SIAT 231

SISTEMA INTEGRATO

Anticorruzione

Trasparenza

Modello di Organizzazione e Gestione (MOG) 231

ai sensi della L. 190/2012 e D.LGS 33/2013

come modificati dal D.LGS 97/2016

e del

decreto legislativo 8 giugno 2001, n. 231

SEZIONE I. MOG 231

PARTE GENERALE

Processo	Ruolo	Nominativo	Data
Predisposto da	Coordinatore 231; Responsabile della Prevenzione della Corruzione e Responsabile Trasparenza	Giuseppe Liguori Giorgio Fiorillo Raffaella Ruggiero	07/04/2022
Inviato in visione	Dirigente - Amministratore Unico - Enti soci- Collegio Sindacale- OdV	Giorgio Fiorillo	07/04/2022
Adottato	Amministratore Unico con decisione n. 08/22	Amelia Luca	11/04/2022

Versione n.	Motivo della revisione	Data
0.0	Proposta	07/04/2022
1.0	Versione adottata	11/04/2022

Indice

Allegati:

0 Premesse.

Con questo documento si concretizza un processo di revisione complessiva degli strumenti organizzativi della SRM con l'obiettivo implementare un Sistema Integrato Anticorruzione, Trasparenza, Modello di Organizzazione e Gestione (MOG) 231, denominato SIAT231, valorizzando l'esperienza maturata in questi anni con la certificazione di Qualità. La SRM ha ottenuto la prima certificazione di qualità ISO 9001 nel 2016 e la certificazione è stata confermata negli anni successivi fino al 2020.

Nel 2016 si è dotata del primo PTPCT in quanto società controllata da enti pubblici e nel 2017 ha adottato il MOG 231 in quanto società di diritto privato (decisione dell'Amministratore Unico della SRM n.7/2017 del 17 maggio 2017).

Questi tre strumenti incidono sull'organizzazione aziendale partendo da analisi e presupposti comuni ma con obiettivi, vocabolari e formalità differenti che costringono la società ad aggiornare e seguire strumenti diversi che potrebbero anche risultare in discordanza tra loro a causa delle diverse fasi di aggiornamento. Mantenere in funzione tre differenti strumenti aumenta inoltre la complessità dell'intero sistema e può creare confusione sulla funzione dello specifico strumento.

Vista la natura della Società, che svolge prevalentemente funzioni pubbliche ed è pertanto più assimilabile, in termini di missione e obiettivi, ad un ente locale, si è deciso di abbandonare progressivamente il Sistema integrato gestione qualità ISO 9001 (SQ) per definire un nuovo Sistema Integrato Anticorruzione, Trasparenza e MOG 231 (SIAT231).

Le procedure sviluppate nel SQ verranno progressivamente aggiornate ove necessario e tenute in essere nel nuovo SIAT231 e con esse l'esperienza maturata nella gestione di un sistema integrato e semplicemente si è deciso di rinunciare ad ottenere la certificazione che implica formalità non necessarie ai fini del SIAT231.

Nel presente piano si è proceduto pertanto ad una revisione dei processi aziendali in essere per meglio descrivere le aree di rischio individuate nel PNA 2019 con estensione alle aree di maggior interesse del MOG 231.

È stato revisionato l'impianto del MOG 231 precedentemente elaborato per renderlo più corrispondente alle previsioni normative ed è stato aggiornato al 31.12.2021 l'elenco dei reati previsti oggetto del MOG.

Si è modificato il metodo di valutazione e ponderazione del rischio adottando le modalità descritte nel MOG231 che si ritengono coerenti con le indicazioni del PNA 2019 e sono state individuate le relative misure di mitigazione del rischio.

Si è ottenuta pertanto una descrizione più completa e dettagliata dei processi e delle attività sviluppate dalla SRM e un'analisi ed una valutazione unica dei rischi sia con riferimento ai reati anticorruzione, sia con riferimento ai reati 231 che hanno radici comuni, come comuni sono le misure per mitigare i rischi.

Il SIAT 231 ("Sistema" nella sua accezione più ampia) della SRM è composto da 2 sezioni con i relativi allegati.

Sezione I. MOG 231:

- Parte generale: è descritto l'obiettivo che si intende raggiungere con il SIAT231 e gli aspetti fondanti del MOG231.

- Parte speciale: si analizzano le diverse fattispecie di reato e la loro relazione con i processi aziendali procedendo con la mappatura dei processi aziendali, la valutazione del rischio e l'individuazione delle misure correttive e di controllo.

Sezione II. PTPCT

- Parte Anticorruzione e trasparenza: è descritto il profilo societario della SRM e il contesto esterno ed interno, le normative alla base del Piano anticorruzione e trasparenza, il processo di adozione del documento, i ruoli all'interno della società e gli strumenti organizzativi di attuazione e controllo sul tema dell'anticorruzione e trasparenza, le misure integrative per l'anticorruzione e la trasparenza, il monitoraggio e le misure programmate.

Infine il SIAT 231 è integrato dalla documentazione interna costituita dal Manuale integrato e dalle Procedure adottati dalla SRM con il Sistema Qualità e dai Regolamenti che verranno progressivamente aggiornati ed uniformati.

Infine, nell'ottica di semplificazione e comunicabilità del piano, sia interna, sia esterna, richiesta dall'ANAC anche con il PNA 2019, si è cercato di semplificare il più possibile la parte relativa ai riferimenti normativi essendo essa già rintracciabile nei PNA 2019 per qualsiasi necessità e già valutata al fine della redazione del presente documento. Nei piani precedenti sono già descritti l'ambito soggettivo di competenza della SRM e le principali norme di riferimento.

0.1 Differenza e integrazione tra PTPCT e MOG 231.

Mentre l'adozione del Modello 231 è volta a ridurre al minimo il rischio di commissione dei reati presupposto tassativamente indicati dal D.Lgs. 231/2001, fonte di responsabilità amministrativa dell'ente solo laddove commessi nell'interesse o a vantaggio di quest'ultimo, il Piano Triennale di Prevenzione della Corruzione e della Trasparenza (PTPCT) intende contrastare i fenomeni corruttivi all'interno della Pubblica Amministrazione e delle società controllate, individuando misure idonee a prevenire situazioni in cui, a prescindere dalla rilevanza penale del comportamento posto in essere, si possa verificare una cattiva gestione delle risorse pubbliche ed un malfunzionamento dell'azione amministrativa a causa della deviazione, per fini personali, delle funzioni attribuite.

Con specifico riferimento alle fattispecie corruttive, la suddetta discrasia si traduce nel fatto che per il D.Lgs. 231/2001 assumono rilevanza i soli reati di concussione, induzione indebita a dare o promettere utilità e corruzione, compresa quella tra privati, mentre la L. 190/2012 fa riferimento ad un concetto più ampio di "corruzione", comprensivo non soltanto dell'intera gamma di reati contro la P.A., ma anche delle situazioni di "malamministrazione" delle risorse pubbliche a causa dell'uso a fini privati delle funzioni attribuite. Pur nell'avvenuta integrazione delle misure di prevenzione ad esse riconducibili, permangono dunque evidenti differenze tra la componente 231 e quella 190, afferenti non soltanto agli interessi tutelati e alle aree a rischio considerate, ma anche alle responsabilità configurabili in capo agli Organi deputati alle funzioni di vigilanza, ovvero l'Organismo di Vigilanza (OdV) ed il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT).

A tale proposito si riporta che la Legge 190/2012, nell'ipotesi di commissione all'interno dell'ente di un reato di corruzione accertato con sentenza passata in giudicato, prevede che il RPCT ne risponda sul piano della responsabilità dirigenziale, di quella disciplinare nonché per danno erariale e all'immagine della pubblica amministrazione, salvo che non dimostri di avere predisposto, antecedentemente alla commissione del fatto illecito, il Piano Anticorruzione e di avere vigilato sul funzionamento e l'osservanza dello stesso.

Nell'ambito del Sistema 231, in caso di accertata responsabilità amministrativa dell'ente, la norma non prevede invece in capo all'OdV alcuna responsabilità derivante dall'omessa o carente vigilanza. Ai membri dell'OdV è infatti imputabile la responsabilità contrattuale derivante dall'eventuale condotta omissiva e negligente, ad eccezione del caso di violazione degli obblighi

informativi previsti in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dal D.Lgs. 231/2007 (artt. 52, comma 2 e 55, comma 5). I compiti dell'Organismo non sono infatti connotati da poteri impeditivi, posto che l'adozione e/o la modifica del Modello, ancorché proposti dall'OdV con funzione consultiva e di supporto, sono espressione del potere gestorio dell'organo amministrativo. In ogni caso il RPCT e l'OdV collaboreranno al fine di garantire, nell'ambito delle rispettive competenze, un più elevato livello di prevenzione dei comportamenti illeciti e di assicurare l'efficace attuazione del Sistema Integrato Anticorruzione e Trasparenza 231, così come del resto previsto dalla Delibera ANAC 1134/2017.

1. Introduzione – il decreto 231

Il decreto legislativo 8 giugno 2001, n. 231 (di seguito anche "decreto 231"), ha introdotto nell'ordinamento italiano la responsabilità degli enti per gli illeciti conseguenti alla commissione di un reato.

Si tratta di un sistema di responsabilità autonomo, caratterizzato da presupposti e conseguenze distinti da quelli previsti per la responsabilità penale della persona fisica.

In particolare, l'ente può essere ritenuto responsabile se, prima della commissione del reato da parte di un soggetto ad esso funzionalmente collegato, non ha adottato ed efficacemente attuato modelli di organizzazione e gestione idonei a evitare reati della specie di quello verificatosi.

L'adozione del modello organizzativo è facoltativa: non costituisce un obbligo a carico dell'Ente.

La mancata adozione di tale strumento, tuttavia, espone l'Ente stesso alla possibilità di essere ritenuto responsabile per i reati commessi da dipendenti e amministratori.

Il Modello 231 peraltro nel caso di specie si completa e si integra con il Piano anticorruzione adottato ai sensi della L. 190/2012 e tenuto conto delle indicazioni riportate nella delibera ANAC 1134/2017.

Quanto alle conseguenze, l'accertamento dell'illecito previsto dal decreto 231 espone l'ente all'applicazione di gravi sanzioni, che ne colpiscono il patrimonio, l'immagine e la stessa attività.

Le imprese e le associazioni sono i principali destinatari della disciplina contenuta nel decreto 231.

Gli elementi costitutivi dell'illecito dell'ente dipendono dalla commissione di uno dei reati-presupposto indicati in via tassativa dal decreto 231, negli articoli 24 e seguenti.

La responsabilità dell'ente può sussistere soltanto in relazione al reato-presupposto commesso da parte di uno dei seguenti soggetti qualificati:

- persone che rivestono funzioni di rappresentanza, di amministrazione o direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale e che svolgono, anche di fatto, la gestione e il controllo dell'ente stesso. Si tratta di soggetti che, in considerazione delle funzioni che svolgono, vengono denominati "apicali";
- persone sottoposte alla direzione o alla vigilanza dei soggetti apicali.

Inoltre, l'ente può essere ritenuto responsabile dell'illecito se il reato è stato commesso nel suo interesse o a suo vantaggio.

Se l'interesse manca del tutto perché il soggetto qualificato ha agito per realizzare un interesse esclusivamente proprio o di terzi, l'impresa non è responsabile. Al contrario, se un interesse dell'ente - sia pure parziale o marginale - sussisteva, l'illecito dipendente da reato si configura anche se non si è concretizzato alcun vantaggio per l'impresa, la quale potrà al più beneficiare di una riduzione della sanzione pecuniaria. Nella decodificazione di tale criterio di imputazione, l'aspetto attualmente più controverso attiene all'interpretazione dei termini "interesse" e "vantaggio".

In particolare, il d.lgs. 231/2001 riguarda i reati commessi nell'interesse o a vantaggio della società o che comunque siano stati commessi anche nell'interesse o a vantaggio di questa. La legge 190/2012 è volta invece a prevenire reati commessi in danno della società.

2. Ambito di applicazione – il caso delle Società in *house*

Destinatari della disciplina di cui al decreto 231 sono "g*li Enti forniti di personalità giuridica, le società fornite di personalità giuridica e le società e le associazioni anche prive di personalità giuridica"* (art. 1, comma 2): il Decreto, invece, non si applica "*allo Stato, agli Enti pubblici-territoriali, agli altri Enti pubblici non economici nonché agli Enti che svolgono funzioni di rilievo costituzionale"* (art. 1, comma 3).

Riguardo a questi ultimi, la giurisprudenza ha avuto occasione di precisare che la natura pubblicistica di un Ente è condizione necessaria ma non sufficiente per sottrarlo al regime di responsabilità di cui al Decreto 231: occorre, infatti, anche che l'Ente non svolga un'attività economicamente intesa.

Verrebbero conseguentemente a ricadere all'interno della disciplina del Decreto tutte quelle figure soggettive pubbliche in veste societaria che svolgono attività commerciale considerato che il discrimine tra la non applicazione e l'applicazione del Decreto 231 non deriverebbe dalla natura dell'ente bensì dall'esercizio o non di un'attività economica.

Con sentenze n. 28699/2010 e n. 234/2011, la Corte di Cassazione penale ha affermato che sono esclusi dall'applicazione della disciplina del d.lgs. 231/2001 stante il disposto del comma 3 dell'articolo 1 – soltanto lo Stato, gli enti pubblici territoriali, gli enti che svolgono funzioni di rilievo costituzionale e gli altri enti pubblici non economici. Le conclusioni della Suprema Corte penale indurrebbero a ritenere che il decreto vada applicato a tutti gli enti privati e pubblici, non rientranti tra quelli esonerati per legge, comprese quindi le società in house.

Con la Determinazione n. 1134 del 2017, l'ANAC – in tema di integrazione del Modello di Organizzazione, Gestione e Controllo con il PTPCT – ha stabilito che gli enti pubblici economici e gli enti di diritto privato in controllo pubblico possono adottare un documento unico, comprensivo sia delle misure dettate dal D.Lgs. n. 231/2001, sia di quelle previste dalla L. n. 190/2012, laddove queste ultime costituiscono una sezione apposita del MOG.

Altro tema che si è posto in dottrina e nella pratica è il problema dell'applicabilità dei MOG alle piccole e medie imprese. Posto che è forse proprio in queste realtà che l'esperienza giudiziaria suggerisce di investire maggiormente, il decreto 231 si limita ad affermare, all'art. 6 comma 4, che gli Enti di piccole dimensioni possono attribuire le funzioni dell'Organismo di vigilanza all'organo dirigente.

Per il resto, occorre prendere atto del fatto che nelle imprese in cui il processo decisionale è concentrato in capo a un soggetto, gli strumenti di prevenzione dei reati sono più difficili da approntare.

3. La responsabilità dell'Ente

Ai sensi dell'art. 5 del Decreto 231, l'Ente può essere ritenuto responsabile in presenza di due presupposti oggettivi:

1. il primo e la realizzazione di un reato, compreso tra quelli tassativamente indicati dal Legislatore, da parte di una persona fisica legata all'Ente da un rapporto funzionale (apicale o sottoposto); in particolare, i soggetti apicali sono coloro che rivestono funzioni di

rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia funzionale e finanziaria o che, anche di fatto o con una delega di funzioni, esercitano la gestione e il controllo dell'Ente. Non rientrano in tale categoria i componenti del Collegio sindacale e coloro che svolgono funzioni di controllo o vigilanza, in assenza di poteri di gestione. Sono, invece, soggetti subordinati, coloro che sono sottoposti alla direzione e alla vigilanza degli apicali, anche se esterni alla compagine societaria.

2. il secondo è dato dal fatto che il reato sia commesso nell'interesse dell'Ente o a suo vantaggio.

L'aspetto attualmente più controverso attiene all'interpretazione dei termini "interesse" e "vantaggio", benché i due termini siano ricondotti a un concetto omnicomprensivo di convenienza per l'Ente.

L' "interesse" dell'Ente deve, infatti, essere qualificato come l'obiettivo cui è finalizzata, sulla base di una valutazione *ex ante*, la condotta del soggetto che agisce.

Il "vantaggio", invece, è costituito dal risultato, palesatosi *ex post*, che oggettivamente deriva dall'azione criminale, sia nei casi in cui essa fosse finalizzata a soddisfare l'interesse dell'Ente, sia nei casi in cui, pur difettando questa finalizzazione iniziale, l'Ente abbia comunque tratto un beneficio giuridicamente apprezzabile dalla consumazione del reato.

Tuttavia, quando il catalogo dei reati-presupposto è stato esteso per includervi quelli in materia di salute e sicurezza sul lavoro (art. 25 *septies* del decreto 231) e poi i reati ambientali (art. 25 *undecies*), si è posto un problema di compatibilità del criterio dell'interesse o vantaggio con i reati colposi.

La giurisprudenza ha ritenuto che nei reati colposi l'interesse o vantaggio dell'ente andrebbero valutati con riguardo all'intera fattispecie di reato, non già rispetto all'evento dello stesso. Infatti, mentre nei reati-presupposto dolosi l'evento del reato ben può corrispondere all'interesse dell'ente, non può dirsi altrettanto nei reati presupposto a base colposa, attesa la contro-volontà che caratterizza questi ultimi ai sensi dell'articolo 43 del codice penale.

Si pensi, infatti, ai reati in materia di salute e sicurezza: difficilmente l'evento lesioni o morte del lavoratore può esprimere l'interesse dell'ente o tradursi in un vantaggio per lo stesso.

In questi casi, dunque, l'interesse o vantaggio dovrebbero piuttosto riferirsi alla condotta inosservante delle norme cautelari. Così, l'interesse o vantaggio dell'ente potrebbero ravvisarsi nel

risparmio di costi per la sicurezza ovvero nel potenziamento della velocità di esecuzione delle prestazioni o nell'incremento della produttività, sacrificando l'adozione di presidi antinfortunistici, come di recente ribadito dalla Corte di Cassazione (cfr. anche Cass., IV Sez. pen., sent. n. 16713/2018, Cass., IV Sez. pen., sent. n. 48779/2019, Cass. pen. Sez. III, sent. n. 3157/2019, Cass., IV Sez. pen., sent. n. 3731/2020).

Sul piano soggettivo l'ente risponde se non ha adottato le misure necessarie ad impedire la commissione di reati del tipo di quello realizzato.

In particolare, se il reato è stato commesso da un soggetto apicale, la responsabilità dell'Ente si presume, in quanto si ritiene che l'illecito sia espressione di una consapevole politica societaria finalizzata alla massimizzazione del profitto.

Tale presunzione può essere superata, ai sensi dell'art. 6 comma 1 lett. a) b) e c) del Decreto 231, se l'Ente dimostra:

1. di aver adottato ed efficacemente attuato un modello di organizzazione idoneo a prevenire illeciti della stessa specie di quello verificatosi: tale modello deve essere sottoposto a verifica periodica relativa al rispetto delle procedure previste e deve essere modificato e corretto al verificarsi di significative violazioni delle prescrizioni in esso contenute;
2. di aver adeguatamente controllato l'applicazione del modello, attraverso l'istituzione di un Organismo di vigilanza;
3. oltre a ciò, che gli autori del reato hanno eluso fraudolentemente il modello organizzativo e il controllo dell'Organismo di vigilanza. Sul punto, la giurisprudenza ha precisato che deve configurarsi un aggiramento della norma di legge, attraverso una condotta ingannevole, falsificatrice, subdola.

A norma dell'art. 7 del Decreto 231, quando il fatto è realizzato da un soggetto sottoposto, la pubblica accusa deve provare che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza da parte degli apicali. Questi obblighi non possono ritenersi violati se prima della commissione del reato l'ente abbia adottato ed efficacemente attuato un modello idoneo a prevenire reati della specie di quello verificatosi (art. 7, comma 2).

Tale modello deve prevedere, in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento delle attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio.

Dunque, l'efficace attuazione del modello richiede, in via principale:

- una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello;
- adeguate iniziative di formazione e informazione del personale.

Occorre considerare che la responsabilità dell'impresa può ricorrere anche se il delitto presupposto si configura nella forma del tentativo (art. 26, decreto 231), vale a dire quando il soggetto agente compie atti idonei in modo non equivoco a commettere il delitto e l'azione non si compie o l'evento non si verifica (art. 56 c.p.). In tal caso, le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà. Inoltre, l'ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento**.**

È importante sottolineare che la responsabilità dell'ente può sussistere anche laddove il dipendente autore dell'illecito abbia concorso nella sua realizzazione con soggetti estranei all'organizzazione dell'ente medesimo.

