale non luminosa fornitura, posa in opera, manutenzione o ristrutturazione nonché esecuzione della segnaletica stradale non luminosa, verticale, orizzontale e complementare;
25. apparecchiature strutturali speciali fornitura, posa in opera e manutenzione o ristrutturazione di dispositivi strutturali, quali giunti di dilatazione, apparecchi di appoggio, i dispositivi antisismici per ponti e viadotti stradali e ferroviari;

26. barriere stradali di sicurezza fornitura, posa in opera e manutenzione o ristrutturazione di dispositivi quali barriere, alternatori d'urto, recinzioni e simili, finalizzati al contenimento e sicurezza del flusso veicolare stradale;
27. barriere paramassi, fermaneve e simili fornitura, posa in opera e manutenzione o ristrutturazione delle barriere paramassi e simili, finalizzata al contenimento ed alla protezione dalla caduta dei massi e valanghe, inclusi gli interventi con tecniche alpinistiche;
28. strutture prefabbricate in cemento armato produzione in stabilimento industriale e montaggio in opera di strutture prefabbricate in cemento armato normale a precompresso;
29. impianti di smaltimento e recupero dei rifiuti costruzione e manutenzione ordinaria e straordinaria di impianti di termodistruzione dei rifiuti e connessi sistemi di trattamento dei fumi e di recupero dei materiali, comprensivi dei macchinari di preselezione, compostaggio e produzione di combustibile derivato dai rifiuti, completi di ogni connessa opera muraria, complementare o accessoria, puntuale o a rete;
30. pulizia di acque marine, lacustri, fluviali pulizia con particolari mezzi tecnici speciali di qualsiasi tipo di acqua e trasporto del materiale di risulta nelle sedi prescritte dalle vigenti norme;
31. impianti per centrali di produzione energia elettrica, costruzione, manutenzione o ristrutturazione di impianti ed apparati elettrici a servizio di qualsiasi centrale di produzione di energia elettrica;
32. linee telefoniche e impianti di telefonia fornitura, ontaggio e manutenzione o ristrutturazione di linee telefoniche esterne ed impianti di telecomunicazioni ad alta frequenza qualsiasi sia il loro grado di importanza, completi di ogni connessa opera muraria, complementare o accessoria da realizzarsi separatamente dall'esecuzione di altri impianti, in opere generali che siano state già realizzate o siano in corso di costruzione;
33. componenti strutturali in acciaio produzione in stabilimento e montaggio in opera di strutture in acciaio;
34. componenti per facciate continue: produzione in stabilimento e montaggio in opera di facciate continue costituite da telai metallici ed elementi modulari in vetro o altro materiale;
35. impianti di reti di telecomunicazione e di trasmissione dati la fornitura,montaggio e manutenzione o ristrutturazione di impianti di commutazione per reti pubbliche o private, locali o interurbane, di telecomunicazione per telefonia, telex, dati e video su cavi in rame, su cavi in fibra ottica, su mezzi radioelettrici, su satelliti telefonici, radiotelefonici, televisivi e reti di trasmissione dati e simili, qualsiasi sia il loro grado di importanza, completi di ogni connessa opera muraria, complementare o accessoria, da realizzarsi, separatamente dalla esecuzione di altri impianti, in opere generali che siano state già realizzate o siano in corso di costruzione;
36. rilevamenti topografici: esecuzione di rilevamenti topografici speciali richiedenti mezzi e specifica organizzazione imprenditoriale;
37. indagini geognostiche: esecuzione di indagini geognostiche ed esplorazioni del sottosuolo con mezzi speciali, anche ai fini ambientali, compreso il prelievo di campioni di terreno o di roccia e l'esecuzione di prove in situ;
38. opere strutturali speciali: costruzione di opere destinate a trasferire carichi di manufatti poggianti su terreni non idonei a reggere i carichi stessi, opere destinate a conferire ai terreni caratteristiche di resistenza e di indeformabilità tali da rendere stabili l'imposta di manufatti e da prevenire dissesti geologici, opere per rendere antisismiche le strutture esistenti e funzionanti; comprende esecuzione di pali di qualsiasi tipo, di sottofondazioni, palificate a muri di sostegno speciali, ancoraggi, opere per ripristinare la funzionalità statica delle strutture, pozzi, opere per garantire pendii e lavorazioni speciali per il prosciugamento, l'impermeabilizzazione ed il consolidamento di terreni;
39. impianti di potabilizzazione e depurazione costruzione, manutenzione o ristrutturazione di impianti di potabilizzazione di acque e depurazione di quelle reflue, compreso recupero del biogas e produzione di energia elettrica, completi di ogni connessa opera muraria, complementare o accessoria, puntuale o a rete;
40. demolizione di opere smontaggio di impianti industriali e demolizione completa di edifici con attrezzature speciali ovvero con uso di esplosivi, taglio di strutture in cemento armato e demolizioni in genere, compresa raccolta dei materiali di risulta, separazione e riciclaggio nell'industria dei componenti;
41. verde e arredo urbano: costruzione, montaggio e manutenzione di elementi non costituenti impianti tecnologici che sono necessari a consentire un miglior uso della città nonché realizzazione e manutenzione di verde urbano; comprende campi sportivi, terreni di gioco, sistemazioni paesaggistiche, verde attrezzato, recinzioni;
42. scavi archeologici: scavi archeologici e attività connesse;

43. pavimentazioni e sovrastrutture speciali: costruzione, manutenzione o ristrutturazione di pavimentazioni realizzate con materiali particolari, naturali o artificiali, in quanto sottoposti a carichi e sollecitazioni notevoli quali quelle delle piste aeroportuali;
44. impianti per la trazione elettrica: fornitura, posa in opera e manutenzione sistematica o ristrutturazione degli impianti per la trazione elettrica di qualsiasi ferrovia, metropolitana o linea tranviaria; comprende in via esemplificativa centrali e cabine di trasformazione, tralicci necessari per il trasporto e distribuzione della tensione, fornitura e posa di cavi elettrici per qualsiasi numero di fasi su tralicci o interrati, fornitura e posa in opera di canali attrezzati e cavi di tensione nonché tutti gli impianti elettromeccanici, elettrici, telefonici ed elettronici, necessari in termini di funzionamento, informazione, sicurezza e assistenza;
45. impianti termici e di condizionamento: fornitura,montaggio e manutenzione o ristrutturazione di impianti termici e di impianti per condizionamento del clima, qualsiasi sia il loro grado di importanza, completi di ogni opera muraria, complementare o accessoria, da realizzarsi separatamente dalla esecuzione di altri impianti, in opere generali che siano già realizzate o in costruzione;
46. armamento ferroviario: fornitura, posa in opera e manutenzione sistematica o ristrutturazione di binari per qualsiasi ferrovia, metropolitana o linea tranviaria nonché di impianti di frenatura e automazione per stazioni smistamento merci;
47. impianti interni elettrici, telefonici, radiotelefonici e televisivi: la fornitura, il montaggio e la manutenzione o la ristrutturazione di impianti elettrici, telefonici, radiotelefonici, televisivi nonché di reti di trasmissione dati, completi di ogni opera muraria, complementare o accessoria, da realizzarsi in interventi appartenenti alle categorie generali che siano stati già realizzati o siano in corso di costruzione;
48. impianti per la mobilità sospesa fornitura, montaggio e manutenzione o ristrutturazione di impianti e apparecchi di sollevamento e trasporto, completi di ogni connessa opera muraria, complementare o accessoria, puntuale o a rete (filovie, teleferiche, sciovie, gru e simili);
49. strutture in legno: produzione in stabilimenti industriali e montaggio in situ di strutture costituite di elementi lignei pretrattati;
50. coperture speciali: costruzione e manutenzione di coperture particolari comunque realizzate quali tensostrutture, coperture geodetiche, quelle copriscopri, quelle pennellate e simili;
51. sistemi antirumore per infrastrutture di mobilità costruzione, posa in opera, manutenzione e verifica acustica di opere di contenimento del rumore di origine stradale o ferroviaria quali barriere in metallo calcestruzzo, legno vetro o materiale plastico trasparente, biomuri, muri cellulari o alveolari nonché rivestimenti fonoassorbenti di pareti di contenimento terreno o di pareti di gallerie;
52. interventi a basso impatto ambientale: costruzione e manutenzione di qualsiasi opera interrata mediante utilizzo di tecnologie di scavo non invasive; comprende le perforazioni orizzontali guidate e non, con eventuale riutilizzo e sfruttamento delle opere esistenti, nonché utilizzo di tecnologie di video ispezione, risanamento, rinnovamento e sostituzione delle sottostrutture interrate ovvero di tecnologie per miniscavi superficiali;
53. assunzione ed esecuzione di appalti in proprio e per conto terzi, relativi all'esecuzione di lavori marittimi e portuali, ad acquedotti, fognatura, lavori idraulici in genere, costruzione e manutenzione di reti di gas metano;
54. lavorazione e produzione nonché commercio e rappresentanza per conto proprio e/o di terzi di ogni sorta di materiale occorrente per opere sopra indicate;
55. acquisto e/o vendita di immobili urbani o rustici e di aree edificabili, la gestione e/o locazione degli immobili sociali;
56. studio, progettazione, acquisto e/o la realizzazione in proprio e/o in appalto e l'installazione di impianti industriali e civili di qualsiasi tipo e/o specie, compresi quelli elettrici e di impianti tecnologici in genere, di componenti, attrezzature e strumentazioni relativi a impianti civili, industriali e/o tecnologici e del loro assemblaggio;
57. l'esecuzione di ogni lavoro, anche di sistemazione del suolo o edile, necessario o inerente o complementare per la realizzazione delle sopra indicate opere o impianti;
58. la commercializzazione al dettaglio e/o ingrosso di materiale elettrico, elettronico, hifi, di elettrodomestici in genere, materiale edile in genere, prodotti non alimentari in genere; di detti prodotti la società potrà assumere la rappresentanza con o senza deposito;
59. assunzione ed esecuzione di appalti in proprio e per conto terzi, relativi a: a) installazione di impianti elettrici, telefonici, antifurti, idrici, citofonici, automatismi, antenne e di climatizzazione, nelle varie forme

civili ed industriali; stazioni di distribuzione di energia, cabine di trasformazione, linee elettriche a bassa, media e alta tensione, impianti a gas; b) all'esecuzione di lavori marittimi e portuali, ad acquedotti, fognature, lavori idraulici in genere, costruzione e manutenzione di reti di gas metano; c) progettazione ed esecuzione di costruzioni edili di ogni tipo e specie (immobili urbani e/o rustici, scuole, stabilimenti industriali, etc;

60. lavorazione e produzione nonché commercio e rappresentanza, per conto proprio e/o di terzi, di ogni sorta di materiale occorrente per le opere sopra indicate;

61. noleggio di macchine strumentali ed industriali;

62. esercizio delattività di recupero e messa in riserva di rifiuti non pericolosi derivanti dalle attività di costruzione e demolizione con impianti mobili e/o fissi per la produzione di inerti;

63. distribuzione e commercializzazione di carburante gpl, oli lubrificanti, metano, derivati del petrolio in genere;

64. acquisto e/o vendita di immobili urbani o rustici e di aree edificabili;

65. gestione e/o locazione degli immobili sociali;

66. studio, progettazione, acquisto e/o realizzazione, in proprio e/o in appalto, e installazione di impianti industriali e civili, compresi quelli elettrici, e di impianti tecnologici in genere; di componenti, attrezzature e strumentazioni relativi ad impianti civili, industriali e/o tecnologici e del loro assemblaggio;

67. esecuzione di ogni lavoro, anche di sistemazione del suolo od edile, necessario o, comunque, inerente o complementare per la realizzazione delle sopra indicate opere o impianti;

68. produzione e distribuzione di energia elettrica e di calore,con impianti alimentati da fonti rinnovabili non fossili (eolica,solare,geotermica,del moto ondoso,maremotrice,idraulica,biomasse,gas di discarica,gas residuati dai processi di depurazione e biogas e impianti di cogenerazione;

69. trasmissione di energia elettrica;

70. commercio di energia elettrica;

71. fornitura di vapore e aria condizionata;

72. trasporto e smaltimento di rifiuti speciali;

73. fornitura di acqua depurata e non;

74. commercializzazione, vendita, noleggio, riparazione e manutenzione di tutti i tipi di veicoli nuovi e usati e loro accessori; attività di soccorso stradale;

75. trasporto conto proprio e conto terzi;

76. produzione e distribuzione di energia elettrica e di calore, con impianti alimentati da fonti non rinnovabili;

77. commercio di tutti i tipi di energia rinnovabili e non rinnovabili;

78. attività di gestione ed esercizio di impianti a tecnologia complessa ed altre dotazioni patrimoniali e del connesso servizio, volti al recupero, al trattamento ed allo smaltimento, anche a mezzo di incenerimento con termovalorizzazione, di qualunque genere di rifiuto e segnatamente dei rifiuti urbani, dei rifiuti assimilabili ai rifiuti urbani, dei rifiuti speciali inerti, dei rifiuti speciali pericolosi e non pericolosi, dei rifiuti ospedalieri, dei rifiuti di imballaggio provenienti da insediamenti produttivi, industriali e commerciali in conformità alle autorizzazioni ricevute dalla società stessa.

79. attività di progettazione e realizzazione di impianti a tecnologia complessa e di qualunque altro impianto o bene connesso o strumentale alle predette attività;

80. attività di recupero energetico, connesso allo smaltimento a mezzo di incenerimento, con conseguente produzione e vendita di calore ed energia elettrica, nei limiti e con le modalità previsti dalla normativa vigente;

81. attività di trasporto e di conferimento dei rifiuti da o verso impianti di recupero, trattamento o smaltimento, nei limiti in cui siano strumentali alle attività di cui sopra;

82. attività di gestione di discariche di rifiuti non pericolosi,compresa l'attività di captazione e recupero di biogas e ripristino ambientale;

83. ogni attività di ricerca e di sperimentazione studio e consulenza, direttamente o indirettamente connesse all'oggetto sociale;

84. le attività di gestione tecnicomanutentiva di impianti connessi e strumentali all'oggetto sociale;

85. produzione, vendita, commercializzazione ed attività commesse di prefabbricati di qualsivoglia materiale;

86. trasformazione e lavorazione di materiale lavico;

87. interventi a basso impatto ambientale: costruzione e manutenzione di qualsiasi opera interrata mediante l'utilizzo di tecnologie di scavo non invasive;
88. attività di manutenzione dei propri mezzi;
89. attività di gestione officina per manutenzione mezzi;
90. gestione officina interna per la riparazione dei mezzi d'opera ed attrezzature della società;
91. montaggio, smontaggio e riparazione pneumatici;
92. raccolta e trasporto di rifiuti speciali pericolosi;
93. attività di bonifica di beni contenenti amianto, effettuata sui seguenti materiali: materiali edili contenenti amianto legato in matrici cementizie o resinoidi;
94. attività di bonifica di beni contenenti amianto, effettuata sui seguenti materiali: materiali d'attrito, materiali isolanti (pannelli, coppelle, carte e cartoni, tessili, materiali spruzzati, stucchi, smalti, bitumi, colle, guarnizioni, altri materiali isolanti, contenitori a pressione, apparecchiature fuori uso, altri materiali incoerenti contenenti amianto;
95. attività di rimozione, smaltimento e bonifica di manufatti contenenti amianto;
96. montaggio, smontaggio e smaltimento pannelli fotovoltaici, climatizzatori e caldaie.