Tale ipotesi è chiaramente rappresentata nel codice penale e, in particolare, negli artt. 110 c.p. e 113 c.p. Risulta, invece, non altrettanto immediata la sua rilevanza ai fini del decreto 231.

Diversi possono essere i settori di *business* nei quali può annidarsi più facilmente il rischio del coinvolgimento in concorso del dipendente e quindi, ricorrendone i presupposti di interesse e/o vantaggio, dell'ente.

In particolare, rilevano i rapporti connessi agli appalti.

A titolo esemplificativo, si fa riferimento alla possibilità di concorrere a titolo di colpa nei reati presupposto in materia di salute e sicurezza sul lavoro (omicidio e lesioni colpose), laddove alla violazione colposa dell'obbligo della ditta appaltatrice di adottare adeguate misure preventive, cui consegua l'evento delittuoso, abbiano contribuito i criteri economici di aggiudicazione dell'appalto adottati dalla committente o, ancor di più, la violazione dell'obbligo di valutare la congruità dei costi della sicurezza (art. 26, co. 6, d. lgs. n. 81/2008).

Analoghe considerazioni possono essere fatte con riguardo ai reati presupposto in materia ambientale. Si pensi, ad esempio, ai reati in materia di gestione non autorizzata di rifiuti (art. 256,

d. lgs. n. 152/2006), nei casi di mancata valutazione preliminare del committente circa la sussistenza dei requisiti di legge in capo alle ditte potenziali appaltatrici, ovvero di accettazione pedissequa di condizioni economiche di particolare vantaggio, se non addirittura fuori mercato.

Altro ambito da considerare è quello riguardante il rischio di partecipazione concorsuale da parte del committente che manchi di considerare - o escluda in modo non motivato - taluni indici di valutazione previsti per legge ai fini della selezione dei propri *partner* commerciali. In proposito rilevano, ad esempio, le c.d. *white list* previste dalla legge n. 190/2012 e disciplinate dal DPCM del 18 aprile 2013, entrato in vigore il 14 agosto 2013.

Il concorso nel reato può rilevare ai fini della responsabilità dell'ente anche nella particolare ipotesi del c.d. concorso dell'*extraneus* nel reato "proprio". In particolare, la responsabilità in concorso - ai sensi dell'art. 110 c.p. - dell'*extraneus* può ricorrere laddove costui, consapevole della particolare qualifica soggettiva del suo partner criminale (es. pubblico ufficiale, testimone, sindaco, ecc.), concorra nella condotta di reato proprio a quest'ultimo ascrivibile (es. abuso in atti d'ufficio). Tale fattispecie potrebbe realizzarsi, in concreto, nel caso del dipendente di un'impresa che, approfittando di rapporti personali con il funzionario pubblico preposto al rilascio di determinati permessi e/o autorizzazioni, prenda contatto con quest'ultimo per ottenere un provvedimento favorevole nell'interesse dell'impresa, pur consapevole di non averne diritto. In un caso del genere, il dipendente potrebbe supportare il funzionario pubblico fornendogli pareri legali e documenti utili ai fini del perfezionamento del reato. La condotta del funzionario che rilascia il provvedimento non dovuto si inquadrerebbe nella fattispecie dell'abuso d'ufficio (art. 323 c.p.), che si configura come reato "proprio". Tuttavia, il dipendente (e con lui l'impresa nel cui interesse lo stesso abbia agito) risponderebbe a titolo di concorso dell'*extraneus* nel reato "proprio", in quanto nella sua condotta si rinverrebbero:

1. consapevolezza della funzione di pubblico ufficiale del soggetto contattato;
2. consapevolezza dell'antigiuridicità della condotta richiesta;
3. partecipazione attiva alla concretizzazione della condotta stessa.

La casistica sopra richiamata suggerisce l'opportunità di promuovere all'interno dell'impresa un adeguato livello di consapevolezza delle dinamiche realizzative dei reati rilevanti ai fini del decreto 231. Ciò soprattutto per favorire un'attenta selezione e successiva gestione dei propri *partner* e interlocutori, sia pubblici che privati.

Per escludere la responsabilità prevista dal Decreto 231, dunque, occorre:

1. individuare le attività nel cui ambito possono essere commessi i reati;
2. prevedere specifiche regole di comportamento, dirette a prevenire la commissione di illeciti;
3. introdurre un organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
4. prevedere un sistema disciplinare idoneo a sanzionare il mancato rispetto dei protocolli indicati nel modello.

In concreto, dunque, l'esonero da responsabilità dipende dall'esito favorevole del giudizio di idoneità del sistema organizzativo e di controllo effettuato dal Giudice penale, nell'ambito del procedimento giudiziario a carico dell'autore materiale del reato: la formulazione del modello e l'organizzazione dell'organismo di controllo devono dunque porsi come obiettivo l'esito positivo di tale giudizio.

L'art. 8 del Decreto 231 chiarisce che la responsabilità dell'Ente, pur connessa alla commissione di un reato, è da quest'ultimo autonoma. Essa, infatti, sussiste anche quando:

1. l'autore del reato non è identificato o non è imputabile;

2. il reato è estinto per una causa diversa dall'amnistia.

4. Il regime sanzionatorio del Decreto 231

L'accertamento della responsabilità di cui al Decreto 231 determina l'applicazione, in capo all'ente, di gravi sanzioni, che ne colpiscono il patrimonio, l'immagine e la stessa attività.

Sotto il profilo patrimoniale, dall'accertamento dell'illecito dipendente da reato discende sempre l'applicazione di una sanzione pecuniaria e la confisca del prezzo o del profitto del reato, anche per equivalente.

Per quanto attiene le sanzioni pecuniarie, il Decreto 231 istituisce un sistema di quote: per ciascun illecito, la legge determina un numero minimo e massimo di quote, sul modello tradizionale del nostro sistema sanzionatorio.

Ai sensi dell'art. 10 del Decreto 231, il numero di quote non può mai essere inferiore a cento e superiore a mille e l'importo delle singole quote può oscillare tra un minimo di circa 258 euro a un massimo di circa 1.549 euro.

Sulla base di queste indicazioni, il giudice, accertata la responsabilità dell'Ente, determina la sanzione pecuniaria applicabile nel caso concreto, in base alla gravità del fatto, al grado di responsabilità dell'Ente, all'attività eventualmente svolta per riparare le conseguenze dell'illecito commesso e per prevenirne altri.

L'importo delle singole quote è invece determinato in base alle condizioni economiche e patrimoniali dell'Ente, al fine di garantire l'effettività della sanzione.

Nei confronti dell'Ente è inoltre sempre disposta, con la sentenza di condanna (anche in caso di applicazione della pena ex art. 444 c.p.p.), la confisca del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato. Sono fatti salvi i diritti acquisiti dai terzi in buona fede.

A norma dell'ultimo comma dell'art. 6 del Decreto 231, la confisca è prevista anche in caso di assoluzione dell'Ente, allorché il reato "a monte" sia stato commesso da soggetti collocati in posizione apicale nell'ambito della sua organizzazione.

Quando non è possibile eseguire la confisca sui beni costituenti direttamente prezzo o profitto del reato, la stessa può avere a oggetto somme di denaro, beni, o altre utilità di valore equivalente al prezzo o al profitto del reato.

In via cautelare, può essere disposto il sequestro delle cose che, costituendo prezzo o profitto del reato o loro equivalente monetario, sono suscettibili di confisca.

In vista della confisca, può essere disposto il sequestro preventivo: a norma dell'art. 53 comma 1-bis del Decreto 231, in caso di sequestro finalizzato alla confisca per equivalente ex articolo 19, comma 2, il custode giudiziario consente agli organi societari di impiegare società, aziende, titoli, quote azionarie o somme liquide oggetto di sequestro per garantire la continuità e lo sviluppo aziendale. Se tale finalità viene elusa, è prevista la devoluzione di poteri gestori in capo a un amministratore giudiziario.

Nei casi previsti dalla legge, il giudice penale può applicare le sanzioni interdittive, che riguardano l'attività svolta dall'Ente.

A tal fine è necessario che:

1. sia espressamente prevista la possibilità di comminare una sanzione interdittiva a seguito della commissione del reato presupposto, in concreto realizzato;

2. occorre, poi, che il reato dell'apicale abbia procurato all'Ente un profitto di rilevante entità, che il reato del sottoposto sia stato determinato o agevolato da gravi carenze organizzative oppure che vi sia stata reiterazione degli illeciti.

Le sanzioni interdittive possono consistere:

1. nell'interdizione dall'esercizio dell'attività;
2. nella sospensione o nella revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
3. nel divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
4. nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli già concessi;
5. nel divieto di pubblicizzare beni o servizi.

Considerate le ripercussioni di tali sanzioni sulla sopravvivenza dell'Ente, esse devono essere riferite allo specifico settore di attività dell'Ente stesso e devono essere modulate in ossequio ai principi di proporzionalità.

Le sanzioni interdittive non si applicano se, prima della dichiarazione di apertura del dibattimento di primo grado, l'Ente ha riparato le conseguenze del reato, ai sensi dell'art. 17 del Decreto 231.

A tal fine, occorre che l'Ente abbia:

1. risarcito integralmente il danno ed eliminato le conseguenze dannose o pericolose del reato ovvero si sia adoperato – in concreto - in tal senso;
2. adottato e attuato un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi;
3. messo a disposizione il profitto conseguito.

In caso di applicazione delle sanzioni interdittive, il giudice può anche disporre la pubblicazione della sentenza di condanna, in uno o più giornali, per estratto o per intero, unitamente all'affissione nel Comune dove l'Ente ha la sede principale. La pubblicazione è eseguita a cura della Cancelleria del Giudice competente e a spese dell'Ente.

L'art. 22 del Decreto 231 prevede che la prescrizione delle sanzioni amministrative maturi nel termine di 5 anni dalla commissione del reato.

La legge 9 gennaio 2019, n. 3, recante "Misure per il contrasto dei reati contro la pubblica amministrazione e in materia di trasparenza dei partiti e movimenti politici" (cd. legge Spazzacorrotti) ha introdotto una disciplina specifica per l'applicazione delle sanzioni interdittive ad alcuni reati contro la PA, ovvero concussione, corruzione propria semplice e aggravata dal rilevante profitto conseguito dall'ente, corruzione in atti giudiziari, induzione indebita a dare o promettere utilità, dazione o promessa al pubblico ufficiale o all'incaricato di pubblico servizio di denaro o altra utilità da parte del corruttore, istigazione alla corruzione.

In particolare, la legge ha disposto un inasprimento del trattamento sanzionatorio, distinguendo due diverse forbici edittali a seconda della qualifica del reo: le sanzioni interdittive potranno avere una durata compresa tra 4 e 7 anni se il reato è commesso da un soggetto apicale e tra 2 e 4 anni se il colpevole è un soggetto subordinato.

La legge ha invece disposto l'applicazione delle sanzioni interdittive nella misura base di cui all'art. 13, co. 2 del decreto 231 (3 mesi- 2 anni) qualora l'ente, per gli stessi delitti citati e prima della sentenza di primo grado, si sia adoperato per evitare ulteriori conseguenze del reato e abbia collaborato con l'autorità giudiziaria per assicurare le prove dell'illecito, per individuarne i responsabili e abbia attuato modelli organizzativi idonei a prevenire nuovi illeciti e ad evitare le carenze organizzative che li hanno determinati.

Il regime sanzionatorio previsto dal Decreto 231 è il sistema su cui si fonda la misurazione della variabile "impatto" nell'ambito della valutazione del rischio per la cui analisi si rinvia alla sezione I. Parte Speciale.

5. L'Organismo di Vigilanza – composizione, compiti, requisiti, poteri

L'articolo 6 del decreto 231 prevede che l'ente possa essere esonerato dalla responsabilità conseguente alla commissione di reati-presupposto se l'organo dirigente ha, fra l'altro:

a) adottato modelli di organizzazione, gestione e controllo idonei a prevenire i reati considerati;
b) affidato il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo (di seguito "Organismo di vigilanza" o "OdV").

Il conferimento di questi compiti all'Organismo di vigilanza e il corretto ed efficace svolgimento degli stessi sono, dunque, presupposti indispensabili per l'esonero dalla responsabilità.

Peraltro, come ogni componente del modello, anche l'istituzione dell'OdV deve essere guidata dal principio di effettività: non deve rappresentare un adempimento meramente formale.

L'Organismo deve essere posto nelle condizioni di assolvere realmente ai complessi e delicati compiti di cui la legge lo investe.

Per una corretta configurazione dell'Organismo di vigilanza, occorre valutare attentamente i compiti ad esso conferiti dalla legge, nonché i requisiti necessari ai fini dell'adeguato svolgimento di tali compiti, anche alla luce della giurisprudenza maturata sul punto.

La giurisprudenza ha più volte affermato che i suoi componenti devono dimostrare di possedere requisiti di professionalità e onorabilità e devono garantire autonomia decisionale e di iniziativa, indipendenza e continuità di azione.

La previsione di cause di ineleggibilità o decadenza dei membri dell'Organismo di vigilanza può contribuire a selezionare individui effettivamente indipendenti.

Allo scopo di assicurare l'effettiva sussistenza dei requisiti descritti, sia nel caso di un Organismo di vigilanza composto da una o più risorse interne, sia nell'ipotesi in cui esso sia composto anche da figure esterne, è opportuno che i membri possiedano i requisiti soggettivi formali che garantiscano l'autonomia e l'indipendenza richiesta dal compito, come onorabilità, assenza di conflitti di interessi e relazioni di parentela con il vertice.

Tali requisiti di autonomia, onorabilità e indipendenza possono anche essere definiti per rinvio a quanto previsto per altri settori della normativa societaria, ad esempio ai fini della nomina del collegio sindacale.

ANAC ha inoltre ritenuto di escludere che il RPCT possa far parte dell'Organismo di vigilanza, nominato ai sensi del d.lgs. 231/2001 con compiti di vigilanza sul funzionamento e l'osservanza del modello di organizzazione e gestione, considerate le diverse funzioni attribuite dalle rispettive normative di riferimento. È comunque raccomandato dalla stessa ANAC un costante coordinamento nello svolgimento delle attività poste in capo al RPCT e all'OdV.

ANAC ha poi avuto modo di osservare che, alla luce anche di quanto disposto all'art. 6, co. 4-bis, del d.lgs. 231/2001, ove è stabilito che nelle società di capitali il collegio sindacale possa svolgere

le funzioni dell'OdV, l'affidamento dell'incarico di RPCT a un componente del collegio sindacale non sia coerente con l'orientamento formulato nella delibera n. 1134/2017.

Al fine di garantire indipendenza e continuità di azione è necessario che l'OdV:

1. disponga di un budget, assegnato in fase di nomina oppure in un atto successivo;
2. abbia accesso a tutte le informazioni utili e necessarie;
3. non abbia al suo interno soggetti che possano essere coinvolti in processi sensibili in relazione alle fattispecie delittuose individuate nel D.lgs. 231/2001;
4. sia configurato quale organo di staff rispetto ai vertici, non in posizione subordinata.

Sul punto, anche alla luce della giurisprudenza più recente, è necessario che, nell'ambito dell'Organismo, non si sovrappongano la figura del controllore e quella del controllato: e dunque preferibile non includere fra i componenti i dirigenti di settore, che hanno compiti operativi in un'area a rischio reato.

Il Decreto 231 non pone vincoli riguardo alla composizione, monocratica o collegiale, dell'OdV: la prima, in genere, è adottata negli Enti di piccole dimensioni. Nel caso di organismo collegiale è da preferire l'opzione che vede coinvolti sia componenti interni che esterni.

Nelle società di capitali, le funzioni di OdV possono essere esercitate dal Collegio sindacale ovvero dal Consiglio di sorveglianza o dal Comitato per il controllo sulla gestione (art. 6 comma 4 e 4 bis del Decreto 231). In ogni caso, è possibile prevedere la partecipazione di un membro del collegio sindacale, per garantire un raccordo tra l'organo di controllo e l'Organismo di Vigilanza.

Negli Enti di piccole dimensioni, è possibile far coincidere l'OdV con l'organo dirigente, ma occorre valutare questa opzione con estrema cautela, in ragione del possibile insorgere di conflitti di interessi all'interno dello stesso organo dirigente, che diventerebbe controllore e controllato.

Normalmente, l'Organismo resta in carica di tre anni. Può essere revocato dall'organo dirigente solo per giusta causa, ovvero per grave negligenza nell'assolvimento dei compiti assegnati.

Nel caso della SRM, alla data di redazione del presente documento, l'OdV è di tipo collegiale e la sua composizione coincide con quella del collegio sindacale. In merito ai requisiti soggettivi formali che garantiscono l'autonomia e l'indipendenza richiesta dal compito, come onorabilità, assenza di conflitti di interessi e relazioni di parentela con il vertice, per l'OdV della SRM viene fatta valere l'analisi dei requisiti effettuata per la nomina del collegio sindacale che viene nominato dall'Assemblea dei soci. La nomina è effettuata dall'organo amministrativo. La durata della carica è

triennale e coincide con quella del collegio sindacale, seppur con possibili differenze in termini di efficacia, data la diversa sede di nomina.

All'OdV spetta la funzione di:

1. vigilare sull'effettività, sull'adeguatezza, sul funzionamento e sul rispetto del MOG, attraverso indagini anche a sorpresa[1] tra cui, ad es., verifiche sulle operazioni finanziarie, controlli contabili, ispezioni, verifica della regolarità dei moduli previsti dai protocolli, verifica in ordine alla conoscenza e rispetto delle procedure, controlli sulla tenuta del codice etico, ecc.;
2. collaborare con il management per rendere effettivo il MOG e curare il suo concreto recepimento all'interno dell'Ente;
3. provvedere al suo aggiornamento, in particolare a fronte di significative violazioni delle prescrizioni o quando intervengono mutamenti nell'organizzazione o nelle attività dell'Ente (art. 7 comma 4 del Decreto 231), attraverso:

- suggerimenti e proposte di adeguamento del modello agli organi o funzioni aziendali in grado di dare loro concreta attuazione nel tessuto aziendale, a seconda della tipologia e della portata degli interventi: le proposte riguardanti aspetti formali o di minore rilievo saranno rivolte alla funzione del Personale e Organizzazione o all'Amministratore, mentre negli altri casi di maggiore rilevanza verranno sottoposte all'Organo amministrativo;
- follow-up: verifica dell'attuazione e dell'effettiva funzionalità delle soluzioni proposte;

4. svolgere attività di informazione e formazione aventi a oggetto il Decreto 231 e il MOG;
5. promuovere l'esercizio dell'azione disciplinare;
6. rilasciare l'attestazione sulla trasparenza secondo le indicazioni fornite da ANAC.

L'OdV si caratterizza per essere un organismo dell'Ente, dotato di autonomi poteri di iniziativa e controllo.

Le attività poste in essere dall'OdV non possano essere sindacate da alcun altro organismo o struttura aziendale, fermo restando che l'Amministratore Unico vigila sull'adeguatezza del suo

[1] Tribunale di Milano, GIP Secchi, ordinanza 09 novembre 2004 - Esame dell'idoneità dei modelli di organizzazione, gestione e controllo ex artt 6 e 7 d.lg. 231/2001

intervento, poiché ad esso compete la responsabilità ultima del funzionamento (e dell'efficacia) del Modello organizzativo.

L'OdV 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 decreto 231.

L'OdV può avvalersi, sotto la sua diretta sorveglianza e responsabilità, dell'ausilio di tutte le strutture della società, ovvero di consulenti esterni.

Peraltro, nel contesto delle procedure di formazione del budget aziendale, l'organo amministrativo dovrà approvare una dotazione adeguata di risorse finanziarie, proposta dall'OdV, della quale quest'ultimo potrà disporre per ogni esigenza necessaria al corretto svolgimento dei compiti (es. consulenze specialistiche, trasferte), salvo che tale budget non venga già previsto in sede di assegnazione dell'incarico.

Al fine di svolgere adeguatamente tali funzioni, l'OdV deve dettagliatamente e tempestivamente essere informato di quanto accade all'interno dell'Ente e riferire all'Amministratore Unico e agli altri organi di controllo.