In via sintetica: Sicil Tecno Plus è una Società primariamente specializzata in *impiantistica tecnologica*, ovvero *opere di progettazione, realizzazione e manutenzione di opere civili e industriali,* tra cui:

- Gasdotti, con relativa rete di allacciamento e distribuzione;
- Acquedotti e fognature, con relativa rete di allacciamento e distribuzione;
- Opere stradali, restauri e perforazioni orizzontali con teleguidata;
- Sostituzione delle reti in fibrocemento contenenti amianto;
- Lavori di revamping di depuratori;
- Controllo, manutenzione e assistenza impianti termici;
- Lavori di restauro, ammodernamento, ristrutturazione e adeguamento impianti energetici;
- Realizzazione di parcheggi di interscambio;

Revisore Legale: Dott. Russo Alessandro Antonio.

Sede legale

- Belpasso (CT), Strada Provinciale 1465, cap 95032, frazione Piano Tavola. Nr. REA, CT – 293846. Codice fiscale e n.iscr. al Registro Imprese 04414740870. Partita IVA, 04414740870. Forma giuridica, società a responsabilità limitata.

Sedi Secondarie e Unità Locali

- Unità Locale n. CT/4 – Ufficio. Data apertura: 30/06/2020. Indirizzo: Catania (CT), Via Nuova Lucello 154/H, cap 95126. Classificazione ATECORI 2007 dell'attività (classificazione desunta dall'attività dichiarata): Codice: 41.2 - costruzione di edifici residenziali e non residenziali Importanza: prevalente svolta dall'impresa.
- Unità Locale n. AG/1. Contrada Zaccanello snc Racalmuto (AG), CAP 92020;
- Strada Statale 36 del L.Como e dello Spluga, Garbagbate Monastero (LC), CAP 23846;
- Unità Locale n. NA/1, via Signorelle A Patria 37, Giugliano in Campania (NA), CAP 80014

Organigramma

L'attuale articolazione organizzativa è in fase di aggiornamento.

Abilitazioni, Classificazioni, Qualificazioni SOA e Certificazioni:

- **Abilitazioni**

L'impresa, ai sensi del Decreto 22 gennaio 2008 n. 37 (*Norme per la sicurezza degli impianti*) è abilitata, salvo le eventuali limitazioni più sotto specificate, all'installazione, alla trasformazione, all'ampliamento e alla manutenzione degli impianti di cui all'Art. 1 del Decreto n. 37/2008, come segue:

- ***Lettera A***, impianti di produzione, trasformazione, trasporto, distribuzione, utilizzazione dell'energia elettrica, impianti di protezione contro le scariche atmosferiche, nonche' gli impianti per l'automazione di porte, cancelli e barriere.
- ***Lettera B***, impianti radiotelevisivi, le antenne e gli impianti elettronici in genere.
- ***Lettera C***, impianti di riscaldamento, di climatizzazione, di condizionamento e di refrigerazione di qualsiasi natura o specie, comprese le opere di evacuazione dei prodotti della combustione e delle condense, e di ventilazione ed aerazione dei locali.
- ***Lettera D***, impianti idrici e sanitari di qualsiasi natura o specie.
- ***Lettera E***, impianti per la distribuzione e l'utilizzazione di gas di qualsiasi tipo, comprese le opere di evacuazione dei prodotti della combustione e ventilazione ed aerazione dei locali.
- ***Lettera F***, impianti di sollevamento di persone o di cose per mezzo di ascensori, di montacarichi, di scale mobili e simili.
- ***Lettera G***, impianti di protezione antincendio.

- **Classificazioni**

- ***Classificazione ATECORI 2007*** dell'attività prevalente (classificazione desunta dall'attività dichiarata):

  - Codice: 41.2 - costruzione di edifici residenziali e non residenziali. Importanza: prevalente svolta dall'impresa.
  - Codice: 42.11 - costruzione di strade, autostrade e piste aeroportuali Importanza: secondaria Registro Imprese. Data inizio: 31/10/2006.
  - Codice: 42.21 - costruzione di opere di pubblica utilita' per il trasporto di fluidi Importanza: secondaria Registro Imprese. Data inizio: 31/10/2006.
  - Codice: 43.12 - preparazione del cantiere edile e sistemazione del terreno Importanza: secondaria Registro Imprese. Data inizio: 31/10/2006.
  - Codice: 43.29.09 - altri lavori di costruzione e installazione nca Importanza: secondaria Registro Imprese. Data inizio: 31/10/2006.
  - Codice: 43.34 - tinteggiatura e posa in opera di vetri Importanza: secondaria Registro Imprese. Data inizio: 31/10/2006.
  - Codice: 81.3 - cura e manutenzione del paesaggio (inclusi parchi, giardini e aiuole) Importanza: secondaria Registro Imprese. Data inizio: 31/10/2006
  - Codice: 43.11 - demolizione di edifici Importanza: secondaria Registro Imprese. Data inizio: 02/07/2009.
  - Codice: 43.13 - trivellazioni e perforazioni Importanza: secondaria Registro Imprese. Data inizio: 20/04/2010.
  - Codice: 43.21.01 - installazione di impianti elettrici in edifici o in altre opere di costruzione (inclusa manutenzione e riparazione). Importanza: secondaria Registro Imprese Data inizio: 26/04/2011.
  - Codice: 43.21.02 - installazione di impianti elettronici (inclusa manutenzione e riparazione). Importanza: secondaria Registro Imprese Data inizio: 26/04/2011.
  - Codice: 43.22.01 - installazione di impianti idraulici, di riscaldamento e di condizionamento dell'aria (inclusa manutenzione e riparazione) in edifici o in altre opere di costruzione. Importanza: secondaria Registro Imprese Data inizio: 26/04/2011.

- Codice: 43.22.02 - installazione di impianti per la distribuzione del gas (inclusa manutenzione e riparazione). Importanza: secondaria Registro Imprese Data inizio: 26/04/2011.
- Codice: 43.22.03 - installazione di impianti di spegnimento antincendio, compresi quelli integrati (inclusa manutenzione e riparazione). Importanza: secondaria Registro Imprese Data inizio: 26/04/2011.
- Codice: 43.29.01 - installazione, riparazione e manutenzione di ascensori e scale mobili Importanza: secondaria Registro Imprese. Data inizio: 26/04/2011
- Codice: 39.00.09 - altre attività di risanamento e altri servizi di gestione dei rifiuti Importanza: secondaria Registro Imprese.
-

➢ **Qualificazioni SOA**

La Certificazione SOA è un'Attestazione di qualificazione per la partecipazione a gare d'appalto per l'esecuzione di appalti pubblici di lavori. Nello specifico, la Certificazione SOA è un attestato obbligatorio (rilasciato da Organismi di Attestazione autorizzati) che comprova la capacità economica e tecnica di un'impresa di qualificarsi per l'esecuzione di appalti pubblici di lavori di importo maggiore a € 150.000 e conferma inoltre che il soggetto certificato sia in possesso di tutti i requisiti necessari alla contrattazione pubblica.

Una volta ottenuta, la Certificazione SOA vale cinque anni (previa conferma di validità al terzo anno). Per averla vengono presi in considerazione i lavori eseguiti negli ultimi dieci anni e i cinque migliori documenti di reddito tra gli ultimi dieci approvati e depositati.

Le categorie di opere sono 52 (13 riguardanti opere di carattere generale e 39 riguardano opere specializzate). Le classifiche di importo sono 10 (dalla I, fino a euro 258.000, alla VIII, oltre euro 15.494.000). Ciascuna classifica abilita l'impresa in possesso di Certificazione SOA a concorre ad appalti di importi pari alla classifica accresciuta di un quinto.

Per ottenere la Certificazione SOA in classifiche di importo maggiori della II (oltre i 516.000 euro) è obbligatorio disporre di un Sistema di Qualità aziendale, che sia certificato secondo la vigente norma (UNI EN ISO 9001).

In base alla normativa vigente, gli Organismi di Attestazione SOA, sono tenuti a riscontrare la bontà, veridicità, correttezza e sostanza di tutti i documenti che l'impresa utilizza ai fini della dimostrazione dei requisiti utili alla propria Qualificazione; tale processo di verifica prevede che la SOA interroghi sistemi informativi, banche dati, Enti che hanno rilasciato dichiarazioni o certificati.

La società ha attualmente le seguenti Qualificazioni:

- **OG 2** (*Restauro e manutenzione dei beni immobili sottoposti a tutela*) – **Classifica III** (fino a euro 1.033.000).
- **OG 3** (*Strade, autostrade, ponti, viadotti, ferrovie, metropolitane*) – **Classifica IV BIS** (fino a euro 3.500.000)
- **OG 6** (*Acquedotti, gasdotti, oleodotti, opere di irrigazione e di evacuazione*) – **Classifica VII** (fino a euro 15.494.000)

➢ **Certificazioni**

La società, attualmente, è in possesso delle seguenti Certificazioni:

- **ISO 9001:2015** (*Costruzione e manutenzione di gasdotti*)
- **EN ISO 3834 – 4: 2006** (*Requisiti qualità per la saldatura per fusione dei materiali metallici - saldatura di tubazioni metalliche per trasporto di fluidi e gas*)
- **EN ISO/IEC 27001: 2017** (*Gestione della sicurezza delle informazioni a supporto delle attività di costruzione, manutenzione di gasdotti e manutenzione di strade*)
- **UNI EN 50001: 2018** (*Sistema di gestione dell'energia. Costruzione e manutenzione di gasdotti. Manutenzione di strade*)

- **UNI/PDR 125:2022** (*Parità di genere*)
- **ISO 45001: 2023** (*Costruzione e manutenzione di gasdotti. Manutenzione strade*)
- **ISO 14001:2015** (*Costruzione e manutenzione di gasdotti. Manutenzione strade*)
- **ISO 39001 : 2016** (*Sistema di gestione della sicurezza stradale – Costruzione e manutenzione di gasdotti. Manutenzione di strade*)
- **ISO 37001:2016** (*Sistema di gestione per la prevenzione della corruzione – Costruzione e manutenzione di gasdotti. Manutenzione di strade*)
- **SA 8000: 2014**

2. GESTIONE DEL RISCHIO DA REATI PRESUPPOSTI

2.1. Mappatura dei rischi e approccio metodologico

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 Progetto Geoambiente, 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 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 Progetto Geoambiente) 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[15] tra di loro correlati;
- 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, purché si raggiunga l'obiettivo di «individuare le aree che, in ragione della natura e delle

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

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 presupposti 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 macroaree 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 e la Mappatura e Gestione dei rischi* sono riportate in Allegato 1).

Si riportano di seguito le *macroaree 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
- ❒ Area Reati contro gli animali

2.3. Macro aree normative e reati presupposti

❖ Area Reati contro la Pubblica Amministrazione

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

- *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. 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.*
- *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. 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 ...: 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 ...: reato presupposto dall'art. 25;*
- *art. 320 - corruzione di persona incaricata ...: reato presupposto dall'art. 25;*
- *art. 321 c.p. - pene per il corruttore: 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;*

Come chiarito nella Parte Generale, accanto ai succitati *reati presupposti ordinari,* Progetto Geoambiente 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.

❖ 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 P.A., quale persona offesa.

I reati inquadrabili in questa categoria sono:

- *art. 640 co. 2, n.1 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.*

- *Art. 2 L. 898 del 23 dicembre 1986*

Anche in questo caso vale quanto prima detto a proposito dell'inserimento nella macroarea 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 macroarea 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 Progetto Geoambiente in favore di privati.

Le ipotesi delittuose riferibili a questa macroarea sono:

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

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

Possono sinteticamente includersi ed accorpare in questa area generale - considerabile a mero "rischio teorico" di illegalità in vista di come concretamente opera Progetto Geoambiente - 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 Progetto Geoambiente,

I reati presupposti in connessione con questa macroarea sono quelli:

➢ ***Contro la Fede Pubblica:***

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

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

➢ ***Contro l'Ordine Pubblico:***

- *art. 416 c.p. - associazione per delinquere: reato presupposto dall'art. 24-ter;*
- *art. 416-bis c.p. - associazioni di tipo mafioso: reato presupposto dall'art. 24-ter;*
- *art. 416-ter c.p. - scambio elettorale politico mafioso: reato presupposto dall'art. 24-ter;*
- *art. 630 c.p. - sequestro di persona a scopo di estorsione: reato presupposto dall'art. 24-ter;*
- *art. 74 D.P.R. 309/1990 - 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.);*
- *Fatti di lieve entità (art. 2621-bis c.c.);*
- *False comunicazioni sociali delle società quotate (art. 2622 c.c.);*
- *Impedito controllo (art. 2625, co. 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 (TUF)***

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 o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di 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 dall'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 dall'art. 25-octies.1;*
- *art. 512-bis c.p. - Trasferimento fraudolento di valori: reato presupposto dall'art. 25-octies.1;*

- *art. 640-ter c.p. – Frode informatica [nell'ipotesi aggravata …]: reato presupposto dall'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 presupposti dal predetto articolo sono quelli previsti dal D.Lgs. 74/2000, aggiornato al D.Lgs. 5 novembre 2024 n. 173 (Testo unico delle sanzioni tributarie amministrative e penali), la cui formale operatività è prevista per il 1° gennaio 2026.