Il MOG deve dunque disciplinare:

1. i flussi informativi che devono essere attivati, presso tutti i componenti dell'Ente, a fronte di particolari eventi (provvedimenti assunti dalla polizia giudiziaria o da altre autorità, procedimenti disciplinari, ecc.), c.d. flussi a evento;
2. i flussi informativi periodici provenienti dai soggetti con funzioni di controllo dei processi cd. sensibili e prevedere che le informazioni si muovano in modo bidirezionale.

A sua volta, l'OdV deve trasmettere agli organi di vertice report periodici dell'attività svolta, informandoli tempestivamente a fronte di eventuali violazioni del MOG o della necessità di aggiornare tale documento.

In particolare, sono previste relazioni periodiche, di regola, almeno a cadenza annuale, dall'OdV verso l'organo amministrativo, fatti salvi report aggiuntivi infrannuali ritenuti opportuni dall'OdV.

La relazione informativa annuale da destinare all'organo amministrativo riguarda le attività di verifica e controllo compiute e l'esito delle stesse e la programmazione delle attività principali.

La relazione annuale deve essere trasmessa anche al collegio sindacale ove non coincidente con l'OdV.

In ordine allo scambio di informazioni fra organi di controllo, quando non coincidenti, si rinvia alle Norme di Comportamento del collegio sindacale.

La definizione degli aspetti attinenti alla continuità dell'azione dell'Organismo di vigilanza, quali la calendarizzazione dell'attività, la verbalizzazione delle riunioni e la disciplina dei flussi informativi dalle strutture aziendali all'OdV stesso potrà essere rimessa a quest'ultimo, il quale dovrà disciplinare il proprio funzionamento interno tramite un Regolamento delle proprie attività (determinazione delle cadenze temporali dei controlli, individuazione dei criteri e delle procedure di analisi, ecc.).

Non è, invece, consigliabile che tale regolamento sia redatto e approvato da organi societari diversi dall'OdV in quanto ciò potrebbe metterne in dubbio l'indipendenza.

Nell'ottica di assicurare l'effettività delle attività poste in essere dall'Organismo di vigilanza, è necessario che lo stesso garantisca la tracciabilità e la conservazione della documentazione delle attività svolte (verbali delle riunioni, relazioni o informative specifiche, report inviati o ricevuti, risultanze delle istruttorie relative alle segnalazioni, ecc.).

6. Obblighi di informazione nei confronti dell'Organismo di vigilanza – i flussi informativi

L'art. 6, comma 2, lettera d) del Decreto 231 prevede obblighi di informazione nei confronti dell'Organismo di vigilanza.

Su questo aspetto, la Relazione di accompagnamento al Decreto non fornisce ulteriori chiarimenti.

L'obbligo di informazione all'OdV sembra concepito quale ulteriore strumento per agevolare l'attività di vigilanza sull'efficacia del Modello e di accertamento a posteriori delle cause che hanno reso possibile il verificarsi del reato.

Se questo è lo spirito della prescrizione normativa, allora è da ritenere che l'obbligo di fornire informazioni all'OdV sia rivolto alle funzioni aziendali e riguardi:

a) le risultanze periodiche dell'attività di controllo dalle stesse posta in essere per dare attuazione ai modelli (report riepilogativi dell'attività svolta, attività di monitoraggio, indici consuntivi, ecc.);

b) le anomalie o atipicità riscontrate nell'ambito delle informazioni disponibili (un fatto non rilevante, se singolarmente considerato, potrebbe assumere diversa valutazione in presenza di ripetitività o estensione dell'area di accadimento).

Tali informazioni potranno riguardare, ad esempio:

- le decisioni relative alla richiesta, erogazione e utilizzo di finanziamenti pubblici;
- le richieste di assistenza legale inoltrate dai dirigenti e/o dai dipendenti nei confronti dei quali la Magistratura procede per i reati previsti dalla richiamata normativa;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati di cui al decreto 231;
- le commissioni di inchiesta o relazioni interne dalle quali emergano responsabilità per le ipotesi di reato di cui al decreto 231;
- le notizie relative all'effettiva attuazione, a tutti i livelli aziendali, del modello organizzativo, con evidenza dei procedimenti disciplinari svolti e delle eventuali sanzioni irrogate ovvero dei provvedimenti di archiviazione di tali procedimenti con le relative motivazioni;
- gli esiti dei controlli - preventivi e successivi - che sono stati effettuati nel periodo di riferimento, sugli affidamenti a operatori del mercato, a seguito di gare a livello nazionale ed europeo, ovvero a trattativa privata;
- gli esiti del monitoraggio e del controllo già effettuato nel periodo di riferimento, sulle commesse acquisite da enti pubblici o soggetti che svolgano funzioni di pubblica utilità;
- copia della reportistica periodica in materia di salute e sicurezza sul lavoro.

Con particolare riferimento ai flussi informativi periodici provenienti dal management, se prevedono l'obbligo di comunicare gli esiti di controlli già effettuati e non la trasmissione di informazioni o documenti da controllare, tali flussi periodici fanno chiarezza sui diversi ruoli in materia di prevenzione.

Infatti, se ben definiti, i flussi informativi precisano che il *management* deve esercitare l'azione di controllo, mentre l'OdV - quale meccanismo di *assurance* - deve valutare i controlli effettuati dal *management*. Peraltro, l'obbligo di riferire gli esiti dei controlli all'OdV, produce un effetto di responsabilizzazione del *management* operativo.

Le informazioni fornite all'Organismo di vigilanza mirano a consentirgli di migliorare le proprie attività di pianificazione dei controlli e non, invece, ad imporgli attività di verifica puntuale e sistematica di tutti i fenomeni rappresentati. In altre parole, all'OdV non incombe un obbligo di agire, essendo rimesso alla sua discrezionalità (e responsabilità) di stabilire in quali casi attivarsi.

L'obbligo di informazione è stato probabilmente previsto anche allo scopo di conferire maggiore autorevolezza alle richieste di documentazione che si rendono necessarie all'Organismo di vigilanza nel corso delle sue verifiche.

7. Il Modello di organizzazione, gestione e controllo

L'adozione di un modello di organizzazione, gestione e controllo (d'ora in avanti MOG) rappresenta l'unico strumento che consente l'esonero dalla responsabilità dell'Ente, a fronte della commissione di un reato presupposto da parte di un soggetto apicale o subordinato, nel suo interesse o a suo vantaggio.

Il Decreto 231 non fornisce, tuttavia, indicazioni specifiche su come tale modello debba essere costruito.

Le Linee guida di Confindustria pubblicate nel giugno del 2021 e Linee guida di Fise Assoambiente pubblicate nel 2020 si propongono di fornire chiarimenti sulla metodologia da utilizzare e suggerimenti operativi.

Se il MOG è stato adottato ed efficacemente attuato prima della commissione di un reato presupposto (cd. MOD *ante factum)*, può esonerare l'Ente dalla connessa responsabilità. Se è adottato dopo il verificarsi del reato presupposto (cd. MOG *post factum*), può comportare un'attenuazione del trattamento sanzionatorio applicabile all'Ente stesso.

In ogni caso, il MOG è un atto proveniente dal vertice dell'ente, costituito da un insieme di procedure volte a disciplinare l'organizzazione, la gestione e il controllo dell'attività aziendale, al fine di prevenire (o, quanto meno, mitigare) il rischio della commissione di reati presupposto.

La finalità del documento non è tanto l'eliminazione totale del rischio della commissione di illeciti, quanto l'abbassamento del rischio che venga commesso un illecito nell'ambito dell'attività aziendale.

L'impostazione del Decreto 231 è del tutto coerente con la riforma del diritto societario operata dai D.lgs. 5 e 6/2003 che ha elevato i principi di corretta amministrazione a clausola generale di comportamento degli amministratori.

In questo senso i Modelli organizzativi ex D.lgs. 231/2001 sono ormai ascritti sistematicamente a quelle norme del diritto societario (e in particolare dell'art. 2381, commi 3 e 5 c.c. e all'art. 2403

c.c., nonché dell'art. 2086 c.c. come emendato con la riforma della crisi d'impresa e dell'insolvenza) che sanciscono il principio di adeguatezza nel governo societario.
La stessa riforma ha elevato il format degli «adeguati assetti organizzativi» (artt. 2381 e 2403 c.c.) a canone necessario di organizzazione interna dell'impresa, sul piano gestionale - amministrativo – contabile quale: (i) strumento fondamentale di tracciabilità dei processi; (ii) criterio di valutazione di responsabilità di amministratori, dirigenti, organi preposti al controllo.

Destinatari del MOG sono i dipendenti dell'Ente, i componenti degli organi sociali e del *management*, mentre con i soggetti terzi che intrattengono rapporti con l'Ente è opportuno stipulare un contratto che preveda l'impegno dei terzi a osservare il MOG e il codice etico dell'Ente.
L'art. 6 comma 2 del Decreto 231 si limita a prevedere alcuni criteri generali da seguire nella costruzione dei modelli:

1. individuare, tramite un'apposita analisi di rischio, le cd. attività sensibili nel cui ambito possono essere commessi i reati;
2. prevedere specifici protocolli volti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;
3. individuare modalità di gestione delle risorse finanziarie idonee a impedire la commissione dei reati;
4. prevedere obblighi di informazione nei confronti dell'Organismo di vigilanza;
5. introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle procedure indicate nel modello.

Per poter approntare un efficace sistema di gestione del rischio reato è necessario svolgere, preliminarmente, un *check up* finalizzato a raggiungere un grado sufficiente di conoscenza dell'Ente, seguito da un'altrettanto adeguata analisi del rischio, finalizzata alla rilevazione delle aree su cui intervenire.
Tale attività si fonda sulla conoscenza del rischio e serve per:

1. ponderare i rischi;
2. assumere decisioni sulla necessità o meno di trattarli;
3. definire strategie e azioni per il loro trattamento.

Per poter svolgere al meglio tale attività, occorre conoscere ed esaminare in modo approfondito:

1. il contesto in cui opera l'Ente;
2. la sua storia;
3. le dimensioni e la complessità dello stesso;
4. la struttura organizzativa e la ripartizione dei poteri;
5. il numero e il tipo di attività svolte;
6. gli interlocutori e i partner;
7. l'esistenza di altri sistemi di gestione di rischi aziendali.

L'indagine su tali aspetti può essere effettuata attraverso:

1. interviste;
2. sopralluoghi;
3. raccolta di documenti aziendali (ad es. statuto, organigramma, schede enti soci, consultazione sito sez. "Società Trasparente", il sistema delle misure adottate, visura camerale).

In questo contesto, occorre tenere presente che, in via generale, il rischio è considerato a*ccettabile* quando i controlli aggiuntivi costano più della risorsa da proteggere.

Rispetto all'ampio catalogo di reati presupposto di cui al Decreto 231 è possibile, di volta in volta, escludere:

1. i reati che si caratterizzano per l'assenza di qualunque rischio di verificazione, in relazione alle caratteristiche e alle attività svolte dall'Ente;
2. i reati per cui non è plausibile possa sussistere il movente dell'interesse o vantaggio dell'Ente.

Fermo restando il ruolo fondamentale del dirigente - occorre, quanto meno:

1. approntare un'efficace comunicazione delle regole e delle procedure contenute nel MOG, rivolta sia all'interno che all'esterno dell'Ente;
2. sviluppare un programma di formazione sul Decreto 231 e sul MOG.

È fondamentale, inoltre, che l'Amministratore Unico curi l'aggiornamento e il miglioramento continuo del modello, anche su sollecitazione dell'OdV.

SIAT 231

SISTEMA INTEGRATO

Anticorruzione

Trasparenza

Modello di Organizzazione e Gestione (MOG) 231

ai sensi della L. 190/2012 e D.LGS 33/2013

come modificati dal D.LGS 97/2016

e del

decreto legislativo 8 giugno 2001, n. 231

SEZIONE I. MOG 231

PARTE SPECIALE

Processo	Ruolo	Nominativo	Data
Predisposto da	Coordinatore 231; Responsabile della Prevenzione della Corruzione e Responsabile Trasparenza	Giuseppe Liguori Giorgio Fiorillo Raffaella Ruggiero	07/04/2022
Inviato in visione	Dirigente - Amministratore Unico -Enti soci- Collegio Sindacale- OdV		07/04/2022
Adottato	Amministratore Unico con decisione n. 08/22	Amelia Luca	11/04/2022

Versione n.	Motivo della revisione	Data
0.0	Proposta	07/04/2022
1.0	Versione adottata	11/04/2022

Indice

0. Premesse.

Il SIAT 231 ("Sistema" nella sua accezione più ampia) della SRM è composto da 2 sezioni con i relativi allegati.

Sezione I. MOG 231:

- **Parte generale:** è descritto l'obiettivo che si intende raggiungere con il SIAT231 e gli aspetti fondanti del MOG231.
- **Parte speciale:** si analizzano le diverse fattispecie di reato e la loro relazione con i processi aziendali procedendo con la mappatura dei processi aziendali, la valutazione del rischio e l'individuazione delle misure correttive e di controllo.

Sezione II. PTPCT

- **Parte Anticorruzione e trasparenza**, è descritto il profilo societario della SRM e il contesto esterno ed interno, le normative alla base del Piano anticorruzione e trasparenza; il processo di adozione del documento; i ruoli all'interno della società e gli strumenti organizzativi di attuazione e controllo sul tema dell'anticorruzione e trasparenza; le misure integrative per l'anticorruzione e la trasparenza, il monitoraggio e le misure programmate.

Infine il SIAT 231 è integrato dalla documentazione interna costituita dal Manuale integrato, dalle Procedure adottate dalla SRM con il Sistema Qualità e dai Regolamenti che verranno progressivamente aggiornati ed uniformati.

1. Il contesto in cui opera SRM e le attività che svolge

Ai fini della redazione del Modello che risulta integrato con il PTPCT (nella sezione II PTPCT sono ampiamente descritte le funzioni della società e le caratteristiche organizzative) si è proceduto ad esaminare i seguenti aspetti:

1. il contesto in cui opera l'ente
2. la sua storia;
3. le dimensioni e la complessità dello stesso;
4. la struttura organizzativa e la ripartizione dei poteri;
5. il numero e il tipo di attività svolte;
6. gli interlocutori e i partner;

7. l'esistenza di altri sistemi di gestione di rischi aziendali.

L'indagine su tali aspetti è stata effettuata attraverso:

1. creazione di un team di lavoro interno che ha supportato tutte le fasi necessarie per l'analisi dei processi aziendali, l'individuazione delle misure e di quelle da programmare, e la valutazione del rischio;
2. interviste, anche mediante la somministrazione di questionari, sviluppate di concerto con il team di lavoro e con il personale di volta in volta coinvolto con i processi mappati;
3. raccolta di documenti aziendali, in parte disponibili sul sito istituzionale in Società Trasparente.

2. La mappatura dei processi

Oltre alla rilevazione dei dati generali relativi alla struttura e alla dimensione organizzativa, l'aspetto centrale e più importante è la cosiddetta mappatura dei processi, consistente nella individuazione e analisi dei processi organizzativi, la c.d. "autoanalisi organizzativa".

L'obiettivo è che l'intera attività svolta dall'ente venga gradualmente esaminata al fine di identificare aree che, in ragione della natura e delle peculiarità dell'attività stessa, risultino potenzialmente esposte a rischi.

Partendo dalle attività sopra elencate si è provveduto a mappare i processi aziendali secondo un approccio integrato 231/190 coinvolgendo il personale di volta in volta interessato, compiendo un'auto-analisi organizzativa.

Un processo può essere definito come una sequenza di attività interrelate ed interagenti che trasformano delle risorse in un output destinato ad un soggetto interno o esterno all'ente (utente).

L'identificazione dei processi è il primo passo da realizzare per uno svolgimento corretto della mappatura dei processi e consiste nello stabilire l'unità di analisi (il processo) e nell'identificazione dell'elenco completo dei processi svolti dall'organizzazione che, nelle fasi successive, dovranno essere accuratamente esaminati e descritti.

In altre parole, in questa fase l'obiettivo è quello di definire la lista dei processi che devono essere oggetto di analisi e approfondimento nella successiva fase.

Per le mappature si veda l'Allegato 1.

Ogni processo aziendale è stato analizzato in un'ottica integrata 231/190 considerando i seguenti aspetti:

- soggetto/funzione coinvolta;
- rischio corrispondente istituendo il c.d. Registro del rischio come suggerito da ANAC nell'allegato 1 al PNA2019;
- fattore abilitante al rischio corrispondente come suggerito da ANAC nell'allegato 1 al PNA2019;
- reato 231 o famiglia di reato 231 corrispondente, considerato che i rischi corruttivi rientrano all'interno dei reati 231 benché con un'accezione più ampia che va oltre al reato penale;
- valutazione del rischio in termini di impatto e probabilità al netto delle misure esistenti;
- pianificazione temporale di misure correttive/da integrare/da istituire.

Tali aspetti possono servire anche per altre finalità per le quali la mappatura dei processi può essere realizzata (es. governo societario, controllo di gestione, ripartizione dei carichi di lavoro, ecc.). Pertanto, essa può rappresentare un utile strumento di gestione, in un'ottica di semplificazione, di integrazione e coordinamento con gli altri strumenti gestionali dell'ente.

3. La valutazione del rischio: i reati 231 esclusi dal Modello integrato 231/190

L'approccio utilizzato è stato quello di individuare preliminarmente le aree di attività, scomporre le aree di attività in processi e collegare ai processi dettagliati in fasi i reati/famiglie di reato previste dal decreto 231, abbinando i processi ai possibili reati.

Dunque, la valutazione dei rischi 231 è stata effettuata partendo dalle aree e dalla scomposizione per ogni area individuata in processi.

Preliminarmente all'analisi dei processi e alla valutazione dei rischi, è stata effettuata una ricognizione dei reati presenti nel catalogo 231, art. 24 e seguenti, al fine di escludere:

- i reati che si caratterizzano per un rischio di verificazione remoto, in relazione alle caratteristiche e alle attività svolte da SRM;
- i reati per cui non è plausibile possa sussistere il movente dell'interesse o vantaggio dell'Ente.

A tal fine si veda la tavola allegata Risk Analysis Reati esclusi e compresi (Tav. 1).

4. La valutazione del rischio: i reati 231 compresi nel Modello integrato 231/190

I reati compresi nel Modello sono quelli indicati nella tavola allegata Risk Analysis (Tav. 2) . Le tavole 3 e 4 collegano i reati 231 dettagliati (tav. 3) e i reati 231 generali (tav. 4) con le aree mappate declinate in processi.

Segue una disamina dei reati compresi nel Modello 231.

Art. 24 D.lgs. n. 231/2001- Malversazione a danno dello Stato (art. 316 bis c.p.), indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.), frode nelle pubbliche forniture (art 356 c.p.), truffa aggravata a danno dello Stato (art. 640 c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.), frode informatica (art. 640 ter c.p.)

Art. 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo provvedimento inserito: Legge 238/2021)	Reato presupposto	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOT (automatico)	Giudizio Qualitativo
24	Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture	Malversazione a danno dello Stato (art. 316-bis c.p.)	600	3	C/D/E	4	3,5	Medio-Alto
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	Indebita percezione di erogazioni a danno dello Stato (art. 316-ter c.p.) [modificato dalla L. n. 3/2019]	600	3	C/D/E	4	3,5	Medio-Alto
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	Truffa in danno dello Stato o di altro ente pubblico o delle Comunità europee (art. 640, comma 2, n.1, c.p.)	600	3	C/D/E	4	3,5	Medio-Alto
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	Truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640- bis c.p.)	600	3	C/D/E	4	3,5	Medio-Alto

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	Frode informatica in danno dello Stato o di altro ente pubblico (art. 640- ter c.p.)	600	3	C/D/E	4	3,5	Medio-Alto
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	Frode nelle pubbliche forniture (art. 356 c.p.) [articolo aggiunto dal D.Lgs. n. 75/2020]	600	3	C/D/E	4	3,5	Medio-Alto

I reati di indebita percezione di erogazioni a danno dello Stato (art. 316 ter c.p.), frode nelle pubbliche forniture (art 356 c.p.), truffa aggravata a danno dello Stato (art. 640 c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.), hanno in comune il fatto che viene tratta in errore la P.A., al fine di conseguire un ingiusto profitto.