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

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

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

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

➢ ***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: *reato presupposto dall'art. 25-sexiesdecies.*

❖ Area Risorse Umane

Le condotte illecite di cui si parla sono:

- *art. 583-bis c.p. - pratiche di mutilazione degli organi genitali femminili: reato presupposto dall'art. 25-quater.1;*
- *art. 600 c.p. - riduzione o mantenimento in schiavitù o servitù: reato presupposto dall'art. 25-quinquies;*
- *art. 600-bis c.p. - prostituzione minorile: reato presupposto dall'art. 25-quinquies;*
- *art. 601 c.p. - tratta di persone: reato presupposto dall'art. 25-quinquies;*
- *art. 602 c.p. - acquisto e alienazione di schiavi: reato presupposto dall'art. 25-quinquies;*
- *art. 603-bis c.p. - intermediazione illecita e sfruttamento del lavoro: 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 dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria: reato presupposto dall'art. 25-decies;*
- *art. 12, co. 3, 3-bis, 3-ter, e 5 D.Lgs. 286/1998: reato presupposto dall'art. 25-duodecies;*
- *art. 22, comma 12-bis D.Lgs. 286/1998: reato presupposto dall'art. 25-duodecies;*

✓ art. 604-bis c.p. - Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa: *reato presupposto dall'art. 25-terdecies;*

✓ art. 3, co. 3-bis, della Legge 654/1975

- *art. 1,* L. n. 401 del 13 dicembre 1989 - *Frode in competizioni sportive*: *reato presupposto dall'art. 25-quaterdecies;*
- *art. 4,* L. n. 401 del 13 dicembre 1989 - (*Esercizio abusivo di attività di giuoco o di scommessa*: *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 dell'Azienda.

I reati inquadrabili in questa macroarea 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 231 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. 640-ter - frode informatica in danno dello Stato o di altro ente pubblico [reato rilevante ex D.Lgs. 231/2001 [se commesso in danno dello Stato o di altro ente pubblico o dell'Unione europea]: reato presupposto dall'art. 24;*
- *art. 629, co. 3, c.p. - estorsione: reato presupposto dall'art. 24-bis.*
- *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 pubblico interesse: reato presupposto dall'art. 24-bis;*
- *art. 640-quinquies c.p. - frode informatica del soggetto che presta servizi di certificazione di firma elettronica: reato presupposto dall'art. 24-bis.*

B) i reati accorpabili "lato sensu" come informatici

Oggetto di tutela di questa categoria normativa 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.*
- *art. 1, c. 11 D.L. n. 105 del 21 settembre 2019 (ostacolare o condizionare l'espletamento dei procedimenti … o delle attività ispettive e di vigilanza … fornisce informazioni, dati o elementi di fatto non rispondenti al vero … è punito con la reclusione da uno a tre anni).*

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

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

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

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

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

❖ Area Sicurezza Lavoratori

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

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

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

❖ Area Reati Ambientali

L'area in oggetto si riferisce:

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

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

La Legge del 22 maggio 2015 n. 68 ha introdotto, invece, la categoria dei "*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.);*
- *Impedimento del controllo (art. 452 septies);*
- *Circostanze aggravanti (art. 452-octies c.p.);*
- *Omessa bonifica (art. 452 terdecies);*
- *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. 255 bis (Abbandono di rifiuti non pericolosi in casi particolari);*
  - *art. 255 ter (Abbandono di rifiuti pericolosi);*
  - *art. 256, commi 1, 3, 5 e 6 (Attività di gestione di rifiuti non autorizzata);*
  - *art. 256 bis (Combustione illecita di rifiuti);*
  - *art. 257, commi 1 e 2 (Bonifica dei siti);*
  - *art. 258, comma 4 seconda parte (Violazione degli obblighi di comunicazione…);*
  - *art. 259 (Traffico illecito di rifiuti);*
  - *art. 260 bis, commi 6, 7 e 8;*
  - *art. 279, comma 5, (in materia di gestione stabilimenti).*

- I reati previsti dalla Legge 7 febbraio 1992 n. 150 *(in materia di commercio internazionale e detenzione di specie animali),* ed in particolare quelli ex:
  - *art. 1, commi 1 e 2 (in materia di importazione ed esportazione specie animali Allegato A);*
  - *art. 2, commi 1 e 2 (in materia di importazione ed esportazione specie animali Allegati B e C);*
  - *art. 6, commi 1 e 4 (in materia di detenzione animali selvatici).*

- I reati del codice penale richiamati dall'art. 3-bis della Legge 7 febbraio 1992 n. 150 (*in materia di commercio internazionale e detenzione di specie animali*), ed in particolare quelli ex:
  - *art. 476 c.p. (Falsità materiale commessa dal pubblico ufficiale in atti pubblici);*
  - *art. 477 c.p. (Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative);*
  - *art. 478 c.p. (Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti);*
  - *art. 479 c.p. (Falsità ideologica commessa dal pubblico ufficiale in atti pubblici);*
  - *art. 480 c.p. (Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative);*
  - *art. 481 c.p. (Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità);*
  - *art. 482 c.p. (Falsità materiale commessa dal privato);*
  - *art. 483 c.p. (Falsità ideologica commessa dal privato in atto pubblico);*
  - *art. 484 c.p. (Falsità in registri e notificazioni);*
  - *art. 485 c.p. (Falsità in scrittura privata);*
  - *art. 486 c.p. (Falsità in foglio firmato in bianco. Atto privato);*
  - *art. 487 c.p. (Falsità in foglio firmato in bianco. Atto pubblico);*
  - *art. 488 c.p. (Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali);*
  - *art. 489 c.p. (Uso di atto falso);*
  - *art. 490 c.p. (Soppressione, distruzione e occultamento di atti veri);*
  - *art. 491 c.p. (Documenti equiparati agli atti pubblici agli effetti della pena);*
  - *art. 491-bis c.p. (Documenti informatici);*
  - *art. 492 c.p. (Copie autentiche che tengono luogo degli originali mancanti);*
  - *art. 493 c.p. (Falsità commesse da pubblici impiegati incaricati di un servizio pubblico).*

- I reati previsti dalla Legge 28 dicembre 1993, n. 549 ("*Misure a tutela dell'ozono stratosferico e dell'ambiente*"), ed in particolare quelli ex:
  - *art. 3 (Cessazione e riduzione dell'impiego delle sostanze lesive)*

- I reati previsti D.Lgs. 6 novembre 2007 n. 202 (*Attuazione della direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e conseguenti sanzioni*) ed in particolare quelli ex:
  - *art. 8 (Inquinamento doloso).*
  - *art. 9 (Inquinamento colposo);*

❖ 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;*

❖ **Area Reati contro gli animali**

- *art. 544 bis c.p. - uccisione di animali: reato presupposto dall'art. 25 undevicies*
- *art. 544 ter c.p. - maltrattamento di animali: reato presupposto dall'art. 25 undevicies*
- *art. 544 quater c.p. - spettacoli o manifestazioni vietate: reato presupposto dall'art. 25 undevicies*
- *art. 544 quinquies - divieto di combattimento tra animali: reato presupposto dall'art. 25 undevicies*
- *art. 638 c.p. - uccisione o danneggiamento di animali altrui: reato presupposto dall'art. 25 undevicies*

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

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

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

In Allegato 3 è riportata l'analisi dettagliata della valutazione e stima dello specifico *livello di rischio da reati* utilizzando i criteri della succitata UNI ISO 31000:2018.

Le tabelle che seguono sintetizzano e riepilogano i risultati ottenuti, ovvero: *il livello di rischio residuo.*

OMISSIS

2.5. Gestione dei Rischi: Protocolli e sistemi di controllo

Si è più volte ricordato che, nello specifico ambito di un Modello 231, per protocollo[16] 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 esaltare 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 Modello, 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 Modello si è deciso di strutturare la parte dei *Protocolli* in due grandi sotto-categorie:

- **Protocolli Generali**, valevoli per tutte le ipotesi di "reato presupposto" e tutte le azioni aziendali;
- **Protocolli Speciali**, che comunque presuppongono la costante applicazione dei protocolli generali, ma che sono aderenti in modo mirato alle singole specifiche 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 in *tutte* le fasi della vita aziendale ed in relazione a tutte le possibili condotte societarie.

Si ribadisce, quindi, che nel Modello 231 della Società le due fattispecie di Protocolli opereranno in via sinergica e complementare:

- i Protocolli Generali, applicabili sempre e comunque da parte di tutti i Destinatari del Modello 231 in relazione a tutte le fasi di attività aziendale o le possibili ipotesi di reati presupposte;
- 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).

[16] 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.

2.6. I Protocolli Generali

Le caratteristiche di efficacia di un sistema di prevenzione dei comportamenti a rischio di commissione dei reati sono riconducibili soprattutto alla *robustezza*[17] ed i Protocolli Generali devono assicurare, anche secondo le Linee Guida di Confindustria, il rispetto dei seguenti **tre principi di robustezza**:

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

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

- **I controlli 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). La tracciabilità, la separazione dei ruoli ed una corretta assegnazione dei poteri costituiscono un requisito fondamentale nell'ottica della prevenzione dei reati del D.Lgs. 231/2001 in quanto rendono più difficile e complessa la realizzazione di illeciti.

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

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

I Protocolli Generali del presente Modello 231 includono i predetti principi di robustezza ed anche i seguenti **ulteriori principi**:

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

La necessità di individuare i soggetti agenti, oltre che in vista dei necessari controlli *in itinere*, è anche legata alla legittima possibilità di difesa della Società - ex artt. 5, co.2 e 6 co.1. lett. c) del D.Lgs. 231/2001 - in caso di malaugurata commissione di un fatto di reato. Il riparto delle responsabilità è uno dei principi cardine di un corretto Modello 231, sintetizzabile nel: *deve essere sempre chiaro ed univoco "chi" fa "che cosa", in relazione e/o "con chi"*, così come il corretto rilascio di deleghe (quale attribuzione, a carattere bilaterale, di funzioni e di compiti normativamente delegabili, al fine di innalzare i livelli di

[17] La robustezza in un sistema di prevenzione e controllo è intesa come la capacità del sistema di mantenere l'efficacia nel prevenire e rilevare errori, frodi o violazioni normative, nonostante le variazioni nelle condizioni operative o gli eventi imprevisti. Un sistema di controllo interno robusto è progettato per essere flessibile e adattabile, in grado di identificare e affrontare tempestivamente le minacce o le inefficienze emergenti senza compromettere la sua capacità di garantire la conformità normativa, proteggere gli asset aziendali e sostenere l'attuazione degli obiettivi aziendali. La robustezza viene promossa attraverso la progettazione e l'implementazione di procedure, politiche e controlli appropriati, nonché attraverso una supervisione continua e un monitoraggio attivo del sistema di controllo interno.

efficienza e di controllo aziendale e societario) o di procure (quali atti a carattere unilaterale che conferiscono al procuratore tutto o parte dei poteri diretti ed esclusivi del titolare).

L'attribuzione dei poteri è un diretto corollario del riparto di compiti e responsabilità. A tal fine, deve essere assicurata la conoscibilità, trasparenza e pubblicità dei poteri attribuiti.

Il protocollo è strettamente correlato al principio secondo cui: *chiunque, interno o esterno a Sicil Tecno Plus srl, 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 Sicil Tecno Plus srl.**
- **Il Codice Etico e di Comportamento** adottato da Sicil Tecno Plus srl (parte integrante del Modello 231), che fotografa l'assetto morale e comportamentale che la Società richiede sia rispettato nella conduzione della propria attività.
- **Le prescrizioni dell'Organismo di Vigilanza 231.**
- **Il Sistema Qualità** e quanto previsto dai Sistemi di Certificazione adottati dalla Società.
- **Le procedure e le prescrizioni** di tutti i sistemi gestionali adottati dalla Società.
- **Le norme e le circolari aziendali**, quali linee direttrici cui attenersi nello svolgimento dell'attività.

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

Tale presidio richiede che tutte le azioni siano descritte nel loro svolgimento e che tutte le fasi del processo siano individualizzate nei compiti 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 di ciò che è stato concretamente posto in essere. L'obiettivo è di rendere ricostruibili, tracciabili *ex post,* e dunque meglio controllabili, le azioni e i processi. L'informatizzazione è una prescrizione necessaria e 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 practices*. 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 – e, 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 efficace di comunicazione interna**

Dovrà essere assicurato un adeguato supporto informatico al fine di consentire una corretta ed esaustiva conoscenza, diffusione e condivisione, dei dati e delle informazioni aziendali di cui ai punti precedenti. Il suddetto presidio informatico deve rappresentare un reale e concreto ausilio per la gestione dei processi di lavoro. La razionalizzazione dei flussi ed adeguati filtri dovranno assicurare che dati e informazioni vengano differenziati in base a specifiche esigenze o singole aree lavorative. Sempre in via di correlata conseguenzialità rispetto ai punti precedenti, la strutturazione di un efficace 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 responsabile di funzione. 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, anche informale, a cadenza ravvicinata di razionale periodicità, in ordine ai fatti salienti societari riguardanti la gestione delle situazioni "sensibili".

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

La misura in oggetto offre diversi vantaggi significativi per un'organizzazione:

a) *efficienza*: elimina la necessità di gestire fisicamente documenti cartacei, riducendo i tempi e i costi associati alla manipolazione e alla conservazione della corrispondenza. Ciò consente un flusso di lavoro più rapido ed efficiente; b) *riduzione degli errori*: riduce il rischio di errori umani nella classificazione, nell'indirizzamento e nella registrazione dei documenti; c) *tracciabilità*: consente di tenere traccia del percorso della corrispondenza in entrata e uscita in modo accurato e dettagliato. Questo migliora la visibilità e il controllo sull'intero processo, facilitando la ricerca e il recupero dei documenti; d) *sicurezza*: offre livelli più elevati di sicurezza dei dati rispetto ai processi cartacei, infatti, le informazioni possono essere crittografate e protette da accessi non autorizzati, garantendo la riservatezza e l'integrità della corrispondenza; e) *risparmio di spazio*: eliminando la necessità di archiviare documenti cartacei, si libera spazio fisico negli uffici, riducendo i costi associati all'archiviazione e alla manutenzione degli archivi; f) *risposta rapida*: è possibile accedere istantaneamente alla corrispondenza in arrivo e in uscita da qualsiasi posizione, consentendo una risposta più rapida e tempestiva alle richieste dei clienti, dei partner commerciali o delle autorità.

- **Archiviazione dei dati**

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

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

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

L'identità del segnalante di illeciti, dovrà sempre essere tutelata, nei limiti di quanto previsto dalla legge e, in presenza di eventuali segnalazioni di illeciti, l'Organismo di Vigilanza dovrà intervenire immediatamente ove venga a conoscenza (per via diretta o indiretta) di licenziamenti, ritorsioni, discriminazioni subite dal segnalante a seguito o per causa della succitata segnalazione.

Alla luce, poi, delle modifiche normative intervenute nell'anno 2023, la Società ha provveduto ad implementare quanto richiesto dal Decreto Legislativo n. 24 del 10 Marzo 2023, ossia una nuova e specifica procedura in materia di *whistleblowing* - che ha lo scopo di disciplinare ex novo il sistema di segnalazioni previste dal succitato provvedimento di legge - fornendo opportune indicazioni ai Segnalanti per l'effettuazione di una Segnalazione.