Ciò posto, i reati di truffa aggravata richiedono la realizzazione di artifici e raggiri, mentre per l'indebita percezione è sufficiente aver utilizzato o presentato dichiarazioni non veritiere o aver omesso informazioni dovute al fine di conseguire contributi o finanziamenti da parte dello Stato.

Questo tipo di reati si perfeziona con la prima percezione del contributo pubblico, ma permane fino alla cessazione della condotta criminosa, con l'ultimo incasso del finanziamento.

Per quanto attiene alla frode informatica, il reato rileva ai fini della responsabilità ai sensi del Decreto 231 solo se, attraverso l'alterazione del funzionamento di un sistema informatico o la manipolazione dei dati in esso contenuti, si ottiene un ingiusto profitto e si determina un danno allo Stato o ad altro Ente pubblico.

Sotto il profilo sanzionatorio, in caso di condanna è prevista la sanzione pecuniaria fino a 500 quote. Nelle ipotesi aggravate, la sanzione è compresa tra 200 e 600.

In presenza dei requisiti di cui all'art. 13 del Decreto 231, si applicano anche le sanzioni interdittive del divieto di contrarre con la P.A., dell'esclusione di agevolazioni finanziamenti contributi o sussidi e dell'eventuale revoca di quelli già concessi, oltre che il divieto di pubblicizzare beni o servizi.

I reati di truffa ai danni dello Stato e indebita percezione comportano, in caso di condanna, la confisca, anche per equivalente, nei confronti dell'ente imputato oltre che la confisca obbligatoria ai sensi dell'art. 640 quater c.p..

L'art. 24 del Decreto 231 è stato oggetto di modifiche ad opera del D.Lgs. 75/2020 (in vigore da 30 luglio 2020) il quale ha aggiunto, fra le molte cose, il delitto di frode nelle pubbliche forniture ex art. 356 c.p. fra i reati presupposto.

La fattispecie punisce chiunque commette frode nell'esecuzione di contratti di fornitura conclusi con lo Stato, con un ente pubblico, o con un'impresa esercente servizi pubblici o di pubblica necessità.

Per "contratto di fornitura" si intende ogni strumento contrattuale destinato a fornire alla P.A. beni o servizi. Il delitto di frode nelle pubbliche forniture è infatti ravvisabile non soltanto nella fraudolenta esecuzione di un contratto di somministrazione (art. 1559 c.c.), ma anche di un contratto di appalto (art. 1655 c.c.); l'art. 356 c.p., infatti, punisce tutte le frodi in danno della pubblica amministrazione, quali che siano gli schemi contrattuali in forza dei quali i fornitori sono tenuti a particolari prestazioni (Cass., VI, 27 maggio 2019).

Con riferimento alla condotta punibile, a differenza dell'art. 355 c.p., nel quale rileva il mero inadempimento contrattuale consistente nella mancata o ritardata consegna delle cose dovute, nell'ipotesi di frode nelle pubbliche forniture il mero inadempimento contrattuale non determina la consumazione del reato in esame, in quanto la condotta tipica presuppone anche la fraudolenta dissimulazione operata in danno del contraente pubblico (Cass. pen. Sez. VI Sent., 23-11-2017, n. 9081). La norma richiede, infatti, la sussistenza della malafede contrattuale, ovvero la presenza di un espediente malizioso o di un inganno, tali da far apparire l'esecuzione del contratto conforme agli obblighi assunti (Cass., VI, 11 febbraio 2011, n. 5317).

Quanto all'elemento soggettivo, la giurisprudenza ritiene sufficiente il dolo generico, costituito dalla consapevolezza di consegnare cose in tutto o in parte difformi (per origine, provenienza, qualità o quantità) in modo significativo dalle caratteristiche convenute

Anche per le nuove fattispecie ora richiamate dall'art. 24 è prevista l'applicazione della circostanza aggravante prevista dal comma 2 (per il caso in cui l'Ente abbia conseguito un profitto di rilevante entità ovvero dall'illecito sia derivato un danno di particolare gravità: in questo caso la sanzione

pecuniaria sarà da 200 a 600 quote) e delle sanzioni interdittive previste dal co. 3, che richiama l'art. 9, co. 2, lett. c), d), ed e), ossia: il divieto di contrattare con la P.A. (salvo che per ottenere 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.

In considerazione di tali elementi, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo sono:

- Codice etico
- Sistema sanzionatorio
- Check list di controllo controparti
- Controllo gerarchico
- Trasparenza
- Formalizzazione di una reportistica relativa al rapporto intercorso, salvo che non sia già predisposta apposita documentazione dalla controparte
- Raccolta, verifica e approvazione della documentazione da trasmettere
- Controlli di completezza e correttezza della documentazione da presentare
- Gestione password di abilitazione per l'accesso a sistemi informativi della PA
- Segregazione
- Whistleblowing
- Tracciabilità finanziaria
- Verifica requisiti operatori economici

Art. 24 bis D.lgs. n. 231/2001 - Delitti informatici e trattamento illecito dei dati

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo provvediment	Reato presupposto	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo

	o inserito: Legge 238/2021)							
24bis	Delitti informatici e trattamento illecito di dati	Documenti informatici (art. 491-bis c.p.)	400	2	C/D/E	4	3,0	Medio
24bis	Delitti informatici e trattamento illecito di dati	Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)	500	3	A/B/E	5	4,0	Medio-Alto
24bis	Delitti informatici e trattamento illecito di dati	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)	300	2	B/E	3	2,5	Medio-Basso
24bis	Delitti informatici e trattamento illecito di dati	Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)	300	2	B/E	3	2,5	Medio-Basso
24bis	Delitti informatici e trattamento illecito di dati	Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)	500	3	A/B/E	5	4,0	Medio-Alto
24bis	Delitti informatici e trattamento illecito di dati	Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)	500	3	A/B/E	5	4,0	Medio-Alto
24bis	Delitti informatici e trattamento illecito di dati	Danneggiamento di informazioni, dati e programmi informatici (art. 635- bis c.p.)	500	3	A/B/E	5	4,0	Medio-Alto

24bis	Delitti informatici e trattamento illecito di dati	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter c.p.)	500	3	A/B/E	5	4,0	Medio-Alto
24bis	Delitti informatici e trattamento illecito di dati	Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)	500	3	A/B/E	5	4,0	Medio-Alto
24bis	Delitti informatici e trattamento illecito di dati	Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)	500	3	A/B/E	5	4,0	Medio-Alto
24bis	Delitti informatici e trattamento illecito di dati	Frode informatica del certificatore di firma elettronica (art. 640-quinquies c.p.)	400	2	C/D/E	4	3,0	Medio
24bis	Delitti informatici e trattamento illecito di dati	Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)	400	2	C/D/E	4	3,0	Medio

L'articolo 24-bis del decreto 231 ha esteso la responsabilità amministrativa delle persone giuridiche e degli enti alla quasi totalità dei reati informatici.

Si tratta di fattispecie introdotte con la L. 48/2008, che riguardano i delitti in materia di violazione della privacy, previsti dal D.lgs. 196/2003, (il richiamo al Codice Privacy riguarda i delitti di cui alla Parte III, Titolo III, Capo II), ovvero:

1. trattamento illecito dei dati, ex art. 1673;
2. falsità nelle dichiarazioni e notificazioni al garante, di cui all'art. 1684;
3. inosservanza dei provvedimenti del Garante, di cui all'art. 170.

Nello specifico, la norma prevede le seguenti fattispecie:

1. falsificazione di documenti informatici da parte di Enti che procedono a rendicontazione elettronica di attività;
2. cancellazione o alterazione di informazioni a valenza probatoria presenti sui propri sistemi, allo scopo di eliminare le prove di un altro reato (es. l'Ente ha ricevuto un avviso di garanzia per un reato e procede ad eliminare le tracce elettroniche del reato stesso);
3. falsificazione di documenti informatici contenenti gli importi dovuti dall'Ente alla P.A. nel caso di flussi informatizzati dei pagamenti tra privati e P.A. (es. riduzione degli importi) o alterazione dei documenti in transito nell'ambito del SIPA (Sistema Informatizzato pagamenti della P.A.) al fine di aumentare gli importi dovuti dalla P.A. all'Ente;
4. falsificazione di documenti informatici compiuta nell'ambito dei servizi di Certification Authority da parte di un soggetto che rilasci certificati informatici, aventi valenza probatoria, corrispondenti a false identità o attestanti falsi titoli professionali;
5. falsificazione di documenti informatici correlata all'utilizzo illecito di dati identificativi altrui nell'esecuzione di determinate operazioni informatiche o telematiche in modo che queste risultino eseguite dai soggetti legittimi titolari dei dati (es. attivazione di servizi non richiesti);
6. rilascio di certificati digitali da parte di un Ente certificatore senza che siano soddisfatti gli obblighi previsti dalla legge per il rilascio di certificati qualificati (es. identificabilità univoca del titolare, titolarità certificata), con lo scopo di mantenere un alto numero di certificati attivi;
7. aggiramento dei vincoli imposti dal sistema per la verifica dei requisiti necessari al rilascio dei certificati da parte dell'amministratore di sistema allo scopo di concedere un certificato e produrre così un guadagno all'Ente.

Per non incorrere nelle pesanti sanzioni previste dalla norma, occorre dunque considerare e prevenire tali delitti. Sul punto, peraltro, si segnala la sentenza emessa il 5/9/2017 della Grande Camera della Corte Europea dei Diritti dell'Uomo di Strasburgo, che ha dichiarato meritevole di precise tutele la vita privata del lavoratore, sancendo come arbitraria e contraria al diritto alla vita privata e alla corrispondenza del dipendente, la condotta del datore che controlla illegittimamente le sue e-mail.

Pur in presenza di tale orientamento giurisprudenziale, peraltro, resta ferma la possibilità che il datore di lavoro limiti i tempi di accesso o ponga dei filtri escludendo, ad esempio, la possibilità di poter accedere ai social network. Tali provvedimenti sono da considerarsi legittimi, anche alla luce delle Linee Guida per posta elettronica e internet emesse dal Garante della Privacy nel 2007.

Le sanzioni previste per tali reati sono quella pecuniaria, fino a 500 quote, e quelle interdittive.

Alla luce dei presupposti applicativi del decreto, gli enti saranno considerati responsabili per i delitti informatici commessi nel loro interesse o a loro vantaggio da persone che rivestono funzioni di rappresentanza, amministrazione, direzione dell'ente o di una sua unità organizzativa, ma anche da persone sottoposte alla loro direzione o vigilanza.

Lo sviluppo della tecnologia informatica ha generato nel corso degli anni modifiche sostanziali nell'organizzazione del business di impresa e ha inciso sensibilmente sulle opportunità a disposizione di ciascun esponente aziendale per realizzare o occultare non soltanto schemi di condotte criminali già esistenti ma anche fattispecie nuove, tipiche del cd. mondo virtuale.

A ciò si aggiunga l'ingresso massivo di dispositivi mobili (es. *tablet* e *smartphone*), l'utilizzo di server di *cloud* (per esempio servizi di memorizzazione e archiviazione dei dati distribuiti su reti e server remoti) che:

- moltiplicano le opportunità di realizzazione di un reato informatico;
- introducono criticità in relazione al loro utilizzo aziendale;
- determinano la necessità per le imprese di adeguarsi rapidamente al fine di disciplinare correttamente la gestione di tali fenomeni.

Quanto ai soggetti maggiormente esposti a tale fattispecie di reato, tale fenomeno può potenzialmente coinvolgere qualsiasi ente che utilizzi in maniera rilevante gli strumenti informatici e telematici per lo svolgimento delle proprie attività. É chiaro, tuttavia, che tale categoria di reato risulta di più probabile accadimento in quei settori attivi nell'erogazione di servizi legati all'*Information Technology* (es. gestione delle infrastrutture di rete, sistemi di e-commerce, etc.) ovvero in cui tali servizi costituiscono un valore aggiunto per il cliente (es. soluzioni di e-commerce, gestione di pagamenti on line, etc.).

Le imprese devono anche verificare che il loro stato in tema di ICT *Security Governance & Management* sia tale da aspirare al riconoscimento dell'esimente dalla responsabilità prevista dal decreto 231 in caso di commissione di un delitto informatico al loro interno.

In considerazione di tali elementi, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo sono:

- codice etico;
- sistema sanzionatorio;
- controllo gerarchico;
- misure di protezione dei documenti elettronici (es. firma digitale);
- adozione di procedure di validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche;
- procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro o professionale;
- aggiornamento regolare dei sistemi informativi in uso;
- modalità di accesso ai sistemi informatici aziendali mediante adeguate procedure di autorizzazione, che prevedano, ad esempio, la concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze derivanti dalle mansioni aziendali che competono al ruolo ricoperto dal soggetto;
- procedura per il controllo degli accessi;
- tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici aziendali;
- inclusione negli accordi con terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni;
- ricorso a misure di protezione di accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse;
- allestimento di misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall'operare al di fuori del perimetro dell'organizzazione;

- definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte di personale all'uopo incaricato;
- controllo sistemi (siti inconferenti);
- formazione;
- procedure di controllo della installazione di software sui sistemi operativi.

Art. 24 ter D.lgs. n. 231/2001 - Delitti di criminalità organizzata

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo provvedimento inserito: Decreto legislativo 8 novembre 2021, n. 195)	Reato presupposto	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo
24-ter	Delitti di criminalità organizzata	Associazione per delinquere (art. 416 c.p.)	800	4	A/B/C/D/E	5	4,5	Medio-Alto
24-ter	Delitti di criminalità organizzata	Associazione di tipo mafioso anche straniere (art. 416-bis c.p.) [articolo modificato dalla L. n. 69/2015]	1000	5	A/B/C/D/E	5	5,0	Alto
24-ter	Delitti di criminalità organizzata	Scambio elettorale politico-mafioso (art. 416-ter c.p.) [così sostituito dall´art. 1, comma 1, L. 17 aprile 2014, n. 62, a decorrere dal 18 aprile 2014, ai sensi di quanto disposto dall´art. 2, comma 1 della medesima L. 62/2014]	1000	5	A/B/C/D/E	5	5,0	Alto
24-ter	Delitti di criminalità organizzata	Tutti i delitti se commessi avvalendosi delle condizioni previste dall´art. 416-bis c.p. per agevolare l´attività delle	1000	5	A/B/C/D/E	5	5,0	Alto

		associazioni previste dallo stesso articolo (L. 203/91)						

Questi delitti sono stati introdotti dalla L. 94/2009 e fanno riferimento all'art. 416 c.p. il quale punisce coloro che promuovono, costituiscono ovvero organizzano l'associazione allo scopo di commettere più delitti. La rilevanza penale delle condotte descritte dalla norma appare condizionata all'effettiva costituzione dell'associazione criminosa.

I reati associativi, essendo questi normalmente legati alla commissione dei reati c.d. fine (es. associazione per delinquere finalizzata alla truffa, alla corruzione, al riciclaggio, ecc.), possono essere connessi ad altre tipologie di reato.

Il reato è integrato anche ove non sia stato ancora posto in essere alcun reato-fine.

Un aspetto controverso è quello riguardo alla possibilità di estendere all'ente, ai fini dell'individuazione del profitto confiscabile, anche reati fine che non siano compresi nel Decreto 231.

In giurisprudenza è stato osservato che se l'ente non potesse essere ritenuto responsabile ex art. 24-ter perché l'associazione posta in essere è finalizzata al compimento di reati extra catalogo (catalogo 231), l'articolo in esame sarebbe totalmente svuotato di qualsiasi capacità punitiva, nell'ipotesi in cui sussista comunque una associazione criminosa.

La configurazione dei reati associativi come reati-mezzo ha l'effetto di estendere la responsabilità dell'ente ex decreto 231 a una serie indefinita di fattispecie criminose commesse in attuazione del *pactum sceleris* e non necessariamente incluse nell'elenco dei reati presupposto.

Si pensi, ad esempio, alla turbata libertà degli incanti (art. 353 c.p.), all'illecita concorrenza con violenza o minaccia (art. 513-bis, c.p.), all'inadempimento di contratti di pubbliche forniture (art. 355 c.p.) e alla frode nelle pubbliche forniture (art. 356 c.p.).

Pertanto, le diverse possibili manifestazioni dei reati presupposto considerati dall'art. 24-ter decreto 231, anche laddove di rilievo transnazionale, rendono necessaria una scrupolosa mappatura dei rischi, con particolare riferimento a quello di verificazione di condotte dirette a favorire o recare vantaggio all'organizzazione criminale, nonché l'individuazione di adeguati controlli preventivi. A quest'ultimo proposito, ad esempio, la prevenzione dei delitti previsti dai

richiamati articoli 355 e 356 c.p. presuppone il rafforzamento dei controlli nelle aree aziendali che si occupano dell'attività di fornitura pubblica di beni e servizi.

Sotto il profilo sanzionatorio, è prevista l'interdizione non inferiore a un anno e quella definitiva dall'esercizio dell'attività se l'ente o una sua unità organizzativa vengono stabilmente utilizzati allo scopo unico o prevalente do consentire o agevolare la commissione dei reati di cui ai commi 1 e 2 (ossia quelli di cui agli artt. 416, sesto comma, 416-bis, 416-ter e 630 del c.p., i delitti commessi avvalendosi delle condizioni previste dal predetto articolo 416-bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo, nonché ai delitti previsti dall'articolo 74 del testo unico di cui al DPR 309/1990, n. 309). La sanzione pecuniaria è compresa tra 400 e 1000 quote.

In considerazione di tali elementi, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo sono:

- adesione a Protocolli di legalità;
- check list di controllo degli operatori economici
- digitalizzazione degli affidamenti
- regolamento per il reclutamento del personale e progressioni
- regolamento nomina commissioni selezione personale e commissioni di gara e relative dichiarazioni rilasciate
- trasparenza
- codice etico
- sistema disciplinare
- whistleblowing

Art. 25 - Peculato, concussione, induzione indebita a dare o promettere utilità e corruzione e abuso d'ufficio

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo	Reato presupposto	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo

	provvedimento inserito: Legge 238/2021)							
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Concussione (art. 317 c.p.) [articolo modificato dalla L. n. 69/2015]	800	4	A/B/C/D/E	5	4,5	Medio-Alto
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Corruzione per l'esercizio della funzione (art. 318 c.p.) [articolo modificato dalla L. n. 190/2012, L. n. 69/2015 e L. n. 3/2019]	200	1	NESSUNA	1	1,0	Basso
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Corruzione per un atto contrario ai doveri di ufficio (art. 319 c.p.) [articolo modificato dalla L. n. 69/2015]	800	4	A/B/C/D/E	5	4,5	Medio-Alto
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Circostanze aggravanti (art. 319-bis c.p.)	800	4	A/B/C/D/E	5	4,5	Medio-Alto
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Corruzione in atti giudiziari (art. 319-ter c.p.) [articolo modificato dalla L. n. 69/2015]	800	4	A/B/C/D/E	5	4,5	Medio-Alto
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Induzione indebita a dare o promettere utilità (art. 319-quater) [articolo aggiunto dalla L. n. 190/2012 e modificato dalla L. n. 69/2015]	800	4	A/B/C/D/E	5	4,5	Medio-Alto
25	Peculato, concussione, induzione indebita a dare o promettere	Corruzione di persona incaricata di un pubblico servizio (art.	800	4	A/B/C/D/E	5	4,5	Medio-Alto

	utilita`, corruzione e abuso d'ufficio	320 c.p.)						
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Pene per il corruttore (art. 321 c.p.)	800	4	A/B/C/D/E	5	4,5	Medio-Alto
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Istigazione alla corruzione (art. 322 c.p.)	600	3	A/B/C/D/E	5	4,0	Medio-Alto
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri (art. 322-bis c.p.) [articolo modificato dalla L. n. 190/2012 e dalla L. n. 3/2019]	800	4	A/B/C/D/E	5	4,5	Medio-Alto
25	Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio	Traffico di influenze illecite (art. 346-bis c.p.) [articolo modificato dalla L. 3/2019]	800	4	A/B/C/D/E	5	4,5	Medio-Alto

Si tratta di tipologie di reato che rientrano nell'ambito dei reati contro la Pubblica Amministrazione e, in quanto tali, presuppongono l'instaurazione di rapporti con soggetti pubblici e/o l'esercizio di una pubblica funzione o di un pubblico servizio.

Nel nostro ordinamento non è raro che la qualità di soggetto pubblico (pubblico ufficiale e incaricato di pubblico servizio) sia estesa anche nei confronti di soggetti privati e, quindi, che tale qualifica sia attribuita ad esponenti di realtà societarie a carattere privato, investite dello svolgimento di pubblici servizi o di pubbliche funzioni, nei limiti e in relazione alle attività aziendali riconducibili all'assolvimento di tali compiti, come anche di seguito specificato. A tale proposito si deve ricordare che, secondo l'attuale disciplina, ciò che rileva è, infatti, l'attività svolta in concreto e non la natura giuridica, pubblica o privata, del soggetto.

Ne consegue che il nostro ordinamento accoglie una nozione di pubblico ufficiale e di incaricato di pubblico servizio di tipo "oggettivo", che comporta la necessità di una valutazione "caso per caso" -peraltro non sempre agevole - delle singole funzioni ed attività svolte, sia per determinare la qualificazione del soggetto interessato (pubblico ufficiale, incaricato di pubblico servizio o semplice privato) sia, di conseguenza, per stabilire la natura delle azioni realizzate dal medesimo.

Da ciò discende che possono coesistere in capo ad un medesimo soggetto, almeno a fini penalistici, qualifiche soggettive diverse.

È possibile dedurre che, limitando per il momento l'analisi ai soli reati di natura corruttiva, in taluni casi possono configurarsi sia corruzioni c.d. attive (es. l'amministratore o il dipendente della singola società corrompe un pubblico ufficiale o un incaricato di pubblico servizio per far ottenere all'ente qualcosa), sia corruzioni cd. passive (es. l'esponente dell'ente - nello svolgimento di un'attività di natura "pubblicistica" - riceve denaro per compiere un atto contrario ai doveri del proprio ufficio). Tale ultima forma d'illecito, nell'ottica del decreto 231, si verificherà con minore frequenza della prima, giacché nella maggior parte dei casi si tratterà di corruzioni realizzate nell'esclusivo interesse della persona fisica senza, cioè, che sia configurabile un interesse o vantaggio dell'ente. Tuttavia, anche in questi casi, non è possibile escludere che si verifichino ipotesi di corruzione passiva che generano responsabilità dell'ente (ad es. laddove quest'ultimo abbia tratto un vantaggio - eventualmente anche indiretto - dalla commissione del reato da parte del proprio esponente) e ciò, verosimilmente, si potrà verificare proprio con riferimento a quei

soggetti, di diritto privato o di diritto pubblico (ad es. i c.d. enti pubblici economici) la cui attività sia, in tutto o in parte, da considerare come pubblica funzione o pubblico servizio.

Le fattispecie di cui all'art. 25 del Decreto 231 sono reati contro la Pubblica Amministrazione e possono essere suddivise in categorie, di differente gravità, l'oggetto giuridico di tali reati è il regolare e imparziale svolgimento delle funzioni pubbliche da parte degli Enti competenti: la responsabilità delle imprese ai sensi del Decreto 231 si colloca in questo contesto di tutela rafforzata della funzione statale.

La nozione di pubblico ufficiale e di persona incaricata di un pubblico servizio è contenuta negli artt. 357 e 358 c.p.. La definizione di persona esercente un servizio di pubblica necessità è, invece, contenuta nell'art. 359 c.p..

La Suprema Corte (Cass. pen., sez. VI, 21 febbraio 2003, n. 11417) è intervenuta sul tema, chiarendo che «al fine di individuare se l'attività svolta da un soggetto possa essere qualificata come pubblica, …ha rilievo esclusivo la natura delle funzioni esercitate, che devono essere inquadrabili tra quelle della P.A.. Non rilevano, invece, la forma giuridica dell'ente e la sua costituzione secondo le norme del diritto pubblico, né lo svolgimento della sua attività in regime di monopolio, né tanto meno il rapporto di lavoro subordinato dell'agente con l'organismo datore di lavoro».

Ne consegue che, ad esempio, nelle società a partecipazione pubblica, per accertare la qualifica di pubblico ufficiale e incaricato di pubblico servizio di amministratori e/o dipendenti, occorre tener conto della natura dell'attività svolta, verificando se l'interesse pubblico si sovrappone e prevale sull'attività imprenditoriale.

La disposizione in oggetto è stata modificata dalla L. 190/2012, che è intervenuta sulla disciplina della concussione e ha introdotto il delitto di induzione indebita.

In relazione a tali reati, possono costituire aree di rischio:

- procedure di gara o di negoziazione diretta nonché la successiva attività di erogazione del servizio e/o della prevista prestazione contrattuale;
- la partecipazione a procedure per l'ottenimento di licenze, provvedimenti amministrativi ed autorizzazioni da parte della P.A.;

- la partecipazione a procedure per l'ottenimento di erogazioni, contributi o finanziamenti da parte di organismi pubblici italiani o comunitari e il loro concreto utilizzo;
- assunzione di personale e progressioni.

La L. 3/2019 (cd «spazzacorrotti») ha introdotto misure per il contrasto dei reati contro la pubblica amministrazione ed è intervenuta, con l'art. 7, anche sulla disciplina della responsabilità da reato degli Enti. In particolare, la nuova normativa inserisce nell'elenco dei reati presupposto quello di traffico di influenze illecite, previsto dall'art. 346 bis c.p.: tale disposizione, oggi include anche le condotte di millantato credito (reato abrogato), che consistono nella intermediazione illecita tra il privato e il pubblico funzionario, finalizzate alla corruzione di quest'ultimo, senza distinguere a seconda che le relazioni col pubblico funzionario vantate dall'intermediario siano realmente esistenti o anche solo «asserite».

La legge del 2019 aggrava la disciplina delle sanzioni interdittive previste per l'ente, attraverso l'aumento della durata della sanzione. Si prevede, peraltro, l'applicazione di sanzioni interdittive di durata inferiore a quella stabilita dall'art. 25, comma 5 «se prima della sentenza di primo grado l'ente si è efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità trasferite e ha eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di Modelli organizzativi idonei a prevenire reati della specie di quello verificatosi».

Sui reati in oggetto si segnala l'intervento di ANAC con la delibera n. 1134 dell'8/11/2017 di approvazione delle «Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli Enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli Enti pubblici economici». Il documento muove dalle disposizioni normative vigenti, tra cui il D.lgs. 97/2016 in materia di trasparenza e lotta alla corruzione. Tale Decreto introduce l'art. 2 bis nel D.lgs. 33/2013, precisa che le norme sulla trasparenza si applicano a tutte le pubbliche amministrazioni quali definite dall'art. 1, comma 2, D.lgs. 165/2001 e ne amplia i destinatari comprendendovi anche Enti di diritto privato.

Il Decreto 97/2016 introduce il comma 2 bis nell'art. 1 della L. 190/2012 e dispone che il Piano Nazionale Anticorruzione (PNA) costituisce atto di indirizzo per le P.A. di cui all'art. 1, comma 2,

D.lgs. 165/2001, ai fini dell'adozione dei propri piani triennali di prevenzione della corruzione, e per gli altri soggetti di cui all'art. 2 bis comma 2 D.lgs. 33/2013, ai fini dell'adozione di misure di prevenzione della corruzione integrative di quelle adottate ai sensi del D.lgs. 231/2001.

Di fatto, l'art. 2 bis del Decreto 33 assoggetta agli obblighi di trasparenza previsti per le P.A. le società in controllo pubblico e le associazioni, fondazioni e gli altri Enti di diritto privato quando ricorrano le condizioni previste dalla norma. Tali Enti sono tenuti anche ad ottemperare alle norme per la prevenzione della corruzione ma, per loro, il PNA costituisce un atto di indirizzo ai fini dell'adozione di misure di prevenzione della corruzione integrative di quelle adottate ai sensi del Decreto 231 (art. 1, comma 2 bis, l. 190).

L'ANAC rileva che a tale integrazione si doveva provvedere entro il 31/12/2018.

Il D.Lgs. 75/2020 (in vigore dal 30 luglio 2020) ha affiancato alle ipotesi già previste dall'art. 25 del Decreto 231: - I reati di peculato di cui all'art. 314 c.p., primo comma (rimanendo dunque escluso il peculato d'uso) e all'art. 316 (ossia la particolare forma di peculato mediante profitto dell'errore altrui); - Il reato di abuso d'ufficio di cui all'art. 323 c.p.

Per quanto sopra esposto, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo sono:

- adesione a Protocolli di legalità
- check list di controllo degli operatori economici
- digitalizzazione degli affidamenti
- regolamento per il reclutamento del personale e progressioni
- regolamento nomina commissioni selezione personale e commissioni di gara e relative dichiarazioni rilasciate
- regolamento per il conferimento incarichi professionali
- trasparenza
- formazione
- codice etico
- sistema disciplinare
- whistleblowing

- segregazione

Articolo 25 bis 1 - Delitti contro l'industria e il commercio

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo provvedimento inserito: Legge 238/2021)	Reato presupposto	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo
25-bis.1	Delitti contro l'industria e il commercio	Turbata libertà dell'industria o del commercio (art. 513 c.p.)	500	3	NESSUNA	1	2,0	Medio-basso

Le fattispecie in parola sono state inserite nel catalogo dei reati presupposto dalla L. 99/2009, al fine di sanzionare le politiche aziendali finalizzate ad alterare la concorrenza, danneggiando i consumatori.

Il reato di cui all'art. 513 c.p. punisce «chiunque adopera violenza sulle cose ovvero mezzi fraudolenti per impedire o turbare l'esercizio di un'industria o di un commercio».

La giurisprudenza di settore ha precisato che «l'art. 513 bis c.p. punisce soltanto quelle condotte tipicamente concorrenziali (quali il boicottaggio, lo storno dei dipendenti, il rifiuto di contrattare, etc.) attuate, però, con atti di coartazione che inibiscono la normale dinamica imprenditoriale, non rientrando, invece, nella fattispecie astratta, gli atti intimidatori che siano finalizzati a contrastare o ostacolare l'altrui libera concorrenza»: «la condotta di chi altera la concorrenza ricorrendo a mezzi fraudolenti», infatti, «integra il delitto di cui all'art. 513 c.p. soltanto se si ripercuote sull'ordine economico, ossia quando è posta in essere al fine specifico di turbare o impedire il normale svolgimento dell'industria o del commercio e di attentare in tal modo alla libertà di iniziativa economica». Si tratta, in ogni caso, di un reato di pericolo: non è dunque necessario che la condotta abbia in concreto alterato la normale dinamica dei rapporti commerciali.

In considerazione di tali elementi, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo:

- adesione a Protocolli di legalità
- check list di controllo degli operatori economici
- digitalizzazione degli affidamenti
- regolamento nomina commissioni di gara e relative dichiarazioni rilasciate
- regolamento per il conferimento incarichi professionali
- trasparenza
- formazione
- codice etico
- sistema disciplinare
- whistleblowing
- segregazione

Art. 25 ter - Reati societari

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo provvedimento inserito: Legge 238/2021)	Reato presupposto	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo
25-ter	Reati societari	False comunicazioni sociali (art. 2621 c.c.) [articolo modificato dalla L. n. 69/2015]	400	2	NESSUNA	1	1,5	Basso
25-ter	Reati societari	Fatti di lieve entità (art. 2621-bis c.c.)	200	1	NESSUNA	1	1,0	Basso
25-ter	Reati societari	Impedito controllo (art. 2625, comma 2, c.c.)	360	2	NESSUNA	1	1,5	Basso
25-ter	Reati societari	Indebita restituzione di conferimenti (art. 2626 c.c.)	360	2	NESSUNA	1	1,5	Basso
25-ter	Reati societari	Illegale ripartizione degli utili e delle riserve (art. 2627 c.c.)	260	2	NESSUNA	1	1,5	Basso

25-ter	Reati societari	Operazioni in pregiudizio dei creditori (art. 2629 c.c.)	660	4	NESSUNA	1	2,5	Medio-Basso
25-ter	Reati societari	Formazione fittizia del capitale (art. 2632 c.c.)	360	2	NESSUNA	1	1,5	Basso
25-ter	Reati societari	Indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.)	660	4	NESSUNA	1	2,5	Medio-basso
25-ter	Reati societari	Corruzione tra privati (art. 2635 c.c.) [aggiunto dalla L. n. 190/2012; modificato dal D.Lgs. n. 38/2017 e dalla L. n. 3/2019]	600	3	A/B/C/D/E	5	4,0	Medio-Alto
25-ter	Reati societari	Istigazione alla corruzione tra privati (art. 2635-bis c.c.) [aggiunto dal D.Lgs. n. 38/2017 e modificato dalla L. n. 3/2019]	400	2	A/B/C/D/E	5	3,5	Medio-Alto
25-ter	Reati societari	Illecita influenza sull'assemblea (art. 2636 c.c.)	660	4	NESSUNA	1	2,5	Medio-basso
25-ter	Reati societari	Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638, comma 1 e 2, c.c.)	800	4	NESSUNA	1	2,5	Medio-basso

L'art. 25 ter del Decreto 231 è stato introdotto dal D.lgs. 61/2002 e successivamente modificato dalla L. 262/2005, dalla L. 190/2012 e dalla L. 69/2015.

Esso prevede la responsabilità dell'Ente in relazione alla commissione dei reati previsti nel codice civile, a chiusura della disciplina delle società.

Il reato di false comunicazioni sociali è stato di recente modificato dalla L. 69/2015, che ha ripristinato il regime sanzionatorio introdotto con la riforma del 2002, mantenendo invece la

previsione di due fattispecie: 1. le false comunicazioni sociali di cui all'art. 2621 c.c., commesse nell'ambito di società non quotate in borsa; 2. le false comunicazioni sociali delle società quotate, di cui all'art. 2622 c.c.

In ordine al contenuto delle false comunicazioni, si richiama la precisazione effettuata dalle Sezioni Unite della Cassazione, secondo cui «il reato di false comunicazioni sociali, previsto dall'art. 2621 cod. civ., nel testo modificato dalla L. 69/2015, è configurabile in relazione alla esposizione in bilancio di enunciati valutativi, se l'agente, in presenza di criteri di valutazione normativamente fissati o di criteri tecnici generalmente accettati, se ne discosti consapevolmente e senza fornire adeguata informazione giustificativa, in modo concretamente idoneo ad indurre in errore i destinatari delle comunicazioni»

Sotto il profilo sanzionatorio, le riforme hanno determinato un inasprimento delle pene. Non sono, tuttavia, previste sanzioni interdittive, il Decreto ha previsto la sanzione pecuniaria da 400 a 600 quote per i reati di cui all'art. 2635 bis comma 1 c.c. e quella da 200 a 400 quote per i fatti di istigazione alla corruzione passiva di cui all'art. 2635 bis comma 1 c.c., mentre per entrambe le fattispecie ha previsto l'applicazione di misure interdittive.

In considerazione di tali elementi, le principali aree di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo:

- formazione
- codice etico
- sistema disciplinare
- tempestiva segnalazione di eventuali conflitti di interesse
- segregazione
- presenza degli organi di controllo

Art. 25-septies d.lgs. 231/2001 – Omicidio colposo o lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15	Reato presupposto	SI/NO	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo

	dicembre 2021 (ultimo provvedimento inserito: Legge 238/2021)								
25-septies	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	Omicidio colposo (art. 589 c.p.)		1000	5	A/B/C/D/E	5	5	Alto
25-septies	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	Omicidio colposo (art. 589 c.p.)		500	3	A/B/C/D/E	5	4	Medio-alto
25-septies	Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro	Lesioni personali colpose (art. 590 c.p.)		250	2	A/B/C/D/E	5	4	Medio-alto

La legge 123/2007 ha per la prima volta previsto la responsabilità dell'ente in dipendenza di un reato colposo. Tale circostanza impone un coordinamento con l'art. 5 del decreto 231, che definisce il criterio oggettivo di imputazione della responsabilità dell'ente, subordinandola all'esistenza di un interesse o vantaggio per l'ente, nonché con l'esimente di cui all'art. 6, nella parte in cui richiede la prova della elusione fraudolenta del modello organizzativo, sicuramente incompatibile con una condotta colposa. A tal proposito, l'*impasse* si potrebbe superare facendo ricorso ad una interpretazione che, tenendo conto del diritto di difesa e del principio di uguaglianza, permetta di prescindere da tale prova o quantomeno di disancorare il concetto di "elusione fraudolenta" dalle tipiche fattispecie proprie del codice penale e di assumerlo in termini di intenzionalità della sola condotta dell'autore (e non anche dell'evento) in violazione delle procedure e delle disposizioni interne predisposte e puntualmente implementate dall'azienda per

prevenire la commissione degli illeciti di cui si tratta o anche soltanto di condotte a tali effetti "pericolose".

Questa interpretazione si fonda sui seguenti presupposti. Le condotte penalmente rilevanti consistono nel fatto, da chiunque commesso, di cagionare la morte o lesioni gravi/gravissime al lavoratore, per effetto dell'inosservanza di norme antinfortunistiche.

In linea teorica, soggetto attivo dei reati può essere chiunque sia tenuto ad osservare o far osservare le norme di prevenzione e protezione. Tale soggetto può quindi individuarsi, ai sensi del decreto 81/2008, nei datori di lavoro, nei dirigenti, nei preposti, nei soggetti destinatari di deleghe di funzioni attinenti alla materia della salute e sicurezza sul lavoro, nonché nei medesimi lavoratori.

I delitti contemplati dagli artt. 589 e 590 c.p. sono caratterizzati dall'aggravante della negligente inosservanza delle norme antinfortunistiche. L'elemento soggettivo, dunque, consiste nella cd. colpa specifica, ossia nella volontaria inosservanza di norme precauzionali volte a impedire gli eventi dannosi previsti dalla norma incriminatrice.

L'individuazione degli obblighi di protezione dei lavoratori è tutt'altro che agevole, infatti oltre decreto 81/2008 e agli altri specifici atti normativi in materia, la giurisprudenza della Cassazione ha precisato che tra le norme antinfortunistiche di cui agli artt. 589, comma 2, e 590, comma 3, c.p., rientra anche l'art. 2087 c.c., che impone al datore di lavoro di adottare tutte quelle misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica dei lavoratori.

Prediligendo un approccio interpretativo sistematico che valuti il rapporto di interazione tra norma generale (art. 2087 c.c.) e singole specifiche norme di legislazione antinfortunistica previste dal decreto 81 del 2008, appare coerente concludere che:

• l'art. 2087 c.c. introduce l'obbligo generale contrattuale per il datore di lavoro di garantire la massima sicurezza tecnica, organizzativa e procedurale possibile;

• conseguentemente, l'elemento essenziale ed unificante delle varie e possibili forme di responsabilità del datore di lavoro, anche ai fini dell'applicabilità dell'art. 25-septies del decreto 231 del 2001, è rappresentato dalla mancata adozione di tutte le misure di sicurezza e prevenzione tecnicamente possibili e concretamente attuabili (come specificato dall'art. 3, comma

1, lett. b), del decreto 81/2008), alla luce dell'esperienza e delle più avanzate conoscenze tecnico-scientifiche. Secondo la sentenza della Corte Costituzionale n. 312 del 18 luglio 1996 l'obbligo generale di massima sicurezza possibile deve fare riferimento alle misure che nei diversi settori e nelle diverse lavorazioni, corrispondono ad applicazioni tecnologiche generalmente praticate e ad accorgimenti generalmente acquisiti, sicché penalmente censurata è la deviazione del datore di lavoro dagli standard di sicurezza propri, in concreto ed al momento, delle singole diverse attività produttive. Il novero degli obblighi in materia antinfortunistica si accresce ulteriormente ove si consideri che secondo la migliore dottrina e la più recente giurisprudenza l'obbligo di sicurezza in capo al datore di lavoro non può intendersi in maniera esclusivamente statica quale obbligo di adottare le misure di prevenzione e sicurezza nei termini sopra esposti (forme di protezione oggettiva), ma deve al contrario intendersi anche in maniera dinamica implicando l'obbligo di informare e formare i lavoratori sui rischi propri dell'attività lavorativa e sulle misure idonee per evitare i rischi o ridurli al minimo (forme di protezione soggettiva).

In considerazione di tali elementi, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo sono:

- formazione;
- codice etico;
- sistema disciplinare;
- whistleblowing;
- organigramma sicurezza.