In particolare, la procedura adottata prevede che le eventuali Segnalazioni debbano essere circostanziate, rilevanti ai sensi del predetto decreto e fondate su elementi di fatto precisi e concordanti di cui il Segnalante sia venuto a conoscenza in ragione delle funzioni svolte, o di violazioni del Modello 231.

A tal fine, nella procedura, sono stati definiti dei canali "sicuri" che garantiscano la riservatezza dell'identità del Segnalante nelle attività di gestione della Segnalazione. È stato anche sottolineato il divieto assoluto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del Segnalante per motivi collegati, direttamente o indirettamente alla Segnalazione effettuata, prevedendo sanzioni nei confronti di chi viola le misure di tutela del Segnalante, nonché di chi effettua con dolo o colpa gravi segnalazioni che si rivelino infondate.

2.7. I 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.

NOTA: In testa ad ogni protocollo viene indicata l'Area organizzativa (Amministrativa o Tecnica) *responsabile dell'applicazione di quel protocollo*. Ovvero, chi ne deve coordinare l'applicazione e ne deve verificare l'efficacia. Ma, in considerazione del fatto che i protocolli sono disegnati sulla logica dei processi, nella maggior parte dei casi essi attraversano l'organizzazione orizzontalmente; questo significa che implicano il coinvolgimento di funzioni appartenenti ad entrambe le Aree. Tutto ciò determina l'obbligo per tutti i collaboratori di Sicil Tecno Plus di conoscerli ed applicarli pedissequamente.

OMISSIS

3. L'ORGANISMO DI VIGILANZA DI STP

Volendo presidiare, monitorare e vigilare, l'efficacia del proprio Modello 231 in modo quanto più razionale e capillare possibile, Sicil Tecno Plus ha deciso di nominare un Organismo di Vigilanza ad alta professionalità tecnica e a composizione plurisoggettiva a due membri: uno, a competenza giuridico-penalistica; uno, a competenza organizzativa. Tale tipologia di composizione e competenze è quella espressamente suggerita anche nelle Linee Guida di Confidustria[18].

Si riporta di seguito lo Statuto OdV di Sicil Tecno Plus (il Regolamento OdV sarà predisposto dall'OdV nell'ambito della sua autonomia di azione e di regolamentazione attività).

❖ **STATUTO dell'Organismo di Vigilanza**

Articolo 1 - Scopo ed ambito di applicazione

1. È istituito presso Sicil Tecno Plus srl 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 STP è composto da due professionisti esterni.

2. L'Organismo di Vigilanza provvede a nominare il suo Presidente, cui compete l'espletamento delle formalità relative alla convocazione, alla fissazione degli argomenti da trattare e allo svolgimento delle riunioni/sessioni.

3. La nomina dell'Organismo di Vigilanza, da parte dell'Organo Amministrativo, deve essere resa nota a ciascun componente nominato e da questi essere formalmente accettata.

Articolo 3 - Requisiti di professionalità e di onorabilità

1. I componenti dell'Organismo di Vigilanza devono 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,

[18] «*È auspicabile che almeno taluno dei membri dell'Organismo di Vigilanza abbia competenze in tema di analisi dei sistemi di controllo e di tipo giuridico e, più in particolare, penalistico. Infatti, la disciplina in argomento ha natura sostanzialmente punitiva e lo scopo del modello è prevenire la realizzazione di reati. È dunque essenziale la conoscenza della struttura e delle modalità di consumazione dei reati …… Quanto all'attività ispettiva e di analisi del sistema di controllo, la giurisprudenza ha fatto riferimento - a titolo esemplificativo - al campionamento statistico; alle tecniche di analisi, valutazione e contenimento dei rischi, (procedure autorizzative; meccanismi di contrapposizione di compiti; ecc.); al flow-charting di procedure e processi per l'individuazione dei punti di debolezza; alla elaborazione e valutazione dei questionari; alle metodologie per l'individuazione di frodi. Si tratta di tecniche che possono essere utilizzate per verificare che i comportamenti quotidiani rispettino effettivamente quelli codificati: in via preventiva, per adottare - all'atto del disegno del Modello 231 e delle successive modifiche - le misure più idonee a prevenire, con ragionevole certezza, la commissione dei reati (approccio di tipo consulenziale); oppure ancora, a posteriori, per accertare come si sia potuto verificare il reato presupposto (approccio ispettivo)* » (Linee Guida Confindustria).

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 di un membro dell'OdV, provvede, il prima possibile, alla nomina del sostituto. L'incarico di componente dell'OdV del nuovo membro avrà termine contestualmente alla scadenza dei componenti già in carica.

5. In caso di cessazione dall'incarico di Presidente OdV, il nuovo Presidente verrà nominato subito dopo aver ricomposto l'OdV e sarà eletto tra i componenti dell'Organismo. Nel periodo di *vacatio*, sarà il segretario dell'OdV a farne le veci.

6. Ciascun componente dell'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. I componenti dell'Organismo di Vigilanza devono 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. I componenti dell'Organismo di Vigilanza sono tenuti 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 il Presidente o un componente dell'Organismo di Vigilanza incorrano 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 dei protocolli previsti 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. L'Organismo di Vigilanza deve riunirsi con frequenza adeguata a garantire la continuità dei compiti previsti (non meno di 3 volte all'anno) e comunque ogni qual volta se ne presenti la necessità e/o opportunità.

3. 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.

4. Agli eventuali consulenti di cui al precedente comma è richiesto il rispetto degli obblighi di diligenza previsti per i componenti dell'Organismo di Vigilanza.

Articolo 9 - Poteri

1. L'OdV 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 D.Lgs. 231/01.

2. Per esercitare efficacemente le proprie funzioni, l'Organismo di Vigilanza:

a) deve avere libero accesso presso tutte le funzioni della società - senza necessità di alcun consenso preventivo - onde ottenere ogni informazione o dato ritenuto necessario per lo svolgimento dei compiti previsti dal D.Lgs. 231/01;

b) ha la facoltà di avvalersi del supporto e della collaborazione delle funzioni interne, alle quali potrà essere chiesto di attivarsi per svolgere compiti strettamente collegati e funzionali alle attività di controllo;

c) può avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di consulenti esterni. Ha, pertanto, la facoltà di chiedere e/o assegnare a soggetti terzi, in possesso delle competenze specifiche necessarie, incarichi di consulenza e/o di assistenza al fine di poter svolgere le attività di propria competenza. A tal fine e nel contesto delle procedure di formazione del budget aziendale, l'Organo Amministrativo deve obbligatoriamente approvare una dotazione di risorse finanziarie per l'OdV (budget), della quale lo stesso potrà disporre in totale autonomia per ogni esigenza necessaria al corretto svolgimento dei suoi compiti;

3. L'OdV dovrà essere costantemente informato dal management societario sugli aspetti dell'attività aziendale che possono esporre la Società al rischio di commissione di uno dei reati presupposti dal D.Lgs. 231/2001.

4. Al fine di consentire il corretto svolgimento dell'attività dell'OdV, la Società e i suoi dipendenti/responsabili dovranno rispettare gli obblighi, i criteri ed i tempi, dettati in materia di flussi Informativi.

Articolo 10 - Flussi informativi

1. I flussi informativi provenienti dall'Organismo di Vigilanza nei confronti dell'Organo Amministrativo sono: a) di natura continuativa, in occasione delle sessioni OdV e dell'invio dei relativi verbali nonché in occasione dell'invio della relazione annuale, riassuntiva dell'attività svolta e delle valutazioni riportate in ordine alle eventuali criticità, ai comportamenti ed eventi societari a rischio di reato, alla maggiore o minore efficacia del MOGC; b) di natura occasionale, al fine di segnalare eventuali violazioni del Modello 231 o del Codice Etico e di Comportamento emerse durante lo svolgimento delle verifiche, nonché al fine di avanzare proposte di incontri/riunioni con una o più funzioni societarie per l'eventuale analisi di situazioni, problemi o livelli di criticità ex D.Lgs. 231/2001.

2. I flussi informativi provenienti dalla Società nei confronti dell'Organismo di Vigilanza costituiscono un'asse portante del sistema di controllo societario, una componente essenziale del Modello 231 e dell'attività di monitoraggio dello stesso OdV, un obbligo legislativamente stabilito dall'art. 6 del D.Lgs. 231/2001, in base al quale il Modello 231 deve «prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli».

3. L'Organismo di Vigilanza deve essere messo in grado di svolgere la sua corretta attività di controllo e di ausilio preventivo anti-illiceità societarie attraverso un adeguato sistema strutturato di flussi informativi proveniente da tutte le funzioni aziendali.

4. I flussi informativi nei confronti dell'Organismo di Vigilanza dovranno essere: chiari ed inequivoci nella loro rappresentazione; idonei a rappresentare compiutamente l'evento riportato; attendibili, completi e genuini, nel senso che il dato riportato dovrà essere completo e aderente a quello originale; aggiornati, nel senso che le informazioni dovranno essere il più possibile attuali rispetto al periodo di osservazione; obbligatori e tali da poterne derivare responsabilità di natura disciplinare in caso di inottemperanza, parziale o totale.

5. I flussi informativi nei confronti dell'OdV si distinguono in flussi periodici e flussi ad hoc:

a) I flussi informatici periodici, o di cd. reporting periodico, sono quelli provenienti da: Organo

Amministrativo (Verbali, Delibere, Disposizioni di Servizio di particolare rilevanza, …); Responsabili di Unità Operative (su attività ordinaria e straordinaria, a cadenza periodico-ordinaria eventualmente da concordare tra OdV e Organo Amministrativo); Organi di Controllo interno, su specifica e motivata richiesta dell'OdV.

b) I flussi informativi straordinari e/o ad hoc sono quelli provenienti da tutti gli organi sociali, funzioni, responsabili/dipendenti, riguardanti: gli accessi delle Autorità Istituzionali; le ispezioni o le perquisizioni o i sequestri da parte delle succitate Autorità Istituzionali; le Richieste di Rinvio a Giudizio o i Decreti di Citazione a Giudizio da parte dell'Autorità Giudiziaria Penale; gli atti di citazione in giudizio civile di particolare rilevanza sociale; le eventuali denunce/segnalazioni, anonime o non; le convocazioni da parte delle Autorità Istituzionali; le notizie relative ai procedimenti disciplinari svolti e alle eventuali sanzioni irrogate, ovvero i provvedimenti di archiviazione di tali procedimenti con le relative motivazioni, qualora gli stessi siano legati alla commissione di reati o di violazione delle regole di comportamento o procedurali del MOGC; gli eventi a carattere straordinario e/o eccezionale (soprattutto in materia ambientale o di sicurezza sui luoghi di lavoro); tutte le situazioni fattuali a carattere straordinario o eccezionale.

c) Ulteriore flusso informativo ad hoc nei confronti dell'Organismo di Vigilanza è quello riguardante le eventuali segnalazioni di reato o di condotte illecite ex D.Lgs. 231/2001, o di comportamenti in violazione del Codice Etico, o di ritorsioni da whistleblowing, eventualmente inviate anche in forma anonima.

6. In presenza di alcuna delle segnalazioni di cui al punto 5.c (whistleblowing), l'OdV dovrà valutarle con discrezionalità e responsabilità, attivando tutti gli approfondimenti ritenuti necessari, effettuando le dovute indagini e adoperandosi affinché venga definito quanto previsto dal sistema sanzionatorio aziendale, ma, soprattutto, dovrà garantire che le informazioni acquisite saranno trattate in modo da garantire: a) la riservatezza e l'anonimato del segnalante; b) la tutela del segnalante da qualsiasi forma di ritorsione, penalizzazione, discriminazione (fatti salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente e/o in mala fede); c) il rispetto di una specifica e strutturata procedura di trasmissione da parte del Responsabile dell'area Informatica.

7. L'Organismo di Vigilanza ha diritto di stabilire, di concerto con l'Organo Amministrativo, la tempistica e le modalità di trasmissione dei flussi informativi, da comunicare alle relative aree operative o funzioni societarie alla stregua di disposizione di servizio dal carattere di inderogabilità.

8. L'Organismo di Vigilanza ha diritto di chiedere e di ottenere altri e diversi flussi informativi specifici (a carattere periodico od occasionale) in presenza di ritenute emergenze di rischio o particolari criticità aziendali oltre a quelli riportati nella tabella della pagina seguente.

FLUSSI INFORMATIVI verso l'OdV

Descrizione flusso informativo	Funzione Referente	Tempistica
Delibere dell'Organo Amministrativo Delibere notarili Operazioni societarie Deleghe di funzione e procure e relativi aggiornamenti Comunicazioni e rapporti con Soggetti Pubblici per l'ottenimento di autorizzazioni e licenze e per lo svolgimento di attività regolate dalla legge	Amministratore Unico	AD EVENTO
Procedimenti penali Cause Civili Contenziosi Amministrativi Contenziosi Tributari Pagamento contravvenzioni e Contenziosi contravvenzionali Accordi Transattivi	Amministratore Unico	AD EVENTO
Bilancio	Amministratore Unico	ANNUALE
Flussi finanziari e contabili (fatture emesse, incassate, ricevute e pagate, disponibilità di cassa)	Responsabile Amministrazione	TRIMESTRALE
Flussi e adempimenti fiscali	Responsabile Amministrazione	AD EVENTO
Gestione di rimborsi spese, anticipi e spese di rappresentanza (Rimborsi spese a dipendenti e assimilabili superiori a € 500)	Responsabile Amministrazione	A RICHIESTA ODV
Gestione di donazioni, sponsorizzazioni, omaggi e liberalità (Elenco spese di rappresentanza superiori a € 500)	Responsabile Amministrazione	SEMESTRALE
Consulenze e Incarichi Professionali	Responsabile Risorse Umane	SEMESTRALE
Segnalazioni inoltrate alla Società da Dipendenti Azioni Disciplinari	Responsabile Risorse Umane	AD EVENTO
Selezione, Assunzione e gestione del personale dipendente e dei collaboratori (Elenco assunzioni e cessazioni avvenute nel periodo di riferimento; Avanzamenti di carriera e variazione remunerative del personale.	Responsabile Risorse Umane	TRIMESTRALE
Partecipazione gare di appalto e committenze private	Responsabile Gare	TRIMESTRALE
Albo fornitori Flusso analitico acquisti (RdA, OdA, Contratto, Destinazione Cantiere, Movimenti Magazzino) Elenco contratti e forniture	Responsabile Acquisti	TRIMESTRALE
Gestione, amministrazione e manutenzione degli apparati ITC, dei database e delle applicazioni	Responsabile ICT	SEMESTRALE
Sicurezza sui Luoghi di Lavoro (Elenco Cantieri; Aggiornamento DVR; DUVRI; POS; Formazione Lavoratori; Adempimenti 81/2008, etc.)	RSPP / eventuale Responsabile Sicurezza ex art. 16 D.Lgs. 81/2008	TRIMESTRALE
Sicurezza sui Luoghi di Lavoro (infortuni - quasi infortuni)	RSPP / eventuale Responsabile Sicurezza ex art. 16 D.Lgs. 81/2009 / Preposti	AD EVENTO
Verifiche, accertamenti e ispezioni da parte dei Soggetti Pubblici preposti e delle Autorità Pubbliche di vigilanza (Dettaglio delle visite ispettive ricevute e delle eventuali criticità riscontrate)	Responsabili di funzione	AD EVENTO
Fatti inerenti i Sistemi di Certificazioni (richieste, conformità, ispezioni, rilascio aggiornamenti)	Responsabile SGI	SEMESTRALE
Ogni informazione, proveniente anche da terzi, attinente all'attuazione non corretta o ad eventuali violazioni del Modello 231	Tutti i dipendenti	AD EVENTO
Situazioni di criticità che potenzialmente potrebbero configurare o concretizzare reati ambientali	Tutti i dipendenti	AD EVENTO
Eventuali pressioni o condizionamenti subiti durante un procedimento penale	Tutti i dipendenti	AD EVENTO

4. APPROVAZIONE E AGGIORNAMENTO DEL MODELLO 231

L'adozione e l'efficace attuazione del Modello costituiscono - ai sensi dell'art. 6, comma I, lett. a) del D.Lgs. 231/2001 - atti di competenza e di emanazione dell'Organo Amministrativo. Viene, in particolare, rimesso all'Organo Amministrativo il potere di approvare e recepire, mediante apposita delibera, sia il *Modello di Organizzazione, Gestione e Controllo*, sia il *Codice Etico.* Una volta approvati, rappresentano obbligatoria attività di manutenzione, del Modello di Organizzazione, Gestione e Controllo e del Codice Etico, le attività di:

- *Verifica*;
- *Aggiornamento.*

In particolare il MOGC - anche su impulso e coordinamento dell'Organismo di Vigilanza - dovrà essere soggetto a due tipi di verifiche:

- *verifiche sull'osservanza del Modello*, e sulle principali attività poste in essere nelle aree di attività cd. "sensibili";
- *verifiche sul funzionamento del Modello,* sulla sua validità ed efficacia o sulle eventuali correzioni da effettuare sulla base: delle indicazioni dell'Organismo di Vigilanza; delle segnalazioni ricevute nel corso dell'anno da parte dell'Organismo di Vigilanza; delle proposte da parte di tutti i soggetti che operano "con" o "per" Sicil Tecno Plus srl.

Il MOGC e il Codice Etico e di Comportamento dovranno essere – obbligatoriamente e costantemente - aggiornati.

L'aggiornamento del MOGC è obbligatorio soprattutto in corrispondenza di:

- mutamenti di natura aziendale;
- innovazioni di natura normativa;
- evidenziazione di punti di criticità del Modello;
- indicazioni e suggerimenti dell'Organismo di Vigilanza.

5. I DESTINATARI DEL MODELLO 231

Per tracciare con precisione l'area di operatività del Modello, è innanzitutto necessario individuarne i "*Destinatari",* 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 *Sicil Tecno Plus srl*, a prescindere cioè dalle specifiche peculiarità delle singole categorie, possiamo senz'altro inserire tra i destinatari del Modello 231 della Società i seguenti soggetti:

- i componenti dell'Organo Amministrativo;
- il personale apicale in genere;
- i collaboratori, anche esterni e a titolo occasionale (nei limiti delle funzioni svolte nell'interesse della Società);
- i dipendenti e gli operai, anche a titolo occasionale;
- i consulenti e/o i professionisti chiamati a svolgere uno o più incarichi (nei limiti delle funzioni svolte nell'interesse della Società);
- i fornitori e gli outsourcers (nei limiti delle prestazioni rese nell'interesse della Società);
- i subappaltatori e i sub fornitori (nei limiti delle prestazioni rese in regime di subappalto e subfornitura);
- le persone giuridiche che eventualmente intrattengano con la Società rapporti di lavoro in termini di collaborazione, Associazione Temporanea di Imprese, joint venture, partnership, qualunque forma di cooperazione o di co-ausilio Societario (nei limiti dei rapporti intrattenuti nell'interesse della Società).

Una annotazione di particolare importanza è che rientrano nella categoria dei Destinatari, sempre nei limiti delle funzioni svolte nell'interesse della società:

- gli appartenenti alle strutture o enti che si occupano dei controlli sulla Società;
- i membri dell'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[19].

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

[19] 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.

Avuto specifico riferimento ad alcuna delle succitate categorie, si reputa necessaria qualche puntualizzazione.

Per ciò che riguarda gli **amministratori, i dirigenti e il personale apicale**, l'art. 5 del D.Lgs. 231/2001, al primo comma lett. a), è chiaro nello statuire: *"L'ente è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso".*

In tema la giurisprudenza chiarisce: "*La nozione di soggetto apicale di un ente viene definita dall'esercizio formale di funzioni di rappresentanza, amministrazione o direzione, mentre l'esercizio di fatto per essere rilevante deve avere riguardo cumulativamente alle funzioni di gestione e controllo, volendosi includere tra i vertici solo quei soggetti che esercitano un penetrante dominio sull'ente. In assenza di una definizione delle citate funzioni di amministrazione, rappresentanza e direzione, si possono utilizzare in via interpretativa le norme dettate in proposito in altre branche dell'ordinamento interno, così da ricostruire il concetto di amministrazione come legato al potere di gestione e controllo delle risorse materiali dell'ente, il concetto di direzione come legato al potere di gestione e controllo del personale dell'ente, il concetto di rappresentanza come legato alla formazione, manifestazione all'esterno e alla ricezione della volontà dell'ente in relazione agli atti negoziali"* (Tribunale Milano, sez. XI, 26 giugno 2008).

Sulla necessità di individuare le precise cariche amministrative e/o gestionali si è pronunciata anche la Suprema Corte a Sezioni Unite: "*… la responsabilità dell'ente per gli illeciti (nella specie, manipolazione del mercato) commessi nel suo interesse o a suo vantaggio, prevista dall'art. 187 quinquies d.lg. 24 febbraio 1998 n. 58, postula l'accertamento della qualifica gestoria apicale del soggetto agente, ovverosia dello svolgimento da parte di quest'ultimo di funzioni di rappresentanza, amministrazione o direzione dell'ente, in virtù delle quali il comportamento illecito possa ascriversi ad un'esplicita manifestazione di politica aziendale, e non è pertanto configurabile nell'ipotesi in cui la condotta illecita sia stata tenuta in esecuzione di un incarico di consulenza professionale*" (Cass. Civ., Sez. Un., 30 settembre 2009, n. 20936).

In definitiva, le persone che rivestono le funzioni di rappresentanza, di amministrazione, di direzione dell'ente o di una sua unità organizzativa, sono certamente responsabili in prima persona dei reati commessi nell'interesse o a vantaggio della Società (si parla, in questi casi, di "amministratori infedeli"), tanto quanto lo è la Società, per gli stessi eventuali reati, in via amministrativa e sul piano squisitamente aziendale (cioè ai fini dell'applicabilità a suo carico delle sanzioni e misure interdittive previste dal D.Lgs. 231/2001).

Altrettanto pacifico è il concetto di amministratore o di dirigente "*di fatto*" – ossia di colui che, pur non rivestendo alcuna carica o potere direzionale sul piano formale, lo eserciti in via concreta e fattuale - pienamente equiparato all'amministratore o dirigente di diritto.

I **soci** della Società, sono da considerare a tutti gli effetti Destinatari del MOGC 231.

I **dipendenti** rientrano a tutti gli effetti nel paradigma normativo dell'art. 5, co.1, lett. b) del D.Lgs. 231/2001, quali "*persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui sopra*, ossia amministratori, dirigenti e personale apicale.

Ne deriva il loro inserimento di diritto nella categoria dei Destinatari, quali soggetti in grado di commettere reati in favore o nell'interesse della Società, nonché persone per le quali quest'ultima rimane esposta al rischio di rispondere - a titolo di "responsabilità amministrativa" - del loro eventuale operato illecito.

Da notare che, proprio nel caso dei dipendenti, la Società è soggetta ad un duplice livello di responsabilità:

a) *"amministrativa*", all'interno di un processo penale ed ai sensi del D.Lgs. 231/2001, con le note sanzioni pecuniarie e misure interdittive;

b) "*civile*", sia nell'ambito di un giudizio civile *ex* art. 2049 c.c. ("*responsabilità dei padroni e committenti"*), sia in sede di processo penale *ex* art. 83 c.p.p., quale "responsabile civile" per il fatto dell'imputato.

Entrambe le due succitate forme di responsabilità, univocamente a carico della Società, sono idonee a concorrere giuridicamente con la responsabilità strettamente personale del singolo dipendente. Emblematico, al riguardo, il caso in cui il dipendente sia chiamato a rispondere quale responsabile di un reato colposo in materia di infortuni sul lavoro.

L'eventuale condotta illecita del dipendente comporterà a catena: la violazione dei "reati presupposti" dall'art. 25 septies del D.Lgs. 231/2001; il processo penale a suo carico per i predetti "reati presupposti"; la chiamata in causa della Società, sempre nell'ambito dello stesso processo penale, quale *padrone e committente* e dunque "responsabile civile" per il fatto del dipendente-imputato (si ricordi, peraltro, che in questi casi la responsabilità civile è di tipo oggettivo e prescinde dall'accertamento della colpa del "committente"); la chiamata della Società, ancora una volta nello stesso processo penale in cui è già presente come "responsabile civile", per l'eventuale ed ulteriore responsabilità amministrativa ai sensi del D.Lgs. 231/2001.

Tra i criteri esegetici utilizzati per meglio comprendere gli esatti confini di una eventuale duplice responsabilità "da" D.Lgs. 231/2001 – quella penale e personale dei dipendenti e collaboratori in relazione ad un reato commesso nell'interesse della Società; quella amministrativa ed aziendale della Società, per lo stesso reato commesso nel suo interesse dai predetti soggetti – il più importante è certamente quello della "*immedesimazione organica*".

In base a questo principio e parametro giuridico, Sicil Tecno Plus srl potrà essere considerata responsabile (a titolo "amministrativo" ed ai sensi del D.Lgs. 231/2001) dell'operato dei suoi dipendenti e collaboratori unicamente se, e nella misura in cui, la condotta illecita posta in essere dagli stessi soggetti sia immediatamente e direttamente *"riferibile alla Società*".

Si ricordi, a titolo di completezza, che il concetto di "*immedesimazione organica*" nasce nell'ambito del diritto amministrativo, specificamente legato alla ratio dell'art. 28 della Costituzione: "*Affinché ricorra la responsabilità della P.A. per un fatto lesivo posto in essere dal proprio dipendente - responsabilità il cui fondamento risiede nel rapporto di immedesimazione organica - deve sussistere, oltre al nesso di causalità fra il comportamento e l'evento dannoso, anche la riferibilità all'amministrazione del comportamento stesso, la quale presuppone che l'attività posta in essere dal dipendente sia e si manifesti come esplicazione dell'attività dell'ente pubblico, e cioè tenda, pur se con abuso di potere, al conseguimento dei fini istituzionali di questo nell'ambito delle attribuzioni dell'ufficio o del servizio cui il dipendente è addetto"* (Cass. civ., Sez. III, 25 maggio 2007, n. 20986; conf. Cass., civ., Sez. III, 8 ottobre 2007, n. 20986; Id., SS.UU., 23 novembre 2007 n. 24397; Id. pen. Sez. III, dep. 6 luglio 2007, n. 26054).

L'istituto della "immedesimazione organica" è stato, altresì, esteso dalla Suprema Corte di Cassazione al settore civilistico (v. per tutte Cass. civ., Sez. II, 29 settembre 2003, n. 14455).

Da ultimo ed alla stregua di vera e propria interpretazione autentica, si consideri peraltro che lo stesso istituto è stato attratto nella sfera dei criteri di esegesi applicativa dei Modelli di Organizzazione, Gestione e Controllo per il tramite della Relazione Ministeriale di accompagnamento al D.Lgs. 231/2001: "*Ribadito ancora una volta che anche la materia dell'illecito penale-amministrativo è assoggettata al dettato costituzionale dell'art. 27, già la teoria della c.d. immedesimazione organica consente di superare le critiche che un tempo ruotavano attorno alla violazione del principio di personalità della responsabilità penale, ancora nella sua accezione "minima" di divieto di responsabilità per fatto altrui. Vale a dire: se gli effetti civili degli atti compiuti dall'organo si imputano direttamente alla Società, non si vede perché altrettanto non possa accadere per le conseguenze del reato, siano esse penali o - come nel caso del decreto legislativo - amministrative. Anzi, a rigore, questa soluzione si profila quasi necessitata sul piano logico (dal momento che assicura la corrispondenza tra chi commette l'illecito e chi ne paga le conseguenze giuridiche), oltre che auspicabilmente idonea, su quello pratico …"*.

In conclusione, la Società potrà essere considerata "amministrativamente responsabile" degli eventuali reati posti in essere dai suoi collaboratori e dipendenti solo se gli stessi reati:

- siano stati commessi nell'esercizio delle specifiche funzioni assegnate dalla Società;
- siano direttamente imputabili alla Società, quale espressione del principio di immedesimazione organica;

- non siano frutto di elusione fraudolenta del Modello di Organizzazione, Gestione e Controllo.

Per ciò che concerne **i fornitori e gli outsourcers** - non importa se persone fisiche o giuridiche (evenienza che potrebbe solo presupporrebbe una maggiore autonomia ed organizzazione di mezzi e di persone) – *Sicil Tecno Plus srl* li considera *parzialmente* Destinatari del Modello di Organizzazione, Gestione e Controllo adottato. Sebbene i fornitori non esercitino in via diretta l'attività di *Sicil Tecno Plus srl,* gli stessi possono certamente considerarsi "*sottoposti alla direzione o alla vigilanza*" di amministratori e di personale apicale della Società laddove siano chiamati a prestare una determinata attività accessoria e di ausilio, e ciò seguendo le specifiche direttive, domande e standard richiesti dalla committente. Si pensi, al riguardo, all'attività dei fornitori o tecnici chiamati a fornire e a gestire sistemi hardware e software (materia cui sono correlati molteplici reati informatici), o mezzi, materiale e strumenti di complemento per la gestione di una commessa avente ad oggetto un appalto di beni o di servizi.

Sono tutte situazioni in cui *Sicil Tecno Plus srl* ha pieno diritto di chiedere che siano rispettate le proprie regole di natura etica e morale (interamente riportate nel Codice Etico), nonché i protocolli e gli standard di legalità specificamente indicati nel proprio Modello di Organizzazione, Gestione e Controllo.