Art. 25 octies - Ricettazione, riciclaggio e impiego di denaro e autoriciclaggio

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo provvedimento inserito: Legge 238/2021)	Reato presupposto	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo
25-octies	Ricettazione, riciclaggio e	Ricettazione (art. 648 c.p.)	1000	5	A/B/C/D/E	5	5	Alto

	impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	[articolo modificato dal D.Lgs. 195/2021]						
25octies	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	Riciclaggio (art. 648-bis c.p.) [articolo modificato dal D.Lgs. 195/2021]	1000	5	A/B/C/D/E	5	5	Alto
25octies	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	Impiego di denaro, beni o utilità di provenienza illecita (art. 648-ter c.p.) [articolo modificato dal D.Lgs. 195/2021]	1000	5	A/B/C/D/E	5	5	Alto
25octies	Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio	Autoriciclaggio (art. 648-ter.1 c.p.) [articolo modificato dal D.Lgs. 195/2021]	1000	5	A/B/C/D/E	5	5	Alto

Nel nostro ordinamento è presente una disciplina, di derivazione Europea, con la quale sono previsti una serie di adempimenti antiriciclaggio allo scopo di proteggere la stabilità e l'integrità del sistema economico e finanziario.

L'azione di prevenzione e contrasto del riciclaggio di denaro, beni o altre utilità, diretta tradizionalmente alle banche ed agli intermediari finanziari, è stata progressivamente estesa ad altri soggetti che svolgono attività ritenute particolarmente esposte al rischio di riciclaggio. In tale contesto, il richiamo dei presidi antiriciclaggio, ivi compresi i limiti all'utilizzo del contante, è utile anche per i non destinatari del D.lgs. 231/2007 nell'ottica dell'individuazione delle aree di attività a rischio, della prevenzione dei reati di riciclaggio e autoriciclaggio e, quindi, dell'esclusione della responsabilità ex D.lgs. 231/01.

Il riciclaggio di beni e capitali illeciti genera gravi distorsioni nell'economia legale, alterando le condizioni di concorrenza, il corretto funzionamento dei mercati e i meccanismi fisiologici di allocazione delle risorse con riflessi in definitiva sulla stessa stabilità ed efficienza del sistema economico. L'azione di prevenzione e contrasto del riciclaggio si esplica, quindi, attraverso

l'introduzione di presidi volti a garantire la piena conoscenza del cliente, la tracciabilità delle transazioni finanziarie e l'individuazione delle operazioni sospette.

Il D.lgs. n. 231/2007, in questi termini, non ha solo creato nuove fattispecie penali, ma ha inteso dare corpo a specifiche metodologie di approccio alla valutazione del rischio di riciclaggio nelle attività economiche e finanziarie, estendendo la rete delle misure amministrative per rafforzare la collaborazione nell'attività di contrasto al riciclaggio, passando dai vincoli sull'identificazione della clientela alla segnalazione delle operazioni sospette.

Queste attività di prevenzione spettano oggi, anche grazie alle importanti integrazioni del D.lgs. 90/2017 e del D.lgs. 125/2019 ad una moltitudine di soggetti tra i quali si richiamano:

1. intermediari bancari e finanziari quali banche; poste italiane S.p.a.; istituti di moneta elettronica; SIM; SGR; (SICAV); agenti di cambio ecc.;
2. altri operatori finanziari quali società fiduciarie, mediatori creditizi, ecc.;
3. professionisti quali ragionieri, commercialisti, notai, avvocati ecc.;
4. altri operatori non finanziari quali i c.d. compro oro (i cui obblighi sono stabiliti dal D.lgs. 92/2017);
5. gli agenti in affari che svolgono attività in mediazione immobiliare, anche quando agiscono in qualità di intermediari nella locazione di un bene immobile e, in tal caso, limitatamente alle sole operazioni per le quali il canone mensile è pari o superiore a 10.000 euro;
6. prestatori di servizi di gioco;
7. altri soggetti quali pubbliche amministrazioni, società in controllo pubblico (a cui si applica il regime di cui all'art. 10 del D.lgs. 231/2007);
8. le succursali "insediate" degli intermediari assicurativi (ossia le succursali insediate in Italia di agenti e *broker* aventi sede legale e amministrazione centrale in un altro Stato membro o in uno Stato terzo);
9. i soggetti che esercitano il commercio di opere d'arte o che agiscono in qualità di intermediari nel commercio delle medesime opere, anche quando tale attività è effettuata da gallerie d'arte o case d'asta o all'interno di porti franchi qualora il valore dell'operazione, anche se frazionata o di operazioni collegate sia pari o superiore a 10.000 euro;

10. i prestatori di servizi di portafoglio digitale, quali persone fisiche o giuridiche che forniscono, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali.

In questo campo, specifico interesse ricopre l'area della gestione finanziaria, dove il controllo procedurale si deve avvalere di strumenti consolidati nella pratica amministrativa, quali per esempio abbinamento di firme, supervisione, separazione di compiti con la contrapposizione di funzioni (ad esempio fra la funzione acquisti-gare e appalti e quella finanziaria).

L'articolo 49 del D.lgs. 231/2007 prevede il divieto di trasferire denaro contante o titoli al portatore tra soggetti diversi, siano essi persone fisiche o giuridiche, per somme maggiori o uguali a 3.000 €. L'art. 18 della legge 19 dicembre 2019, n. 157 è intervenuto da ultimo sull'utilizzo del contante stabilendo che dal 1° luglio 2020 e fino al 31 dicembre 2021 il limite è ridotto da 3.000 € a 2.000 €. Dal 1° gennaio 2022 tale limite è di 1.000 €.

L'analisi sull'utilizzo del contante nel nostro Paese rileva che l'86 per cento delle transazioni viene effettuato in contanti (68 per cento del valore complessivo. Fonte: Banca d'Italia). L'art. 7-quater del D.L. n. 193 del 2016, modificando il testo unico sull'accertamento delle imposte (DPR n. 600 del 1973, articolo 32), ha previsto, con riferimento ai titolari di reddito di impresa (i quali percepiscono "ricavi": articoli 57 e 85 del TUIR), un parametro quantitativo oltre il quale scatta la presunzione di evasione per i prelevamenti o importi riscossi di valore superiore a 1.000 e giornalieri e a 5.000 € mensili. Da tale presunzione sono esclusi i compensi dei professionisti.

Entrando nel dettaglio delle singole fattispecie, il D.lgs. 231/2007, con l'introduzione dell'art. 25 octies, ha inserito tra i reati presupposto alcune fattispecie di illeciti contro il patrimonio. Successivamente l'articolo è stato modificato dalla L. 186/2014, cui si deve l'introduzione del reato di autoriciclaggio (art. 648 ter 1 c.p.). L'art. 25 octies del Decreto 231 prevede dunque che «in relazione ai reati di cui agli articoli 648, 648-bis, 648-ter e 648-ter.1 del codice penale, si applica all'ente la sanzione pecuniaria da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote». Sotto il profilo sanzionatorio, è prevista l'applicabilità delle sanzioni interdittive, per una durata non superiore a due anni.

Il reato in questione può essere realizzato in molte aree aziendali, alcune funzioni/aree/processi sono maggiormente esposti al rischio: tra questi, il settore acquisti-gare e appalti, l'erogazione di contributi, il rilascio di autorizzazioni.

Il Dlgs 8 novembre 2021 n. 195 pubblicato in G.U. il 30.11.2021 ha ampliato il novero dei reati presupposto dei delitti di ricettazione, riciclaggio, autoriciclaggio e impiego di beni o utilità di provenienza illecita (articolo 25- octies del Dlgs 231/2001) che comprende quindi anche le contravvenzioni (punite con l'arresto superiore nel massimo a un anno o nel minimo a sei mesi) e, nel caso del riciclaggio e dell'autoriciclaggio, anche i delitti colposi.

In precedenza, perché ricorressero questi reati occorreva che il denaro o i beni da "ripulire" fossero il frutto di delitti non colposi, ora, invece, possono provenire anche da contravvenzioni e da reati colposi.

Quanto alle contravvenzioni, potrebbero far scattare i reati di riciclaggio e ricettazione le violazioni delle norme sulla sicurezza sul lavoro o ambientali. Sarebbe il caso, ad esempio, dell'impiego in attività di impresa di risorse sottratte agli investimenti su sicurezza e ambiente. Quanto ai delitti colposi, potrebbero divenire reati presupposto di riciclaggio fattispecie come infortuni sul lavoro, inquinamento, disastri ambientali, da cui possono discendere proventi economici.

In considerazione di tali elementi, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo:

- adesione a Protocolli di legalità
- check list di controllo per affidamenti
- check list di controllo contributi
- check list di controllo autorizzazioni
- digitalizzazione degli affidamenti
- regolamento per il reclutamento del personale e progressioni
- regolamento nomina commissioni selezione personale e commissioni di gara e relative dichiarazioni rilasciate
- regolamento per il conferimento incarichi professionali
- trasparenza

- formazione
- codice etico
- sistema disciplinare
- whistleblowing
- segregazione

Art. 25 novies - Delitti in materia di violazione del diritto d'autore

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo provvedimento inserito: Legge 238/2021)	Reato presupposto	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo
25-novies	Delitti in materia di violazione del diritto d'autore	Messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, L. n.633/1941 comma 1 lett. a) bis)	500	3	A/B/C/D/E	5	4	Medio-alto
25-novies	Delitti in materia di violazione del diritto d'autore	Reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, L. n.633/1941 comma 3)	500	3	A/B/C/D/E	5	4	Medio-alto
25-novies	Delitti in materia di violazione del diritto d'autore	Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE;	500	3	A/B/C/D/E	5	4	Medio-alto

		predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171-bis L. n.633/1941 comma 1)						
25-novies	Delitti in materia di violazione del diritto d'autore	Riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche di dati (art. 171-bis L. n.633/1941 comma 2)	500	3	A/B/C/D/E	5	4	Medio-alto
25-novies	Delitti in materia di violazione del diritto d'autore	Abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o	500	3	A/B/C/D/E	5	4	Medio-alto

		composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva, vendita o commercio, cessione a qualsiasi titolo o importazione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171-ter L. n.633/1941)						
25-novies	Delitti in materia di violazione del diritto d'autore	Mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171-septies L. n.633/1941)	500	3	A/B/C/D/E	5	4	Medio-alto
25-novies	Delitti in materia di violazione del diritto d'autore	Fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171-octies L. n.633/1941)	500	3	A/B/C/D/E	5	4	Medio-alto

I reati presupposto inseriti nell'art. 25-novies non sono fattispecie di reato di esclusivo interesse delle imprese operanti nello specifico settore software/audiovisivo, ma, al contrario, alcune fattispecie di reato impongono, alla quasi totalità dei soggetti collettivi portatori di interesse economico che intendono contenere i rischi, l'esigenza di porre in essere specifiche misure e protocolli.

Nel caso in cui gli illeciti contro la proprietà intellettuale si realizzino con l'impiego di sistemi informatici aziendali, possono rivelarsi utili anche le misure auspicabili per la prevenzione dei reati informatici richiamati dagli artt. 24 e 24-bis, quali ad esempio lo sviluppo, la gestione e il monitoraggio delle infrastrutture informatiche o la presenza del cd. supervisore informatico.

La disposizione include le fattispecie che possono essere classificate come segue:

1. reati contro l'industria del software: sanzionano condotte di utilizzo abusivo di programmi per elaboratore. In particolare, l'art. 171 bis, comma 1, L. 633/1941 prevede due distinte fattispecie di reato: da un lato, la abusiva duplicazione, per trarne profitto, di programmi per elaboratore (prima ipotesi di reato) e, dall'altro lato, l'importazione, distribuzione, vendita, detenzione a scopo commerciale e imprenditoriale, concessione in locazione non già di programmi abusivamente duplicati, ma esclusivamente di programmi contenuti in supporti non contrassegnati dalla Siae.

Il reato può dunque interessare qualsiasi area dell'attività di impresa.

Sul punto, la giurisprudenza ha osservato che «la detenzione ed utilizzazione di programmi software (nella specie Windows, e programmi di grafica, Autocad) nel campo commerciale o industriale (nella specie, esercente attività di progettazione meccanica ed elettronica nel settore auto motive) integra il reato in oggetto, con la possibilità del sequestro per l'accertamento della duplicazione». Esulano, invece, dal campo di applicazione della norma, le violazioni contrattuali delle licenze che non comportino riproduzione, distribuzione, importazione, vendita e detenzione del software.

2. reati contro l'industria audiovisiva e l'editoria: si tratta di fattispecie che sanzionano l'uso abusivo di opere audiovisive o letterarie che interessano, soprattutto, imprese attive nel campo della comunicazione.

3. reati trasversali, tra cui l'immissione abusiva di qualsiasi opera di ingegno protetta dal diritto di autore o di una sua parte, in un sistema di rete telematica (anche social network). In questo caso, non è richiesto il fine di lucro (ossia un guadagno economicamente apprezzabile o un incremento patrimoniale) o di profitto (che può essere integrato anche da un risparmio di spesa).

Sotto il profilo sanzionatorio, il Decreto 231 prevede la sanzione pecuniaria sino a 500 quote e le sanzioni interdittive fino a un anno.

In considerazione di tali elementi, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo sono:

- codice etico;
- sistema sanzionatorio;
- controllo gerarchico;
- misure di protezione dei documenti elettronici (es. firma digitale)
- adozione di procedure di validazione delle credenziali di sufficiente complessità e previsione di modifiche periodiche;
- procedure che prevedano la rimozione dei diritti di accesso al termine del rapporto di lavoro o professionale;
- aggiornamento regolare dei sistemi informativi in uso;
- modalità di accesso ai sistemi informatici aziendali mediante adeguate procedure di autorizzazione, che prevedano, ad esempio, la concessione dei diritti di accesso ad un soggetto soltanto a seguito della verifica dell'esistenza di effettive esigenze derivanti dalle mansioni aziendali che competono al ruolo ricoperto dal soggetto;
- procedura per il controllo degli accessi;
- tracciabilità degli accessi e delle attività critiche svolte tramite i sistemi informatici aziendali;
- inclusione negli accordi con terze parti e nei contratti di lavoro di clausole di non divulgazione delle informazioni;
- ricorso a misure di protezione di accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse;
- allestimento di misure di sicurezza per apparecchiature fuori sede, che prendano in considerazione i rischi derivanti dall'operare al di fuori del perimetro dell'organizzazione;
- definizione e regolamentazione delle attività di gestione e manutenzione dei sistemi da parte di personale all'uopo incaricato;
- formazione;
- controllo sistemi (siti inconferenti);

- procedure di controllo della installazione di software sui sistemi operativi.

Art. 25 decies - Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria

Art. 25-decies Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (aggiunto dalla L. n. 116/2009)									
25-decies	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-bis c.p.)	SI	500	3	nessuna	1	2	Medio-basso

Il D.lgs. 121/2011 ha introdotto nel Decreto 231 il delitto di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'A.G. da parte di un soggetto titolare della facoltà di non rispondere (art. 377 bis c.p.).

Si tratta di un reato che non può essere commesso, qualora non si configuri un reato più grave, da chi rivesta la qualifica di testimone in un giudizio ma solo da imputato, coimputato o imputato di reato connesso che rendano dichiarazioni su fatti altrui. La Suprema Corte ha precisato che «l'art. 377 c.p. tutela la serena acquisizione di dichiarazioni di soggetti su cui grava l'obbligo di rispondere, salva la previsione in loro favore di speciali prerogative cui hanno però la facoltà di rinunziare (caso tipico è quello della deposizione dei prossimi congiunti dell'imputato di cui all'art. 199 c.p.p.), mentre l'art. 377-bis c.p. tutela le analoghe situazioni concernenti soggetti nei cui confronti non grava l'obbligo di rispondere, ma che sono comunque in grado di rendere dichiarazioni utilizzabili nel procedimento».

In considerazione di tali elementi, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo:

- adesione a Protocolli di legalità;
- check list di controllo degli operatori economici
- digitalizzazione degli affidamenti
- regolamento per il reclutamento del personale e progressioni

- regolamento nomina commissioni selezione personale e commissioni di gara e relative dichiarazioni rilasciate
- trasparenza
- codice etico
- sistema disciplinare
- whistleblowing

Art. 25 undecies – Reati ambientali

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo provvedimento inserito: Legge 238/2021)	Reato presupposto	SI/NO	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo
25-undecies	Reati ambientali	Inquinamento ambientale (art. 452-bis c.p.)		600	3	A/B/C/D/E	5	4	Medio-alto
25-undecies	Reati ambientali	Disastro ambientale (art. 452-quater c.p.)		800	4	A/B/C/D/E	5	5	Alto
25-undecies	Reati ambientali	Delitti colposi contro l'ambiente (art. 452-quinquies c.p.)		500	3	nessuna	1	2	Medio-basso
25-undecies	Reati ambientali	Traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.)		600	3	nessuna	1	2	Medio-basso
25-undecies	Reati ambientali	Circostanze aggravanti (art. 452-octies c.p.)		1000	5	nessuna	1	3	Medio
25-undecies	Reati ambientali	Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette (art. 727-bis c.p.)		250	2	nessuna	1	2	Medio-basso
25-undecies	Reati ambientali	Distruzione o deterioramento di habitat all´interno di		250	2	nessuna	1	2	Medio-basso

		un sito protetto (art. 733-bis c.p.)							
25-undecies	Reati ambientali	Importazione, esportazione, detenzione, utilizzo per scopo di lucro, acquisto, vendita, esposizione o detenzione per la vendita o per fini commerciali di specie protette (L. n.150/1992, art. 1, art. 2, art. 3-bis e art. 6)		250	2	nessuna	1	2	Medio-basso
25-undecies	Reati ambientali	Scarichi di acque reflue industriali contenenti sostanze pericolose; scarichi sul suolo, nel sottosuolo e nelle acque sotterranee; scarico nelle acque del mare da parte di navi od aeromobili (D.Lgs n.152/2006, art. 137)		250	2	A/B/C/D/E	5	4	Medio-alto
25-undecies	Reati ambientali	Attività di gestione di rifiuti non autorizzata (D.Lgs n.152/2006, art. 256)		300	2	A/B/C/D/E	5	4	Medio-alto
25-undecies	Reati ambientali	Inquinamento del suolo, del sottosuolo, delle acque superficiali o delle acque sotterranee (D.Lgs n. 152/2006, art. 257)		250	2	nessuna	1	2	Medio-basso
25-undecies	Reati ambientali	Traffico illecito di rifiuti (D.Lgs n.152/2006, art. 259)		250	2	nessuna	1	2	Medio-basso
25-undecies	Reati ambientali	Violazione degli obblighi di comunicazione, di tenuta dei		250	2	nessuna	1	2	Medio-basso

		registri obbligatori e dei formulari (D.Lgs n.152/2006, art. 258)							
25-undecies	Reati ambientali	Attività organizzate per il traffico illecito di rifiuti (art. 452-quaterdecies c.p.) [introdotto dal D.Lgs. n. 21/2018]		800	4	A/B/C/D/E	5	5	Alto
25-undecies	Reati ambientali	False indicazioni sulla natura, sulla composizione e sulle caratteristiche chimico-fisiche dei rifiuti nella predisposizione di un certificato di analisi di rifiuti; inserimento nel SISTRI di un certificato di analisi dei rifiuti falso; omissione o fraudolenta alterazione della copia cartacea della scheda SISTRI - area movimentazione nel trasporto di rifiuti (D.Lgs n.152/2006, art. 260-bis)		300	2	nessuna	1	2	Medio-basso
25-undecies	Reati ambientali	Sanzioni (D.Lgs. n. 152/2006, art. 279)		250	2	nessuna	1	2	
25-undecies	Reati ambientali	Inquinamento doloso provocato da navi (D.Lgs. n.202/2007, art. 8)		300	2	A/B/C/D/E	5	4	Medio-alto
25-undecies	Reati ambientali	Inquinamento colposo provocato da navi (D.Lgs. n.202/2007, art. 9)		250	2	nessuna	1	2	Medio-basso

25-undecies	Reati ambientali	Cessazione e riduzione dell´impiego delle sostanze lesive (L. n. 549/1993 art. 3)		250	2	nessuna	1	2	Medio-basso

La responsabilità dell'ente è stata estesa ai reati ambientali dal d.lgs. 121/2011, emanato in attuazione della direttiva 2008/99/CE.