É solo al di là di questo specifico ambito di lavoro condotto insieme che il fornitore sarà libero di muoversi liberamente in base ai propri ed autonomi assetti regolamentari, senza dovere soggiacere a nessuno Modello di Organizzazione, Gestione e Controllo che non sia quello della sua personale struttura societaria.

Tra le categorie dei destinatari di maggiore importanza, riveste senz'altro un posto di primo piano quella dei **subappaltatori,** tanto più che si tratta di persone fisiche e giuridiche cui *Sicil Tecno Plus srl* affida delle commesse aggiudicatesi nel sistema delle gare pubbliche.

La delicatezza dei rapporti con tali soggetti (nei cui confronti appare, dunque, opportuno muoversi in regime di *"cautela avanzata")* risiede nel fatto che - ad oggi - la valutazione giurisprudenziale in ordine alle eventuali responsabilità di natura civile/penale/amministrativa, derivanti da una possibile non corretta esecuzione o svolgimento dei servizi appaltati, o da un infausto danno di natura extracontrattuale, è tutt'altro che unanime, pacifica e consolidata.

Una premessa di assoluta centralità è che la tematica sulle predette, specifiche, responsabilità di natura extracontrattuale opera su un piano completamente diverso rispetto a quella della eventuale *corresponsabilità solidale* di natura fiscale o contributiva-previdenziale in capo all'appaltatore.

Quest'ultimo tipo di responsabilità è regolata dall' art. 29 del D.Lgs. 276/2003 (delegato dalla Legge 30/2003), che ha introdotto un regime di responsabilità solidale dell'appaltatore verso il subappaltatore in ordine alle ritenute fiscali sui redditi di lavoro dipendente e che, a sua volta, è stato modificato dall'attuale D.Lgs. 175/2014.

Tale specifica forma di responsabilità *non* riguarda però - in alcun modo - il tema del diverso tipo di responsabilità per eventuali fatti illeciti addebitabili al subappaltatore, e quindi della eventuale posizione di corresponsabilità in capo all'appaltatore.

Qui valgono regole tendenzialmente antitetiche, atteso che il regime civilistico del contratto di appalto (e quindi di subappalto) di cui agli artt. 1655-1677 c.c. si basa sul fermo principio secondo il quale l'appalto presuppone: a) l'affidamento in autonomia di una determinata opera/servizio; b) la prestazione del servizio o dell'esecuzione dell'opera subappaltata attraverso una propria organizzazione di mezzi e di risorse; c) il divieto di intromissione gestoria da parte dell'appaltatore.

Ciò comporta un duplice tipo di problema/conseguenza:

a) la necessità di individuare (e dunque prevenire ed evitare) le situazioni in cui le responsabilità del subappaltatore potrebbero estendersi anche all'appaltatore;

b) l'esigenza di predisporre un sistema organizzativo che, da un lato possa ridurre questo specifico rischio, dall'altro eviti però di produrre l'effetto opposto, e cioè di scaricare sull'appaltatore l'eventuale responsabilità del subappaltatore proprio in ragione di una asserita *"intromissione gestoria"*, v. quella che ad avviso della giurisprudenza finisce per snaturare lo stesso contratto di "subappalto", rendendo il

subappaltatore una sorta di "*nudus minister*" e facendo ricadere tutte le responsabilità sull'appaltatore anziché sul subappaltatore (v. tra le tante Cass. Civ., Sez. III, 10 aprile 2014 n.8410).

Corollario dell'una o dell'altra evenienza è l'eventuale affermazione, o negazione, di una possibile, o meno, responsabilità solidale dell'appaltatore *ex* art. 2049 cc. (v. *la responsabilità dei padroni e committenti*, che peraltro è a carattere rigorosamente oggettivo).

In materia - a parte il divieto di "intromissione gestoria", in ordine al quale la giurisprudenza è assolutamente unanime nel confermare l'inderogabilità del principio di natura codicistica - il quadro giurisprudenziale di riferimento è assolutamente equivoco e non conforme.

Più da vicino, in parecchie sentenze viene affermato che: *«l'autonomia dell'appaltatore o sub-appaltatore, il quale esplica la sua attività nell'esecuzione dell'opera assunta con propria organizzazione ed apprestandone i mezzi, nonchè curandone le modalità ed obbligandosi verso il committente o subappaltante a prestargli il risultato della sua opera, esclude ogni rapporto istitutorio tra committente ed appaltatore, con la conseguenza dell'inapplicabilità dell'art. 2049 c.c.»* (Cass. Pen., Sez. 4, 14 gennaio 2010, n. 1479).

Nella stessa sentenza n. 1479 ora citata viene però affermato anche: «*l'appaltatore* (n.d.s. il subappaltatore, ai fini della nostra disamina) *deve, quindi, di regola ritenersi unico responsabile dei danni derivanti a terzi dall'esecuzione dell'opera, salva la corresponsabilità del committente* (n.d.s. dell'appaltatore, ai fini della nostra disamina) *in caso di specifiche violazioni di regole di cautela nascenti ex art. 2043 c.c.*» (Cass. Civ. 10 aprile 2014 n. 8410; Id., Sez. 3, 29 ottobre 2015, n. 286; Id., Sez. 3, 15 ottobre 2013, n. 25758; Cons. St., sez. VI, 28 ottobre 2010, n. 7635)

Per completezza, l'art. 2043 c.c. è quella di norma di salvaguardia generale che stabilisce: «*Qualunque fatto doloso o colposo che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno».*

Sempre al fine di toccare con mano l'eterogeneità di opinioni sul punto, altra importante sentenza sostiene (a specifico proposito della responsabilità per violazione della sicurezza sui luoghi di lavoro ma attraverso una proclamazione di principio assolutamente generica e generale): «è *vero che nel caso di contratto di appalto non può essere posta in dubbio la posizione di garanzia del committente* (n.d.s. dell'appaltatore nel caso di subappalto) *il quale ha l'obbligo di accertare la "idoneità tecnico professionale" dell'impresa appaltatrice, quello di fornire alla stessa dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui questa è destinata ad operare (sono i rischi derivanti dalla peculiarità dell'ambiente di lavoro, che solo il titolare può conoscere appieno) e sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività, nonchè l'ulteriore obbligo di promuovere la "cooperazione" ed il "coordinamento" ai fini dell'attuazione delle misure precauzionali …. La violazione dei suindicati obblighi comportamentali può fondare una (cor)responsabilità (anche) del datore di lavoro/committente per infortuni che abbiano riguardato i lavoratori dipendenti dell'appaltatore … Deve, pertanto, affermarsi il principio di diritto secondo il quale il committente* (n.d.s. l'appaltatore in caso di subappalto) *qualora l'evento si colleghi casualmente anche alla sua colposa omissione ed in quei casi in cui l'omessa adozione delle misure di prevenzione prescritte sia immediatamente percepibile cosicchè il committente medesimo sia in grado di accorgersi dell'inadeguatezza delle stesse senza particolari indagini … Ne consegue che, ai fini della configurazione della responsabilità del committente, occorre verificare in concreto quale sia stata l'incidenza della sua condotta nell'eziologia dell'evento … nonchè alla agevole ed immediata percepibilità da parte del committente di situazioni di pericolo*» (Cass. Pen., Sez. 4 18 dicembre 2014, n. 52658; conf. Cass. Sez. 4, 18 gennaio 2012, n. 3563; Id. Sez. 4, 15 dicembre 2005, n. 5977,Cimenti; Id. Sez. 3, 24 ottobre 2013, n. 50996).

Si consideri a quest'ultimo riguardo che, anche ad avviso di Corte di Cassazione, sez. VI Penale - sentenza n. 17049/11, incombe sul committente (n.d.s. sull'appaltatore in caso di subappalto) «*un dovere di controllo di origine non contrattuale al fine di evitare che dall'opera derivino lesioni del principio del "neminem ledere", idonee, queste si, ad eventualmente corresponsabilizzare il committente* (n.d.s. l'appaltatore in caso di subappalto) *in base al precetto di cui all'art. 2043 c.c.*».

Secondo questa logica, viene ad esempio considerato punibile – in materia di delega di funzioni ma il principio è assolutamente valevole ai nostri fini – il caso in cui non vi sia stata una incolpevole estraneità alle inadempienze del delegato, o vi sia stata una informazione (anche ufficiosa) di condotte censurabili, così da potersi ipotizzare un atteggiamento di inerzia o di colpevole tolleranza in capo ai

titolari delle posizioni di garanzie (Cass. pen. III, 27 giugno 2002, n. 32151; Id., III, 5 novembre 2002, n. 246).

Di avviso nettamente contrario è Cass. pen., III sez. pen, sentenza n. 11029/2015, secondo la quale, a proposito della gestione dei rifiuti: a) *«tranne nel caso di un diretto concorso nella commissione del reato, non può ravvisarsi alcuna responsabilità ai sensi dell'articolo 40, comma 2 cod. pen. per mancato intervento al fine di impedire violazioni della normativa in materia di rifiuti da parte della ditta appaltatrice* (n.d.s. subappaltatrice ai nostri fini)»; b) «*l'appaltatore* (n.d.s. il subappaltatore ai nostri fini), *in ragione della natura del rapporto contrattuale, che lo vincola al compimento di un opera o alla prestazione di un servizio con organizzazione dei mezzi necessari e con gestione a proprio rischio è, di regola, il produttore del rifiuto; su di lui gravano, quindi, i relativi oneri*».

A loro volta, di avviso esattamente antitetico a quest'ultima affermazione giurisprudenziale: Cass. 4957/2000, Cass. 24347/2003, Cass. 36963/2005, secondo le quali «*è produttore dei rifiuti colui nel cui interesse viene svolta l'attività da cui traggono origine i rifiuti*» (v. il committente o l'appaltatore nei confronti del subappaltatore).

Sulla scorta di quanto sin qui delineato è certamente opportuno che Sicil Tecno Plus srl:

a) "personalizzi" il contratto di subappalto integrandolo di prescrizioni e presupposti di legalità in linea con il presente Modello di Organizzazione, Gestione e Controllo, nonché con eventuali ed ulteriori protocolli di legalità;

b) affidi ad un suo dipendente/funzionario una specifica *delega di funzione* avente ad oggetto:

- la valutazione preventiva dei rischi in fase esecutiva (v. soprattutto in presenza di commesse subappaltate dalla prevedibile rischiosità ambientale);
- il controllo sullo svolgimento dei lavori, ma nei limiti del richiamato art. 1622 c.c.;

c) riconsideri/ritocchi le sue procedure di controllo in materia di subappalto, cercando di trovare un giusto punto di equilibrio tra il divieto di intromissione gestoria (che, come prima detto, potrebbe far diventare il subappaltatore un semplice *nudus minister* dell'appaltatore, liberandolo in tal modo dalle sue specifiche e dirette responsabilità) e l'esigenza di un controllo ab externo in grado di abbassare il livello di rischio, soprattutto in fase esecutiva.

Allegato - WHISTLEBLOWING - Procedura per l'attuazione delle Segnalazioni ex D.Lgs. 24/2023

1. PREMESSA E RIFERIMENTI NORMATIVI

Il Decreto Legislativo n. 24 del 10 marzo 2023, 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*" (di seguito il "**Decreto**"), ha esteso in maniera significativa il perimetro di applicazione della disciplina in materia di segnalazioni, già regolato, in ambito privatistico, 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*), nonché, per ciò specificamente riguarda le Società dotate di Modello 231, dall'art. 6, commi 2 *bis*, 2 *ter* e 2 *quater* del D.Lgs. 231/2001.

A quest'ultimo riguardo, con il D.Lgs. 24/2023 sono stati abrogati gli ex commi 2 ter e 2 quater dell'art. 6 del D.Lgs. 231/2001 e lasciato 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».*

Il Decreto 24/2023 ha riformato compiutamente la materia e: a) individuato e disciplinato la posizione dei soggetti segnalanti; b) indicato l'oggetto delle segnalazioni di violazione; c) previsto l'istituzione di specifici canali di segnalazione; d) stabilito gli adempimenti e le tutele che le Società sono tenute a implementare e garantire, definendone anche i criteri e le tempistiche di adeguamento.

Poiché la gestione delle segnalazioni può comportare la raccolta e il trattamento di dati personali, trova applicazione la normativa in materia di protezione dei dati personali: v. il Regolamento 2016/679 del Parlamento europeo e del Consiglio, datato 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "**GDPR**"), e il Decreto Legislativo 30 giugno 2003, n. 196 modificato/aggiornato dal Decreto Legislativo 10 agosto 2018, n. 101, (di seguito congiuntamente denominati "**Codice Privacy**").

Sicil Tecno Plus S.r.l. (di seguito anche "**STP**" o la "**Società**"), nell'ambito del proprio Modello 231 e del proprio Sistema Gestionale 37001:2016, si era già dotata di un sistema per la gestione delle segnalazioni da whistleblowing. Alla luce delle sopra delineate modifiche normative, ha provveduto a rivederne le procedure e gli strumenti di effettuazione e gestione, tenendo conto delle peculiarità previste per i soggetti privati che abbiano impiegato, nell'ultimo anno, più di cinquanta dipendenti e che abbiano adottato un Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/2001[20].

Si precisa che, nell'impostazione del sistema di segnalazioni, la Società ha anche tenuto in debita considerazione quanto riportato nelle "*Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali*" approvate da ANAC con Delibera n°311 del 12 luglio 2023 nonché nella "*Guida Operativa whistleblowing per gli enti privati"* pubblicata da Confindustria nel mese di ottobre 2023.

2. SCOPO DEL DOCUMENTO

[20] La Società appartiene al *cluster* di cui all'art. 2, comma 1, lett. q, n. 3 del Decreto, ossia tra i soggetti che «*rientrano nell'ambito di applicazione del Decreto Legislativo 8 giugno 2001, n. 231, e adottano modelli di organizzazione, gestione e controllo ivi previsti, anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati*».

La presente Procedura per l'effettuazione di Segnalazioni - *Whistleblowing* (di seguito per brevità la "Procedura Segnalazioni-*Whistleblowing*" o la "Procedura") ha lo scopo di descrivere e disciplinare il sistema di segnalazioni implementato dalla Società, fornendo in particolare opportune indicazioni ai segnalanti per l'effettuazione di una segnalazione e illustrando gli aspetti salienti del relativo processo di gestione a cura della Società.

In particolare, il presente documento:

a) definisce l'ambito di applicazione del sistema di segnalazione;
b) identifica i soggetti che possono effettuare segnalazioni;
c) circoscrive il perimetro delle condotte, avvenimenti o azioni che possono essere oggetto di segnalazione;
d) identifica i canali attraverso cui effettuare le segnalazioni;
e) identifica e prescrive i principi e le regole generali che governano il processo di segnalazione, ivi incluse le tutele per il soggetto segnalante e per il soggetto segnalato, nonché le conseguenze di eventuali abusi nell'utilizzo del sistema di segnalazione;
f) delinea gli aspetti salienti del relativo processo di gestione delle Segnalazioni.