L'Unione Europea ha mostrato preoccupazione per la diffusione degli illeciti in materia ambientale, imponendo agli Stati membri di perseguire penalmente condotte che "provochino o possano provocare" pregiudizi all'ambiente e siano tenute "intenzionalmente o per grave negligenza".

Per le sole "gravi violazioni" della disciplina europea in materia ambientale, i legislatori nazionali sono stati vincolati a introdurre sanzioni efficaci, proporzionate e dissuasive sia per la persona fisica che per l'ente.

I punti cardine della disciplina europea sulla tutela penale dell'ambiente sono essenzialmente tre:

- l'incriminazione di gravi violazioni, dannose o almeno concretamente pericolose per l'ambiente;
- la commissione dei reati con dolo o grave negligenza;
- la previsione di sanzioni caratterizzate da efficacia, proporzionalità e dissuasività.

La disciplina legislativa italiana rispecchia in parte l'impulso proveniente dall'Unione Europea

La legge n. 68 entrata in vigore dal 29 maggio 2015 costituisce il più rilevante intervento di riforma della normativa di prevenzione e contrasto della criminalità ambientale. In particolare, la Legge (art. 1, co. 1) introduce per la prima volta nel Libro II del Codice penale, il "Titolo VI-bis – Dei delitti contro l'ambiente" (artt. 452-bis – 452-terdecies), che prevede i seguenti sei nuovi reati contro l'ambiente: il delitto di inquinamento ambientale; il delitto di morte o lesioni come conseguenza del delitto di inquinamento ambientale; il delitto di disastro ambientale; il delitto di traffico e abbandono di materiale ad alta radioattività; il delitto di impedimento del controllo; il delitto di omessa bonifica. Inoltre, viene introdotto nel d. lgs. n. 152/2006 la "Parte sesta-bis – Disciplina sanzionatoria degli illeciti amministrativi e penali in materia di tutela ambientale".

Tra le principali novità della riforma si segnalano le seguenti: i) introdotta un'aggravante ambientale applicabile a tutti i fatti già previsti come reato; ii) per i nuovi delitti contro l'ambiente, raddoppiati i termini di prescrizione; iii) prevista la diminuzione dei due terzi delle pene in caso di "ravvedimento operoso"; iv) previsti sconti di pena per chi si adopera per il ripristino dello stato dei luoghi. La pena accessoria della incapacità di contrattare con la Pubblica Amministrazione viene estesa anche ai condannati per i seguenti reati: inquinamento ambientale; disastro ambientale; traffico e abbandono di materiale ad alta radioattività; impedimento del controllo; attività organizzate per il traffico illecito di rifiuti.

Pressoché tutti i reati introdotti assumono rilevanza ai sensi del decreto 231, quali reati presupposto (inseriti nell'art. 25-undecies) ovvero in via indiretta perché intervengono in modo significativo nella descrizione o valutazione delle condotte penalmente rilevanti anche ai sensi di tale decreto.

Art. 25-quinquiesdecies - I reati tributari

Articolo 231	CATALOGO REATI PRESUPPOSTO 231 - Aggiornato alla data del 15 dicembre 2021 (ultimo provvedimento inserito: Legge 238/2021)	Reato presupposto	sanzione pecuniaria max	IMPATTO (Automatico)	sanzione interdittiva max	IMPATTO 2 (automatico)	IMPATTO TOTALE (automatico)	Giudizio Qualitativo
25-quinquiesdecies	Reati Tributari	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2 D.Lgs. n. 74/2000)	500	3	C/D/E	4	4	Medio-alto
25-quinquiesdecies	Reati Tributari	Dichiarazione fraudolenta mediante altri artifici (art. 3 D.Lgs. n. 74/2000)	500	3	C/D/E	4	4	Medio-alto

25-quinquiesdecies	Reati Tributari	Emissione di fatture o altri documenti per operazioni inesistenti (art. 8 D.Lgs. n. 74/2000)	500	3	C/D/E	4	4	Medio-alto
25-quinquiesdecies	Reati Tributari	Occultamento o distruzione di documenti contabili (art. 10 D.Lgs. n. 74/2000)	400	2	C/D/E	4	3	Medio
25-quinquiesdecies	Reati Tributari	Sottrazione fraudolenta al pagamento di imposte (art. 11 D.Lgs. n. 74/2000)	400	2	C/D/E	4	3	Medio

La Legge 19 dicembre 2019, n. 157, pubblicata in Gazzetta Ufficiale il 24 dicembre 2019, ha convertito con modificazioni il decreto legge 26 ottobre 2019, n. 124 "Disposizioni urgenti in materia fiscale e per esigenze indifferibili", c.d. "Decreto Fiscale", con il quale sono state introdotte nel nostro ordinamento importanti novità in materia di reati tributari e responsabilità amministrativa degli enti.

A pochi mesi dal Decreto Fiscale, poi, il D.Lgs. 75/2020 (in vigore dal 30 luglio 2020) ha esteso nuovamente il catalogo dei reati presupposto per la responsabilità dell'ente in materia tributaria.

Con tale ultimo provvedimento il governo ha integrato le disposizioni del Decreto 231 dando attuazione alla "Direttiva PIF" (Direttiva UE 2017/1371) prevedendo la responsabilità amministrativa da reato delle persone giuridiche anche per le "gravi" frodi in materia IVA, laddove il concetto di gravità è definito dalla "Direttiva PIF" avendo riguardo al carattere transfrontaliero delle condotte illecite ("connessa a due o più Stati membri") e all'elevato ammontare del danno complessivo ("almeno pari a dieci milioni di euro").

La novella, integrata con quanto disposto da ultimo dal D.Lgs. 75/2020, ha previsto l'inserimento dell'art. 25 quinquiesdecies nel D.Lgs. n. 231/2001 il quale oggi prevede: in relazione alla

commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, si applicano all'Ente le seguenti sanzioni pecuniarie:

a) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti previsto dall'articolo 2, comma 1, la sanzione pecuniaria fino a cinquecento quote;
b) per il delitto di dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 2, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
c) per il delitto di dichiarazione fraudolenta mediante altri artifici, previsto dall'articolo 3, la sanzione pecuniaria fino a cinquecento quote;
d) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 1, la sanzione pecuniaria fino a cinquecento quote;
e) per il delitto di emissione di fatture o altri documenti per operazioni inesistenti, previsto dall'articolo 8, comma 2-bis, la sanzione pecuniaria fino a quattrocento quote;
f) per il delitto di occultamento o distruzione di documenti contabili, previsto dall'articolo 10, la sanzione pecuniaria fino a quattrocento quote;
g) per il delitto di sottrazione fraudolenta al pagamento di imposte, previsto dall'articolo 11, la sanzione pecuniaria fino a quattrocento quote. 1-bis.

In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, 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, si applicano all'Ente le seguenti sanzioni pecuniarie:

a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;
b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;
c) per il delitto di indebita compensazione previsto dall'articolo 10-quater, la sanzione pecuniaria fino a quattrocento quote. 2. Se, in seguito alla commissione dei delitti indicati ai

commi 1 e 1-bis, l'ente ha conseguito un profitto di rilevante entità, la sanzione pecuniaria è aumentata di un terzo.

Nei casi previsti dai commi 1, 1-bis e 2, si applicano le sanzioni interdittive di cui all'articolo 9, comma 2, lettere c), d) ed e)."

In considerazione di tali elementi, le principali aree/processi di rischio interessate sono quelle riportate nella tav. 3 Risk analysis.

Le misure di controllo:

- adesione a Protocolli di legalità;
- check list di controllo degli operatori economici
- digitalizzazione degli affidamenti
- procedura pagamenti
- segregazione
- controlli gerarchici
- trasparenza
- codice etico
- sistema sanzionatorio
- whistelblowing

5. La valutazione del rischio-modalità operative

La metodologia integrata di valutazione del rischio è sviluppata considerando le peculiarità metodologiche e normative dei due *framework* ex D. Lgs. 231/01 ed ex L. 190/2012/PNA ed ha come obiettivo la definizione di una matrice di valutazione «complessiva» dei rischi, pur tenendo in considerazione le differenze intrinseche tra i due ambiti (ad esempio criterio di interesse o vantaggio dell'Ente proprio del solo D. Lgs. 231, rispetto alla ratio della c.d. «*maladministration*» propria della L. 190).

L'art. 6, comma 2 lettere a) e b), del D.lgs. 231/2001 indica, tra le caratteristiche essenziali per la costruzione del modello di organizzazione e gestione, l'attivazione di un adeguato processo di *risk management* (gestione del rischio aziendale).

Pertanto, per poter applicare un efficace Modello, una delle prime attività da programmare, dal

punto di vista prettamente organizzativo, è l'introduzione di un sistema di analisi del rischio sviluppato attraverso lo studio della struttura organizzativa, l'analisi delle singole aree di rischio e l'individuazione di cariche e funzioni che guidano l'attività d'impresa.

Per rischio si intende un qualsiasi evento che possa avere un impatto negativo sul raggiungimento degli obiettivi aziendali. Per rischio accettabile si intende l'ammontare del rischio che un'azienda è disposta ad accettare nel perseguire la creazione di valore.

L'identificazione e la valutazione del rischio (cosiddetto *risk assesment*) rappresentano, pertanto, attività tipiche del processo di *risk management*, cui devono seguire specifiche scelte dei soggetti aziendali a vario livello responsabili gestione del rischio appunto, nonché e idonee azioni di monitoraggio dell'adeguatezza delle scelte stesse.

Contestualizzando tale processo nell'ambito dei Modelli di prevenzione dei reati richiesto dal D.lgs. 231/2001, la metodologia della norma UNI EN ISO 31000 fornisce indicazioni utili per procedere alla mappatura ed alla valutazione dei rischi finalizzata all'elaborazione ed attuazione di un modello organizzativo secondo quanto previsto dal D.lgs. 231/2001 anche in una logica integrata 231/190.

Assumere a riferimento metodologico, nei suoi tratti principali, lo standard UNI EN ISO 31000 è utile in quanto questo standard fornisce una serie completa di principi e linee guida per aiutare le organizzazioni a eseguire l'analisi e la valutazione dei rischi.

A tal proposito è opportuno:

a) stabilire il contesto in cui opera l'organizzazione;

b) identificare il rischio;

c) analizzare il rischio;

d) ponderare il rischio.

a) Stabilire il contesto in cui opera l'organizzazione

Il contesto è rappresentato dall'ambiente, interno ed esterno, in cui opera l'Organizzazione. Identificare e definire il contesto settoriale, territoriale, giuridico (contesto esterno) e il contesto organizzativo, economico, finanziario, patrimoniale, tecnologico (contesto interno) è l'attività di partenza per - effettuare una valutazione sintetica del proprio profilo di rischio, identificando le

tipologie di rischio da prendere in considerazione e focalizzando l'attenzione su quelle fattispecie di rischio che, per quanto improbabili, hanno comunque un certo grado di verosimiglianza - stabilire gli obiettivi dell'Organizzazione, le metodiche e le misure da attuare per il raggiungimento di tali obiettivi.

b) Identificare il rischio

I reati presupposti richiamati dal D.lgs. 231/01 sono diversi ed eterogeni e si riferiscono a diversi contesti operativi.

Fatta tale premessa, ne deriva che non tutti i reati previsti dal D.lgs. 231/01 trovano attinenza con la specifica realtà aziendale.

La mancata attinenza dei reati previsti dal D.lgs. 231/01 può derivare da:

- assenza di interesse o vantaggio dalla commissione del reato;
- assenza di risorse per la commissione del reato (risorse finanziarie, infrastrutture, competenze, ecc.);
- assenza di possibilità per la commissione del reato (attività, processi, rapporti in essere).

c) Analizzare il rischio e le priorità

I reati considerati attinenti al contesto di riferimento nel quale l'ente opera, devono essere analizzati per determinare il relativo livello di rischio.

In generale per valutare la pericolosità di un evento e conseguentemente definire la priorità o l'urgenza delle misure necessarie per tenerlo sotto controllo è bene utilizzare la metodologia del "*Risk Approach*" volta alla determinazione del rischio associato a funzioni/processi sensibili. Tale procedura prevede una verifica dello stato delle procedure attuate dall'Organizzazione, per ricercare e valutare il rischio connesso, in modo da individuare le modalità e procedure di gestione del rischio ("*Risk Management*"). Tale procedura permette di determinare l'indice di rischio per ogni tipologia di reato analizzata e conseguentemente definire le priorità nell'intervento ed i relativi programmi di eliminazione o di riduzione e gestione del rischio. Nell'ambito di questa analisi devono essere identificati i soggetti responsabili dei processi e delle attività potenzialmente a rischio ed effettuate le interviste di dettaglio con l'obiettivo di delineare

un quadro completo della realtà aziendale.

Pertanto, il processo di analisi dei rischi di reato può essere considerato, quindi, come composto da due fasi. La prima è quella del c.d. "Inquadramento Organizzativo", in cui si definisce il perimetro di intervento tramite il rilevamento delle aree nelle quali possono essere compiuti atti rilevanti ai fini della commissione dei reati. La seconda sottofase consiste invece nell' "analisi della situazione esistente", nella quale, partendo dalla mappatura preliminare dei processi, si procede ad illustrare la reale situazione approfondendo, per ciascun processo sensibile individuato, gli elementi specifici che lo caratterizzano alla luce di quanto previsto dal Decreto.

La realizzazione di quanto previsto in queste due sottofasi, permette di ottenere la c.d. "Correlazione Rischio/Processo", vale a dire la fotografia dell'assetto organizzativo dell'ente in esame nel periodo di riferimento.

La documentazione raccolta e le interviste effettuate devono essere svolte avendo riguardo alla concreta realtà Aziendale.

Premesso quanto sopra in sintesi dovrà essere svolto quanto segue:

- studio preliminare della documentazione ufficiale disponibile presso la società, e relativa a: Organigramma e ripartizione delle funzioni; Deleghe e procure; Regolamenti operativi e procedure formalizzate; Sistema sanzionatorio esistente; Contrattualistica rilevante;
- Interviste al personale responsabile delle diverse funzioni;
- Interviste al soggetto responsabile della gestione di ogni singola attività rilevante, finalizzata all'identificazione delle procedure operative e concreti controlli esistenti ed idonei a presidiare il rischio individuato.

È necessario individuare quale sia la "struttura organizzativa" dell'Ente. Considerato dalla letteratura specialistica quale primo elemento fondamentale dell'organizzazione aziendale, la struttura definisce il ruolo ed il comportamento che la Società attende dai suoi membri, prescrivendo compiti e modalità di svolgimento.

La struttura consiste anche nelle relazioni tra le diverse funzioni individuate attraverso la razionalizzazione di un modello di divisione e coordinamento del lavoro prettamente "formale".

La rappresentazione di questa struttura avviene attraverso la cosiddetta "mappatura dei processi" che definisce l'attività operativa dell'Ente in esame e dei rispettivi centri di responsabilità.

La struttura organizzativa in esame può sostanzialmente essere rappresentata attraverso l'articolazione di due tipologie di processi:

- primari: ovvero quella serie di attività logiche il cui output è direttamente collegabile al core business aziendale;
- di supporto: ovvero quella serie di attività che supportano le attività primarie nei vari momenti della vita della Società.

All'interno della mappatura effettuata occorre, a questo punto, esplicitare i processi in cui si evidenzia un potenziale rischio di reato nonché le posizioni organizzative interessate (o comunque coinvolte) nello svolgimento delle attività operative del processo stesso. L'individuazione degli ambiti nei quali il rischio può presentarsi in maggiore misura, mette in evidenza come si tratti di tipologie che possono realizzarsi in molte aree aziendali ed a tutti i livelli organizzativi individuati.

L'identificazione dei rischi deve includere tutti gli eventi rischiosi che, anche solo ipoteticamente, potrebbero verificarsi. Per una corretta identificazione dei rischi è necessario definire, in via preliminare, l'oggetto di analisi, ossia l'unità di riferimento rispetto al quale individuare gli eventi rischiosi; nel Modello integrato 231/190 sono state prese a riferimento le singole attività del processo in corrispondenza delle quali è stato identificato il rischio compreso nel c.d. "Registro del rischio".

Si è dunque passati all'identificazione dei fattori abilitanti da intendersi quali cause degli eventi rischiosi, l'analisi di questi fattori consente di individuare le misure specifiche di trattamento più efficaci, ossia le azioni di risposta più appropriate e indicate per prevenire i rischi.

Tra i fattori abilitanti è possibile individuare, considerando le indicazioni fornite da ANAC (allegato 1 PNA 2019):

a) mancanza di misure di trattamento del rischio (controlli): in fase di analisi andrà verificato se presso l'ente siano già stati predisposti – ma soprattutto efficacemente attuati – strumenti di controllo relativi agli eventi rischiosi;

b) mancanza di trasparenza;

c) eccessiva regolamentazione, complessità e scarsa chiarezza della normativa di riferimento;

d) esercizio prolungato ed esclusivo della responsabilità di un processo da parte di pochi o di

un unico soggetto;

e) scarsa responsabilizzazione interna;

f) inadeguatezza o assenza di competenze del personale addetto ai processi;

g) inadeguata diffusione della cultura della legalità;

h) mancata attuazione del principio di distinzione tra politica e amministrazione.

d) Ponderare il rischio

Nella ponderazione del rischio si è fatto ricorso ad una misurazione mista quantitativa-qualitativa valorizzando 2 parametri: impatto e probabilità.

Per "gravità del reato" si intende l'impatto che l'episodio delittuoso può avere, o ha già avuto, sull'organizzazione aziendale secondo il trattamento sanzionatorio previsto per i singoli reati dal D. lgs. 231/2001. La gravità dei reati è pertanto desunta assumendo quale parametro di riferimento esclusivo il trattamento sanzionatorio. Per semplicità si è fatto riferimento alla seguente scala di valutazione:

0-0,99	MINIMO
1-1,99	BASSO
2-2,99	MEDIO-BASSO
3	MEDIO
3,1-4	MEDIO-ALTO
4,1-5	ALTO

In particolare, ponendo l'attenzione sia sulle sanzioni amministrative patrimoniali, sia sulle sanzioni interdittive, è evidente che la previsione di sanzioni interdittive, più consistenti rispetto alle sanzioni patrimoniali, non può che innalzare il livello di gravità dei reati, dunque l'impatto.

Per questo motivo, è ritenuto significativo il valore di gravità anche nei casi di sanzioni patrimoniali di per sé tenui, ma congiunte a sanzioni interdittive.

Per quanto concerne le sanzioni amministrative patrimoniali a carico dell'Ente, si è preso in considerazione, laddove la normativa preveda una forbice tra un minimo e un massimo, solo il massimo. Si ritiene che tale metodo consenta di valutare con la massima prudenza gli effetti dannosi che un reato può determinare nei confronti dell'ente.

Alla luce di quanto descritto, appare evidente come l'impatto del reato rilevato rappresenti una sorta di classificazione dei rischi di reato valutata per la gravità delle loro conseguenze. I valori riportati in questa scala, permettono quindi di valutare l'Impatto del reato ovvero individuare quali rischi di reato possano avere le conseguenze più gravi sulla struttura organizzativa articolata dai processi individuati attraverso la mappatura effettuata.

Nelle tavole 1 e 2 allegate è possibile avere il dettaglio della valorizzazione del parametro impatto per ciascuna singola fattispecie di reato (*risk analysis*).

Nella tabella che segue una valutazione dell'impatto di tipo sintetica.

REATO 231	VALORE/IMPATTO – regime sanzionatorio 231	
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 (modificato dalla L. n. 161/2017 e dal D.Lgs. n. 75/2020)	**3,5**	Medio-Alto
ART 24-BIS Delitti informatici e trattamento illecito di dati aggiunto dalla L. n. 48/2008 (modificato dal D.Lgs. n. 7 e 8/2016, dal D.L. 105/2019 e dalla L. 238/2021)	**3,5**	Medio-Alto
ART 24-TER Delitti di criminalità organizzata (aggiunto dalla L. n. 94/2009 e modificato dalla L. 69/2015)	4,9	Alto
ART 25 Peculato, concussione, induzione indebita a dare o promettere utilita`, corruzione e abuso d'ufficio (modificato dalla L. n. 190/2012, dalla L. 3/2019 e dal D.Lgs. n. 75/2020)	4	Medio-Alto
ART. 25-BIS.1 Delitti contro l'industria e il commercio (aggiunto dalla L. n. 99/2009)	2	Medio-Basso
ART 25-TER Reati societari (aggiunto dal D.Lgs. n. 61/2002; modificato dalla L. n. 190/2012, dalla L. 69/2015 e dal D.Lgs. n. 38/2017)	2,2	Medio-Basso
Art. 25-septies Reati di omicidio colposo e lesioni colpose gravi o gravissime, commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro (aggiunto dalla L. n. 123/2007; modificato L. n. 3/2018)	4	Medio-Alto
Art. 25-octies Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio aggiunto dal D.Lgs. n. 231/2007; modificato dalla L. n. 186/2014 e dal D.Lgs. n. 195/2021)	5	Alto
Art. 25-novies Delitti in materia di violazione del diritto d'autore (aggiunto dalla L. 99/2009)	4	Medio-Alto
Art. 25-decies Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (aggiunto dalla L. n. 116/2009)	2	Medio-Basso
Art. 25-undecies Reati ambientali aggiunto dal D.Lgs. n. 121/2011, modificato dalla L. n. 68/2015, modificato dal D.Lgs. n. 21/2018	2	Medio-Basso
Art. 25-quinquesdecies reati tributari (aggiunto dalla L. n. 157/2019, modificato dal D.Lgs. n. 75/2020)	3	Medio

La “Frequenza di accadimento” riguarda, invece, la probabilità che possa essere commesso uno specifico reato.

Il punteggio assegnato alla probabilità, che si verifichi una tal situazione rappresenta un “significato” piuttosto che un valore.

Il fatto di calmierare attraverso una costante attività di monitoraggio una o più cause/meccanismi che possano addurre ad una commissione di reato è il solo modo in cui si possa influenzare il punteggio della Frequenza, riducendola.

La stima della probabilità di accadimento di tali potenziali causa/meccanismi è valutata su un ranking 1-3.

Nel determinare questa stima sono state considerate le seguenti variabili:

- il grado di discrezionalità nelle attività svolte o negli atti prodotti;
- l’analisi storica delle segnalazioni o degli accadimenti negativi per ogni specifica attività sensibile;
- eventuali cambiamenti delle singole attività operative per processo;
- il grado di significatività del reato;
- la rilevanza degli interessi “esterni”.

Alle misure esistenti, quali strumenti di mitigazione del rischio, è stato attribuito un *ranking* di valutazione da 1 a 2, quale abbattimento del rischio come si evince dalle mappature.

La valutazione è quindi il risultato di:

(IxP)-M

dove:

- “I” impatto ranking 1-5;
- “P” probabilità ranking 1-3;
- “M” misura ranking 1-2.

Da cui deriva la seguente matrice di rischio.

0,1-1,99	BASSO
2-3,99	MEDIO-BASSO
4-8	MEDIO
8,1-12,99	MEDIO-ALTO
13-15	ALTO

6. Le misure di mitigazione del rischio

Per tutti gli enti, siano essi grandi, medi o piccoli, il sistema di controlli preventivi deve essere tale che lo stesso:

- nel caso di reati dolosi, non possa essere aggirato se non fraudolentemente;
- nel caso di reati colposi, come tali incompatibili con l'intenzionalità fraudolenta, risulti comunque violato, nonostante la puntuale osservanza degli obblighi di vigilanza da parte dell'apposito organismo.

Si delineano, in particolare, i seguenti livelli di presidio:

- ✔ un 1° livello di controllo, che definisce e gestisce i controlli cosiddetti di linea, insiti nei processi operativi, e i relativi rischi. È svolto generalmente dalle risorse interne della struttura, sia in autocontrollo da parte dell'operatore, sia da parte del preposto/dirigente ma può comportare, per aspetti specialistici (ad esempio per verifiche strumentali) il ricorso ad altre risorse interne o esterne all'azienda. Tra questi particolare importanza riveste il Servizio di Prevenzione e Protezione che è chiamato ad elaborare, per quanto di competenza, i sistemi di controllo delle misure adottate;
- ✔ un 2° livello di controllo, svolto da strutture tecniche aziendali competenti in materia e indipendenti da quelle del 1° livello, nonché dal settore di lavoro sottoposto a verifica. Tale monitoraggio presidia il processo di gestione e controllo dei rischi legati all'operatività del sistema, garantendone la coerenza rispetto agli obiettivi aziendali dove si collocano anche il RPC e il RT;
- ✔ per le organizzazioni più strutturate e di dimensioni medio-grandi, un 3° livello di controllo, effettuato dall'*Internal Audit*, che fornisce *assurance*, ovvero valutazioni indipendenti sul disegno e sul funzionamento del complessivo Sistema di Controllo Interno, accompagnato da piani di miglioramento definiti in accordo con il *Management*.

Codice etico

L'adozione di principi etici, ovvero l'individuazione dei valori aziendali primari cui l'impresa intende conformarsi è espressione di una determinata scelta aziendale e costituisce la base su cui impiantare il sistema di controllo preventivo. Deve costituire profilo di riferimento per ogni realtà imprenditoriale la raccomandazione di un elevato standard di professionalità, nonché il divieto di comportamenti che si pongano in contrasto con le disposizioni legislative e con i valori deontologici.

Procedure

Le procedure manuali ed informatiche (sistemi informativi) devono essere tali da regolamentare lo svolgimento delle attività prevedendo gli opportuni punti di controllo (es. quadrature).

Una particolare efficacia preventiva riveste lo strumento di controllo rappresentato dalla separazione di compiti fra coloro che svolgono fasi o attività cruciali di un processo a rischio. In questo campo, specifico interesse ricopre l'area della gestione finanziaria, dove il controllo procedurale si avvale di strumenti consolidati nella pratica amministrativa, quali per esempio abbinamento firme, riconciliazioni frequenti, supervisione, separazione di compiti con la già citata contrapposizione di funzioni, ad esempio fra la funzione acquisti e quella finanziaria.

Particolare attenzione deve essere riposta sui flussi finanziari non rientranti nei processi tipici aziendali, soprattutto se si tratta di ambiti non adeguatamente proceduralizzati e con caratteri di estemporaneità e discrezionalità.

In ogni caso è necessario che siano sempre salvaguardati i principi di trasparenza, verificabilità, tracciabilità, inerenza all'attività aziendale.

Sarà opportuno valutare nel tempo la separazione dei compiti all'interno di ogni processo a rischio, verificando che le procedure aziendali e/o le prassi operative siano periodicamente aggiornate e tengano costantemente in considerazione le variazioni o novità intervenute nei processi aziendali e nel sistema organizzativo. Ciò vale soprattutto per l'attribuzione di responsabilità, le linee di dipendenza gerarchica e la descrizione dei compiti che devono essere assegnati in coerenza con le responsabilità organizzative e gestionali.

Sistema organizzativo sufficientemente aggiornato, formalizzato e chiaro

Talune funzioni possono essere assegnate a un soggetto diverso da quello originariamente titolare, ma occorre definire preliminarmente in modo chiaro e univoco i profili aziendali cui sono affidate la gestione e la responsabilità delle attività a rischio reato, avendo riguardo anche al profilo dell'opponibilità delle procure a terzi. La procura deve costituire lo strumento per un più efficace adempimento degli obblighi imposti dalla legge, non per un agevole trasferimento di responsabilità.

In particolare, è opportuno che l'attribuzione delle deleghe e dei poteri di firma relativi alla gestione delle risorse finanziarie e all'assunzione e attuazione delle decisioni dell'ente in relazione ad attività a rischio reato:

- sia formalizzata in conformità alle disposizioni di legge applicabili;
- indichi con chiarezza i soggetti delegati, le competenze richieste ai destinatari della delega e i poteri rispettivamente assegnati;
- preveda limitazioni delle deleghe e dei poteri di spesa conferiti;
- preveda soluzioni dirette a consentire un controllo sull'esercizio dei poteri delegati;
- disponga l'applicazione di sanzioni in caso di violazioni dei poteri delegati;
- sia disposta in coerenza con il principio di segregazione;
- sia coerente con i regolamenti aziendali e con le altre disposizioni interne applicati dalla società.

Procedure e Sistema organizzativo – principi di controllo

Le procedure e il sistema organizzativo devono essere improntati ai seguenti principi di controllo:

- "Ogni operazione, transazione, azione deve essere: verificabile, documentata, coerente e congrua". Per ogni operazione vi deve essere un adeguato supporto documentale su cui si possa procedere in ogni momento all'effettuazione di controlli che attestino le caratteristiche e le motivazioni dell'operazione e individuino chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa;
- "Nessuno può gestire in autonomia un intero processo". Il sistema deve garantire l'applicazione del principio di separazione di funzioni, per cui l'autorizzazione all'effettuazione di un'operazione deve essere sotto la responsabilità di persona diversa da chi contabilizza, esegue operativamente o controlla l'operazione. Occorre che: a nessuno vengano attribuiti poteri illimitati; i poteri e le responsabilità siano chiaramente definiti e conosciuti all'interno dell'organizzazione; i poteri autorizzativi e di firma siano coerenti con le responsabilità organizzative assegnate e opportunamente documentati in modo da garantirne, all'occorrenza, un'agevole ricostruzione ex post;
- "I controlli devono essere documentati". Il sistema di controllo dovrebbe prevedere un sistema di reporting (eventualmente attraverso la redazione di verbali) adatto a documentare l'effettuazione e gli esiti dei controlli, anche di supervisione.

Comunicazione al personale e sua formazione

Sono due importanti requisiti del modello ai fini del suo buon funzionamento e devono essere diversamente modulati in base ai destinatari: i dipendenti nella loro generalità, quelli che operano in specifiche aree di rischio/attività sensibili, i componenti degli organi sociali ecc.

Con riferimento alla comunicazione, essa deve riguardare ovviamente il codice etico, ma anche gli altri strumenti quali i poteri autorizzativi, le linee di dipendenza gerarchica, le procedure, i flussi di informazione e tutto quanto contribuisca a dare trasparenza nell'operare quotidiano.

La comunicazione deve essere: capillare, efficace, autorevole (cioè emessa da un livello adeguato), chiara e dettagliata, periodicamente ripetuta. Inoltre, occorre consentire l'accesso e la consultazione della documentazione costituente il Modello anche attraverso l'intranet aziendale.

Accanto alla comunicazione, deve essere sviluppato un adeguato programma di formazione modulato in funzione dei livelli dei destinatari. Esso deve illustrare le ragioni di opportunità - oltre che giuridiche - che ispirano le regole e la loro portata concreta. In proposito, è opportuno prevedere il contenuto dei corsi di formazione, la loro periodicità, l'obbligatorietà della partecipazione ai corsi, i controlli di frequenza e di qualità sul contenuto dei programmi, l'aggiornamento sistematico dei contenuti degli eventi formativi in ragione dell'aggiornamento del Modello. È importante che l'attività di formazione sul decreto 231 e sui contenuti dei modelli organizzativi adottati da ciascun ente sia promossa e supervisionata dall'Organismo di Vigilanza della società, che a seconda delle singole realtà potrà avvalersi del supporto operativo delle funzioni aziendali competenti o di consulenti esterni.

Le misure di mitigazione dei rischi 231/190 sono indicate nelle mappature integrate 231/190.

Le misure sono state valorizzate con un ranking da 0,1 a 2 quale abbattimento del rischio valutato come prodotto dell'impatto e della probabilità.

Nelle mappature viene anche data indicazione delle misure che saranno oggetto di istituzione ove assenti o di revisione qualora ritenuto opportuno, nella colonna finale delle mappature viene indicata la tempistica con cui si intende procedere.

Le misure ad oggi esistenti sono in parte "misure generali" in parte "misure specifiche" elencate nella sezione II: Parte anticorruzione e trasparenza.

7. Il whistleblowing

In Italia l'istituto giuridico del Whistleblowing è stato introdotto dalla legge 6 novembre 2012, n. 190, in particolare, l'art. 1, co. 51, della richiamata legge ha inserito l'art. 54-bis all'interno del d.lgs. 30 marzo 2001 n. 165 «Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche». Tale norma prevede un regime di tutela del dipendente pubblico che segnala condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro.

L'art. 54-bis, co. 2, del d.lgs. 165/2001, come modificato dall'art. 1 della l. 179/2017, individua l'ambito soggettivo di applicazione della disciplina sulla tutela del dipendente che segnala condotte illecite, ampliando la platea dei soggetti destinatari rispetto al previgente art. 54-bis, che si riferiva genericamente ai "dipendenti pubblici".

L'istituto del whistleblowing è indirizzato alla tutela di chi riveste la qualifica di dipendente pubblico. Per "dipendenti pubblici" la norma intende soggetti fra loro molto diversi, alcuni dei quali non hanno alcun rapporto di lavoro subordinato con le amministrazioni pubbliche di cui al d.lgs. n. 165 del 2001 - che, pure, contiene l'art. 54-bis - ma sono dipendenti di imprese private che svolgono però attività per le pubbliche amministrazioni. È evidente che l'obiettivo primario della legge è quello di fare in modo che il segnalante/dipendente pubblico non subisca conseguenze e discriminazioni per essersi esposto nell'interesse pubblico.

Ai fini della tutela del whistleblower, la legge ha equiparato ai dipendenti pubblici anche i dipendenti di enti pubblici economici e i dipendenti di enti di diritto privato sottoposti a controllo pubblico, secondo la nozione di società controllate di cui all'art. 2359 del c.c., anche le società in house soggette al controllo analogo, disgiunto o congiunto, sono pertanto incluse nell'ambito soggettivo di applicazione della normativa sulla tutela del dipendente.

La nuova formulazione dell'art. 54-bis, d.lgs. n. 165 del 2001, stabilisce al co. 2 che la disciplina sulla tutela degli autori di segnalazioni "si applica anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica". Si tratta dunque di soggetti che, pur dipendenti di enti privati, operano nel contesto lavorativo dell'amministrazione pubblica e, quindi, possono venire a conoscenza di illeciti ivi compiuti. La disposizione sembra riferirsi a tutte quelle situazioni in cui un'impresa si trovi a fornire beni e servizi o a realizzare un'opera nei confronti dell'amministrazione anche al di fuori dell'ambito di

applicazione del Codice dei contratti pubblici (d.lgs. 18 aprile 2016, n. 50), estendendo, ad esempio, l'ambito di applicazione ai cd. contratti esclusi. Questa lettura consente di includere situazioni quali, ad esempio, affidamenti diretti a favore di imprese soggette al controllo analogo, di per sé non qualificabili come contratti pubblici, ovvero situazioni di convenzionamento gratuito o che prevedono meri rimborsi spese a favore dell'affidatario[1].

La legge disciplina:

- le segnalazioni di condotte illecite di cui il dipendente sia venuto a conoscenza in ragione del rapporto di lavoro;
- le comunicazioni di misure ritenute ritorsive adottate dall'amministrazione o dall'ente nei confronti del segnalante in ragione della segnalazione.

Come previsto dall'art 54-bis (art. 1, co. 1), le prime possono essere inviate, a discrezione del whistleblower, al RPCT dell'ente ove si è verificata la presunta condotta illecita o ad ANAC. Il dipendente può anche valutare di inoltrare una denuncia «all'autorità giudiziaria ordinaria o a quella contabile».

L'unico soggetto che, all'interno dell'ente, può ricevere le segnalazioni di whistleblowing, con le connesse garanzie di protezione del segnalante, è il RPCT. Nel caso di segnalazioni destinate unicamente al superiore gerarchico, il whistleblower non sarà tutelato ai sensi dell'art. 54-bis.

L'Organismo di Vigilanza (OdV) potrebbe essere coinvolto in via concorrente ovvero successiva, per evitare il rischio che il flusso di informazioni generato dal meccanismo di whistleblowing sfugga del tutto al suo monitoraggio[2].

Peraltro, in queste ipotesi, se l'impresa attiva dei canali anche per la segnalazione di illeciti diversi rispetto a quelli considerati dalla legge n. 179 e connessi alla disciplina 231, si può assegnare al destinatario anche una funzione di filtro: effettuare una prima valutazione sommaria delle segnalazioni per verificarne l'eventuale rilevanza sul piano 231 e, in caso positivo, informare tempestivamente l'Organismo di Vigilanza[3].

---

[1] Cfr Linee guida ANAC 2021 whistleblowing

[2] Cfr. Parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231, 21.05.2020 "il presente parere ha ad oggetto solo il ruolo, ai fini privacy, che l'OdV assume con riferimento ai flussi di informazioni rilevanti ai sensi dell'art. 6, commi 1 e 2 del d.lgs. n. 231/2001, rimanendo escluso il nuovo e diverso ruolo che l'organismo potrebbe acquisire in relazione alle segnalazioni effettuate nell'ambito della normativa di whistleblowing (art. 6, comma 2-bis, 2-ter, 2-quater cit., d.lgs. n. 231/2001)."

[3] Cfr Linee guida Confindustria giugno 2021

Per quanto riguarda le "comunicazioni di misure ritorsive" la norma prevede, invece, che esse siano trasmesse esclusivamente ad ANAC (art 54-bis, art. 1, co. 1).

Perché al segnalante possa accordarsi la tutela prevista dall'art. 54-bis i presupposti sono i seguenti:

- ✔ il segnalante deve rivestire la qualifica di "dipendente pubblico" o equiparato;
- ✔ la segnalazione deve avere ad oggetto "condotte illecite";
- ✔ il dipendente deve essere venuto a conoscenza di tali "condotte illecite" "in ragione del proprio rapporto di lavoro";
- ✔ la segnalazione deve essere effettuata "nell'interesse all'integrità della pubblica amministrazione";
- ✔ la segnalazione deve essere inoltrata ad almeno uno delle quattro tipologie di destinatari indicati nell'art. 54-bis, co. 1 (RPCT, ANAC, Autorità giudiziaria ordinaria o contabile).

Il sistema di protezione che la legge riconosce al whistleblower si compone di tre tipi di tutela:

- la tutela della riservatezza dell'identità del segnalante e della segnalazione;
- la tutela da eventuali misure ritorsive o discriminatorie eventualmente adottate dall'ente a causa della segnalazione effettuata;
- l'esclusione dalla responsabilità nel caso in cui il whistleblower sveli, per giusta causa, notizie coperte dall'obbligo di segreto d'ufficio, aziendale, professionale, scientifico o industriale ovvero violi l'obbligo di fedeltà.

L'art. 54-bis non include nel proprio campo di applicazione le segnalazioni anonime e cioè quelle del soggetto che non fornisce le proprie generalità; infatti, la protezione opera solo nei confronti di soggetti individuabili, riconoscibili e riconducibili alla categoria di dipendenti pubblici, in ogni caso, l'Ente deve registrare le segnalazioni anonime e quelle di soggetti estranei alla p.a. pervenute attraverso i canali dedicati al whistleblowing.

La legge assegna al RPCT un ruolo fondamentale nella gestione delle segnalazioni.

Il ruolo del RPCT si sostanzia in una significativa attività istruttoria.

Il RPCT è pertanto il soggetto legittimato, per legge, a trattare i dati personali del segnalante e, eventualmente, a conoscerne l'identità.

Le procedure, preferibilmente informatizzate, per la ricezione e gestione delle segnalazioni sono da prediligere per tutelare la riservatezza del segnalante.

SRM ha aderito al progetto WhistleblowingPA di Transparency International Italia e del Centro Hermes per la Trasparenza e i Diritti Umani e Digitali e ha adottato la piattaforma informatica prevista per adempiere agli obblighi normativi, le caratteristiche di questa modalità di segnalazione sono le seguenti: la segnalazione viene fatta attraverso la compilazione di un questionario e può essere inviata in forma anonima. Se anonima, sarà presa in carico solo se adeguatamente circostanziata; la segnalazione viene ricevuta dal Responsabile per la Prevenzione della Corruzione (RPC) e da lui gestita mantenendo il dovere di confidenzialità nei confronti del segnalante; nel momento dell'invio della segnalazione, il segnalante riceve un codice numerico di 16 cifre che deve conservare per poter accedere nuovamente alla segnalazione, verificare la risposta dell'RPC e dialogare rispondendo a richieste di chiarimenti o approfondimenti; la segnalazione può essere fatta da qualsiasi dispositivo digitale (pc, tablet, smartphone) sia dall'interno dell'ente che dal suo esterno.

Le segnalazioni possono essere inviate all'indirizzo web https://srmbologna.whistleblowing.it/#/.