3. AMBITO DI APPLICAZIONE

La Procedura Segnalazioni - Whistleblowing si applica ai soggetti interessati in qualità di *Segnalante* e *Segnalato*, come di seguito definiti, nonché alle figure e funzioni aziendali eventualmente coinvolte nella gestione della Segnalazione di Violazione ricevuta.

4. COMUNICAZIONE E DIFFUSIONE

Il presente documento è portato a conoscenza del personale aziendale all'atto dell'adozione, in caso di aggiornamento e comunque in fase di selezione e al momento dell'inserimento in azienda. Esso è reso facilmente accessibile al personale aziendale mediante **esposizione in bacheca**. Per una diffusione capillare della Procedura, la stessa viene, inoltre, consegnata a mano ad ogni dipendente (far firmare per ricezione). Per finire, il presente documento viene anche pubblicato nel sito istituzionale della Società per essere disponibile nei confronti di tutti gli eventuali interessati.

5. TERMINI E DEFINIZIONI

Termine utilizzato	Descrizione
Soggetto Segnalante (o "Segnalante")	La persona fisica che effettua la Segnalazione, come meglio delineato al Paragrafo 7.1 "*I Soggetti Segnalanti*".
Soggetto Segnalato (o "Segnalato")	La persona fisica o giuridica menzionata nella Segnalazione come persona alla quale la violazione è attribuita o che è comunque implicata in tale violazione.
Segnalazione	Comunicazione scritta od orale di informazione sulle Violazioni effettuata dal Soggetto Segnalante, attraverso uno dei canali di segnalazione previsti. La Segnalazione deve avere le forme e i contenuti minimi previsti nel Paragrafo 7.2.2. "*Forma e contenuti minimi della Segnalazione con Canali Interni*".
Violazione	La Violazione consiste in comportamenti, atti od omissioni, che ledono l'integrità della Società, di cui il Segnalante sia venuto a conoscenza nell'ambito del proprio contesto lavorativo e riconducibili a quanto delineato al Paragrafo 7.2. "*Oggetto della Segnalazione – le Violazioni*".

Gestore delle Segnalazioni	Il soggetto gestore delle segnalazioni, ai sensi dell'art. 4 del D. Lgs. 24 marzo 2023, dovrà essere "*una persona o un ufficio interno autonomo dedicato e con personale specificamente formato (…) ovvero un soggetto esterno, anch'esso autonomo e con personale specificamente formato*". Tale soggetto potrà coinvolgere anche altre funzioni aziendali, a condizione che sia costantemente garantita la riservatezza dell'identità del segnalante e siano espressamente autorizzate a trattare dati ai sensi del GDPR. Nella Società tale soggetto è identificato come al Paragrafo 7.4. "*Processo di Gestione delle Segnalazioni per Canali Interni*" della presente Procedura.
Informazioni riservate	Si tratta di Informazioni coperte dall'obbligo di segreto, dalla tutela del diritto d'autore o dalla protezione dei dati personali.
Riscontro	Il Riscontro è una comunicazione che viene data alla persona segnalante di informazioni relative al seguito che viene dato o che si intende dare alla segnalazione.
Ritorsione	La Ritorsione è un qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione e che provoca o può provocare alla persona segnalante, in via diretta o indiretta, un danno ingiusto.

6. DOCUMENTI DI RIFERIMENTO

- Codice Etico e di Comportamento della Società;
- Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 8 giugno 2001, n. 231, adottato della Società.

7. IL SISTEMA DI SEGNALAZIONI – WHISTLEBLOWING

7.1. Il Gestore delle Segnalazioni

Sicil Tecno Plus S.r.l. ha identificato, ai sensi dell'art. 4 del Decreto, l'**Organismo di Vigilanza** ex D.Lgs. 231/2001 e la **Funzione di Conformità** anticorruzione del proprio Sistema Gestionale 37001:2016 – nelle persone del Dott. Moreno Prosperi e dell'avv. Francesca Bilardo - quale *Gestore del Canale di Segnalazione Interno*; soggetto/organo espressamente autorizzato a trattare i dati di cui al presente processo ai sensi degli artt. 29 e 32 del GDPR e dell'art. 2- quaterdecies del Codice Privacy (D.Lgs. 196/03).

Tutte le Segnalazioni interne dovranno essere inviate, pertanto, ai succitati soggetti/organi secondo le modalità descritte al successivo paragrafo 7.4.

7.2. Soggetti Segnalanti

I Soggetti Segnalanti cui la presente Procedura si rivolge sono tutte le persone assunte dalla Società con contratto di lavoro a tempo indeterminato o a tempo determinato, a tempo pieno o a tempo parziale, inclusi i contratti di lavoro intermittente, di apprendistato, di lavoro accessorio, o tramite contratto di somministrazione di lavoro, nonché i prestatori di lavoro occasionale di cui all'art. 54-bis del D.L. 24 aprile 2017, n. 50; tutti i lavoratori autonomi ai sensi dell'art. 2222 del codice civile e del Capo I della l. 22 maggio 2017, n. 81 (esclusi gli imprenditori, anche piccoli); i collaboratori coordinati e continuativi ai sensi dell'art. 409, n. 3, del codice di procedura civile; gli stagisti, i volontari e i tirocinanti presso la Società; le persone con funzioni di amministrazione, direzione, controllo, vigilanza e rappresentanza (anche di fatto) della Società, gli azionisti, nonché i lavoratori o collaboratori dei soggetti che forniscono beni o servizi o che realizzano opere in favore di terzi, i liberi professionisti e i consulenti che prestino la propria attività presso la Società.

Rientrano tra i Segnalanti anche i soggetti: (i) il cui rapporto giuridico con la Società non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali; (ii) durante il periodo di prova; (iii) dopo lo scioglimento del rapporto, se le informazioni sulle violazioni sono state acquisite nel corso del rapporto.

7.3. Oggetto della Segnalazione – le Violazioni

I Soggetti Segnalanti possono effettuare Segnalazioni di **Violazioni** consistenti in comportamenti, atti od omissioni, **che ledono l'integrità della Società**, di cui il Segnalante sia venuto a conoscenza nell'ambito del proprio contesto lavorativo e relative a **condotte illecite rilevanti ai sensi del D.Lgs. 231/2001 e violazioni del Modello 231**.

La Segnalazione dovrà avere ad oggetto:

a) Violazioni commesse o che potrebbero essere state commesse, sulla base di fondati sospetti;

b) Violazioni non ancora compiute ma che il Segnalante ritiene che potrebbero essere commesse, sulla base di fondati sospetti;

c) condotte volte ad occultare le Violazioni sopra indicate.

Sono escluse:

- «*le contestazioni, rivendicazioni o richieste legate a un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengano esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate*», secondo quanto espressamente previsto dall'art. 1, comma 2, lett. a) del D.Lgs. 24/2023;
- le segnalazioni Vietate come da paragrafo 7.3.1. "*Segnalazioni Vietate: azioni, fatti e condotte che non possono essere segnalati*".

Tra le informazioni sulle Violazioni non segnalabili, sono ricomprese le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché le informazioni acquisite sulla base di indiscrezioni o vociferazioni scarsamente attendibili (c.d. voci di corridoio).

7.3.1 Segnalazioni vietate: azioni, fatti e condotte che non possono essere segnalati

La Segnalazione NON deve assumere toni ingiuriosi o contenere offese personali o giudizi morali volti ad offendere o ledere l'onore e/o il decoro personale e/o professionale della persona o delle persone a cui i fatti segnalati sono riferiti.

È vietato in particolare:

- il ricorso ad espressioni ingiuriose;
- l'invio di Segnalazioni con finalità meramente diffamatorie o calunniose aventi con l'unico scopo quello di danneggiare il Segnalato;
- l'invio di Segnalazioni di natura discriminatoria, in quanto riferite ad orientamenti sessuali, religiosi e politici o all'origine razziale o etnica del Soggetto Segnalato.

7.3.2 Forma e contenuti minimi della Segnalazione con Canali di Segnalazione Interni

È necessario che la Segnalazione sia il più possibile circostanziata ed offra il maggior numero di elementi al fine di consentirne una opportuna gestione e di darne adeguato seguito. Al fine di consentire un proficuo utilizzo della Segnalazione questa dovrebbe avere i seguenti elementi essenziali:

- **Oggetto**: una chiara descrizione della Violazione oggetto di Segnalazione, con indicazione delle circostanze di tempo e luogo in cui sono stati commessi/omessi i fatti (a titolo puramente esemplificativo: contratto, transazione, luogo, ecc.)
- **Soggetto Segnalato e altri soggetti coinvolti**: qualsiasi elemento (come la funzione/ruolo aziendale) che consenta un'agevole identificazione del/i presunto/i autore/i della Violazione segnalata o di altri soggetti eventualmente coinvolti;
- **Effettuata in lingua italiana.**

Al fine di incoraggiare le segnalazioni, si precisa che **la Società accetta altresì Segnalazioni in forma anonima** (da intendersi quali Segnalazioni dalle quali non è possibile ricavare l'identità del Segnalante), sempre che presentino i requisiti essenziali di cui sopra.

Il Segnalante che non vuole restare anonimo, potrà indicare i seguenti ulteriori elementi:

- le **proprie generalità**;
- l'indicazione di **eventuali altri soggetti** che possono riferire sui fatti narrati;
- l'indicazione di **eventuali documenti** che possono confermare la fondatezza di tali fatti e qualsiasi altra eventuale documentazione utile a meglio circostanziare la Segnalazione;
- **ogni altra informazione** che possa agevolare la raccolta di evidenze su quanto segnalato.

7.4. Canali di Segnalazione Interni

La Società ha istituito i seguenti Canali di Segnalazione Interni (che consentono Segnalazioni in forma scritta o orale):

7.4.1 Segnalazione scritta tramite posta ordinaria

La Segnalazione può essere effettuata per iscritto con le seguenti modalità:

a) Segnalazione NON in forma anonima

Si prevede l'utilizzo di due buste chiuse: la prima con i dati identificativi del Segnalante, unitamente alla fotocopia del documento di riconoscimento; la seconda con la Segnalazione (in modo da separare i dati identificativi del Segnalante dalla Segnalazione). Entrambe le buste dovranno poi essere inserite in una terza busta chiusa riportante il destinatario e il suo indirizzo.

Se la Segnalazione viene spedita presso la sede di Sicil Tecno Plus srl, Viale Dioniso 6, 98035, Giardini Naxos (ME), la busta deve recare all'esterno la dicitura "*riservata all'Organismo di Vigilanza/Funzione di Conformità anticorruzione, in qualità di Gestori delle Segnalazioni"*.

Se la Segnalazione viene spedita direttamente al succitato *Organo di Gestione delle Segnalazioni,* dovrà essere inviata a entrambi i seguenti indirizzi: Avv. Francesca Bilardo, Corso Italia 88, 95129, Catania; Dott. Moreno Prosperi, P.zza della Vaschette 14, 00193, Roma.

b) Segnalazioni in forma anonima: utilizzo di una sola busta chiusa con la Segnalazione.

I Destinatari della Segnalazione ed i loro indirizzi sono gli stessi riportati nel precedente punto a).

c) Strumenti e gestione della segnalazione scritta

Entrambi i due succitati tipi di segnalazione, nei confronti del Canale Interno, possono essere effettuati esclusivamente tramite Raccomandata con Ricevuta di Ritorno. Il Segnalante dovrà indicare nella busta l'indirizzo del mittente (al fine di consentire al Gestore della Segnalazione l'interlocuzione con il Segnalante).

Per garantire l'anonimato del Segnalante, lo stesso potrà indicare come propri riferimenti una casella postale o qualsiasi altro nome e indirizzo.

7.4.2 Segnalazione in forma orale

Il segnalante potrà effettuare segnalazione orale tramite contatto telefonico con i due Gestori della Segnalazione ai seguenti numeri: 328.8466021 (Avv. Francesca Bilardo); 348.6388890 (Dott. Moreno Prosperi). Ove il segnalante opti per questa scelta, al fine di consentire un sicuro contatto telefonico, dovrà essere inviato agli stessi Gestori della Segnalazione un messaggio whatsapp di prenotazione/anticipazione della telefonata.

a) Segnalazione tramite richiesta di incontro diretto

Il Segnalante potrà chiedere un incontro diretto al Gestore della Segnalazione. In questo caso, la Segnalazione è effettuata oralmente nel corso dello stesso incontro con il Gestore della Segnalazione (ovvero, uno o tutte e due i su richiamati soggetti).

Il contenuto orale dell'incontro, previo consenso del Segnalante, è documentato mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale.

In caso di verbale, il Segnalante potrà verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione. Copia del verbale deve essere consegnata al Segnalante. Lo svolgimento dell'incontro diretto deve avvenire entro 15 giorni dalla richiesta e deve avvenire in un luogo idoneo a garantire la riservatezza del Segnalante.

7.5. Processo di gestione delle Segnalazioni per Canali Interni

I Canali di Segnalazione Interni assicurano la protezione dei dati personali e la riservatezza: dell'identità del Segnalante e del Segnalato; del contenuto della Segnalazione; della documentazione.

Nel caso in cui la **Segnalazione scritta sia presentata ad un soggetto diverso rispetto al Gestore delle Segnalazioni**, tale soggetto dovrà trasmetterla al Gestore delle Segnalazioni mediante uno dei Canali di Segnalazione Interni di cui al paragrafo 7.4, entro sette giorni dal suo ricevimento.

Il Gestore delle Segnalazioni:

- darà diligente seguito alla Segnalazione;
- adotterà le misure più opportune per verificare la completezza e fondatezza delle informazioni;
- manterrà le interlocuzioni con il Segnalante e potrà richiedere, se necessario, integrazioni o ulteriori confronti ed approfondimenti;
- potrà interfacciarsi con altre funzioni, figure aziendali o eventuali specialisti esterni (v. ad esempio periti informatici), al fine di condurre l'istruttoria sulla segnalazione, ma solo previa ed espressa autorizzazione del Segnalante;
- potrà svolgere attività di indagine anche con il coinvolgimento di consulenti esterni, nell'assoluto rispetto delle garanzie di riservatezza di cui al Decreto e alla presente Procedura e sempre previa espressa autorizzazione del Segnalante.

Viene di seguito delineato il **processo di Gestione delle Segnalazioni**, con particolare riferimento alle seguenti fasi:

1) ricezione e registrazione della Segnalazione;
2) priorità nella gestione delle Segnalazioni (c.d. triage);
3) valutazione preliminare, verifiche e indagini in merito alla Segnalazione;
4) riscontro alla Segnalazione;
5) conclusione del processo;
6) conservazione delle Segnalazioni e della relativa documentazione.

7.5.1 Ricezione e registrazione della Segnalazione

A seguito della Segnalazione pervenuta attraverso il canale della posta con ricevuta di ritorno, il Gestore della Segnalazione provvederà ad attribuire un numero identificativo progressivo che ne consentirà l'identificazione univoca.

7.5.2 Priorità nella gestione delle segnalazioni (c.d. triage)

In presenza di più segnalazioni da gestire contemporaneamente, il Gestore valuta l'urgenza di intervento in base alla combinazione della probabilità della violazione e al suo potenziale impatto sulla Società, tenendo conto dei seguenti fattori:

- la violazione può assumere rilevanza penale?
- la violazione è già avvenuta, è in corso o sta per accadere?

- c'è la necessità immediata di interrompere o sospendere le attività commerciali?
- esiste un rischio immediato per la salute e la sicurezza?
- esiste un rischio immediato per i diritti umani o per l'ambiente?
- c'è la necessità di assicurare e proteggere le prove prima che vengano cancellate o distrutte?
- esiste un rischio per le funzioni, i servizi e/o la reputazione della Società?
- la segnalazione può impattare sulla continuità aziendale?
- quale impatto mediatico può avere la segnalazione?
- sono disponibili ulteriori informazioni a supporto della segnalazione?
- qual è la natura dell'illecito (tipo e frequenza della violazione, ruolo e anzianità dei soggetti coinvolti nella segnalazione)?
- qual è la probabilità che la violazione venga segnalata anche al di fuori dell'ente?
- la violazione è già stata segnalata in precedenza?
- in che modo il segnalante ha ottenuto le informazioni? sono "di prima mano" o "per sentito dire"?

7.5.3 Valutazione preliminare, verifiche e indagini in merito alla Segnalazione

Il Gestore della Segnalazione provvede tempestivamente alla presa in carico e all'analisi preliminare della Segnalazione ricevuta. Se necessario, e laddove le modalità di Segnalazione lo consentano, potrà richiedere al Soggetto Segnalante ulteriori informazioni o documentazione a supporto, al fine di permettere una valutazione maggiormente esaustiva e concludente della Segnalazione.

Al termine della fase di valutazione preliminare, laddove la Segnalazione ricevuta sia stata classificata come "rilevante e trattabile", il Gestore delle Segnalazioni procederà con l'avvio delle verifiche e di indagini interne al fine di raccogliere ulteriori informazioni di dettaglio e verificare la fondatezza dei fatti segnalati, sempre rispettando l'assoluta riservatezza dell'identità del segnalante e nei limiti di eventuali ulteriori autorizzazioni da parte dello stesso segnalante A tale scopo, il Gestore delle Segnalazioni si riserva la facoltà di richiedere ulteriori informazioni o documentazione al Soggetto Segnalante, nonché di coinvolgerlo in fase di istruttoria e fornire allo stesso eventuali informazioni circa avvio e stato avanzamento dell'istruttoria.

Il Segnalato può essere sentito (o, su sua richiesta, *deve* essere sentito) nel processo di gestione della Segnalazione interna, anche attraverso l'acquisizione di osservazioni scritte e documenti.

Nell'ambito dell'attività istruttoria, il Gestore delle Segnalazioni potrà avvalersi del supporto di altre Funzioni aziendali, anche acquisendo atti o documenti, e/o di consulenti esterni, fornendo in ogni caso le dovute garanzia di riservatezza e tutele e/o la specifica autorizzazione del Segnalante.

7.5.4 Riscontro alla Segnalazione

Entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della Segnalazione, il Gestore delle Segnalazioni provvede a dare Riscontro al Segnalante mediante mezzo idoneo in merito al seguito che è stato dato o che s'intende dare alla Segnalazione.

Tale riscontro può consistere, ad esempio, nella comunicazione dell'archiviazione, nell'avvio di un'inchiesta interna ed eventualmente nelle relative risultanze, nei provvedimenti adottati per affrontare la questione sollevata, nel rinvio a un'autorità competente per ulteriori indagini.

Il medesimo riscontro, può anche essere meramente interlocutorio, giacché potrà consistere nella comunicazione delle informazioni relative a tutte le attività sopra descritte che si intendono intraprendere e lo stato di avanzamento dell'istruttoria. In tale ultimo caso, terminata l'istruttoria, anche gli esiti della stessa dovranno essere comunicati alla persona Segnalante.

7.5.5 Conclusione del processo

All'esito della fase di analisi, il Gestore conclude il processo di gestione della segnalazione mediante l'emissione di apposito report nel rispetto dei principi di riservatezza, in cui dovranno risultare:

a. gli elementi descrittivi della Violazione (es: luogo e data di svolgimento dei fatti, elementi di prova e documentali);
b. le verifiche svolte, gli esiti delle stesse e i soggetti aziendali o terzi coinvolti nella fase di analisi;
c. una valutazione di sintesi del processo di analisi con indicazione delle fattispecie accertate e delle relative motivazioni;
d. l'esito e la conclusione dell'analisi.

In esito all'attività di verifica ed indagine di cui sopra, il Gestore delle Segnalazioni:

(i) laddove ravvisi elementi di fondatezza della Segnalazione, si rivolge agli organi/funzioni aziendali competenti (anche condividendo il report predisposto), perché queste individuino e intraprendano le conseguenti iniziative (anche disciplinari e/o giudiziali), di loro esclusiva spettanza;
(ii) laddove, invece, ravvisi elementi di manifesta infondatezza della Segnalazione, ne dispone l'archiviazione con adeguata motivazione;
(iii) laddove, infine, ravvisi elementi di effettuazione con dolo o colpa grave della Segnalazione manifestamente infondata, provvede come sopra previsto *sub* (i) e dispone l'archiviazione come sopra previsto *sub* (ii).

7.5.6 Conservazione delle Segnalazioni e della relativa documentazione

Le Segnalazioni, 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, o fino a conclusione del procedimento giudiziale o disciplinare eventualmente conseguito nei confronti del Segnalato o del Segnalante, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del Decreto e del principio di cui agli articoli 5, paragrafo 1, lettera e), del GDPR (limitazione della conservazione) e 3, comma 1, lettera e), del D.Lgs. n. 51 del 2018.

7.6. Principi generali e tutele

Di seguito si riportano i principi e le tutele che la Società si impegna a garantire nel processo di gestione delle Segnalazioni.

La corretta gestione del sistema di Segnalazioni supporterà la diffusione di una cultura dell'etica, della trasparenza e della legalità all'interno della Società. Tale scopo può essere raggiunto se i Segnalanti hanno a disposizione non solo i canali di segnalazione, ma anche la certezza di non subire ritorsioni da parte di colleghi o superiori o di altri esponenti di Sicil Tecno Plus o di rischiare di vedere la propria Segnalazione inascoltata.

7.6.1 Tutela del Segnalante

La Società tutela il Soggetto Segnalante garantendo la riservatezza sulla sua identità e prevedendo espressamente il divieto di atti di Ritorsione per motivi collegati, direttamente o indirettamente, alla Segnalazione, coerentemente alle previsioni del Decreto, oltre alle limitazioni di responsabilità di cui all'art. 20 del Decreto. Tali tutele e le misure di protezione previste dal Decreto in favore del Segnalante si applicano, solo se ricorrono cumulativamente le seguenti condizioni:

- il Segnalante, al momento della Segnalazione, aveva fondato motivo di ritenere che le Violazioni segnalate fossero vere e rientrassero nell'ambito oggettivo di applicazione riportato nel paragrafo 7.3 - "Oggetto della Segnalazione – le Violazioni",

- la Segnalazione è stata effettuata nel rispetto delle previsioni della presente Procedura, nonché delle disposizioni del Decreto (in particolare, utilizzando i Canali, nel rispetto delle relative condizioni e modalità di accesso).

Inoltre, **tali tutele e misure di protezione si applicano anche in favore**:

- dei cosiddetti "facilitatori", ovvero le persone fisiche che, operanti nel medesimo contesto lavorativo del Segnalante, lo assistono nel processo di segnalazione;
- delle persone del medesimo contesto lavorativo del Segnalante e che sono legate allo stesso da uno stabile legame affettivo o di parentela entro il quarto grado;
- dei colleghi di lavoro del Segnalante che lavorano nel medesimo contesto lavorativo e che hanno con quest'ultimo un rapporto stabile e abituale;
- degli enti di proprietà del Segnalante o per i quali lo stesso lavora nonché gli enti che operano nel medesimo contesto lavorativo del Segnalante.

A tali soggetti la presente Procedura fa sintetico riferimento anche come "Altri Soggetti Tutelati".

Eventuali comportamenti in violazione delle misure di tutela previste in favore del Segnalante e degli ulteriori soggetti sopra indicati, potrà dare origine a procedimenti disciplinari nei confronti del responsabile e potrà essere sanzionata da ANAC con una sanzione amministrativa pecuniaria, secondo quanto previsto dall'art. 21 del Decreto.

7.6.2 Riservatezza

La Società garantisce la riservatezza dell'identità del Segnalante, del Segnalato, degli eventuali facilitatori e degli altri soggetti menzionati nella Segnalazione, nonché la riservatezza del contenuto della Segnalazione e della documentazione ad essa allegata.

Le Segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse.

L'identità del Segnalante e qualsiasi altra informazione da cui possa evincersi – direttamente o indirettamente – tale identità non può essere rivelata senza l'espresso consenso del Segnalante a soggetti diversi da quelli competenti a ricevere o dare seguito alle Segnalazioni, come identificati nella presente Procedura. Tutti coloro che ricevono o sono coinvolti nella gestione delle Segnalazioni sono tenuti a tutelarne la riservatezza.

Inoltre, l'identità del Segnalante:

- nell'ambito del procedimento disciplinare, non può essere rivelata, qualora la contestazione del relativo addebito 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 del Segnalante sia indispensabile per la difesa del soggetto Segnalato, la Segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del Segnalante alla rivelazione della propria identità. In tal caso, dovrà essere data comunicazione scritta al Segnalante delle ragioni della rivelazione dei dati riservati e gli dovrà essere richiesto per iscritto se intenda prestare il consenso a rivelare la propria identità, con avviso che – in caso contrario – la Segnalazione non potrà essere utilizzata nel procedimento disciplinare.

È inoltre dato avviso al Segnalante per iscritto delle ragioni della rivelazione dei dati riservati, quando la rivelazione dell'identità del Segnalante e delle informazioni da cui possa evincersi, direttamente o indirettamente, tale identità, sia indispensabile alla difesa del Segnalato.

L'identità del Segnalato, del facilitatore e delle persone comunque coinvolte e menzionate nella Segnalazione sono tutelate fino alla conclusione dei procedimenti avviati in ragione della Segnalazione, con le medesime garanzie previste in favore del Segnalante al presente paragrafo.

7.6.3 Divieto di Ritorsione

I Segnalanti non possono subire alcuna forma di ritorsione per aver effettuato una Segnalazione rispettando le condizioni per l'applicazione delle tutele ex Decreto. Anche gli Altri Soggetti Tutelati non possono subire alcuna forma di ritorsione a causa del ruolo assunto nell'ambito del processo di Segnalazione o del particolare rapporto che li lega al Segnalante (che abbia effettuato una segnalazione nel rispetto delle condizioni per l'applicazione delle tutele ex Decreto).

Per Ritorsione si intende qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della Segnalazione che provoca o può provocare al Segnalante, in via diretta o indiretta, un danno ingiusto.

A titolo esemplificativo e non esaustivo, possono essere considerate ritorsioni:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato (laddove il Segnalante avesse una legittima aspettativa a detta conversione, sulla base di particolari circostanze di fatto, precise e concordanti); il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine (laddove il Segnalante avesse una legittima aspettativa a detto rinnovo, sulla base di particolari circostanze di fatto, precise e concordanti);
- i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

I Segnalanti e gli Altri Soggetti Tutelati che ritengano di subire ritorsioni potranno comunicarlo (Segnalazione esterna) esclusivamente ad ANAC (e non anche a soggetti diversi per non vanificare le tutele che il Decreto garantisce, prima fra tutte, la riservatezza), secondo le modalità e gli strumenti previsti dalla stessa[21], per i provvedimenti del caso.

7.6.4 Segnalazione esterna

Il segnalante può effettuare una segnalazione esterna quando:

a) il canale di segnalazione interna non è attivo o, anche se attivato, non è conforme a quanto previsto dall'art. 4 del D.Lgs. 24/23;

b) la persona segnalante ha già effettuato una segnalazione interna ai sensi dell'art. 4 del D.Lgs. 24/23 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;

[21] Si rimanda a tal proposito al link https://www.anticorruzione.it/-/whistleblowing.

d) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Le segnalazioni esterne sono effettuate in forma scritta tramite la piattaforma informatica istituita dall'ANAC, oppure in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta del segnalante, mediante un incontro diretto.

7.6.5 Trattamento dei dati personali

Si precisa che i dati personali della Segnalazione, del Segnalante e del Segnalato (questi ultimi considerati "interessati" ai sensi dell'art. 4 GDPR) sono trattati in conformità al GDPR ed al Codice Privacy.

8. CONFLITTO DI INTERESSI

Nel caso in cui il Gestore della Segnalazione coincida con il Segnalante, con il Segnalato o sia comunque una persona coinvolta o interessata dalla Segnalazione, quest'ultima dovrà essere indirizzata al Consiglio di Amministrazione, il quale dovrà applicare e rispettare gli obblighi di riservatezza previsti dalla presente procedura.

9. SISTEMA DISCIPLINARE

Si rammenta che l'eventuale mancato rispetto di quanto contenuto nella presente Procedura può comportare l'irrogazione di sanzioni disciplinari, nelle ipotesi previste dalla legge.

A tale riguardo si chiarisce che la Società potrà irrogare sanzioni disciplinari così come previsto dal Contratto Collettivo Nazionale di Lavoro di riferimento applicabile e dal Modello 231, a coloro i quali, a titolo esemplificativo:

- effettuano segnalazioni in mala fede;
- effettuano una segnalazione di cui l'Autorità giudiziaria abbia accertato la natura diffamatoria o calunniosa;
- rivelano l'identità del segnalante, delle persone connesse e di ogni altra informazione dalla quale possa evincersi la loro identità;
- pongono in essere comportamenti volti ad ostacolare la segnalazione;
- tentano di identificare il segnalante;
- non gestiscono la segnalazione per dolo o colpa grave, ivi compreso il mancato rimedio, da parte di chi ne abbia i poteri, alle violazioni o alle ritorsioni segnalate;
- adottano comportamenti ritorsivi.