CNDCEC - Reg. nr.0011689/2025 del 24/11/2025 - ore 13.59.04

Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

DOCUMENTO

LINEE GUIDA PER LO SVOLGIMENTO DELLE FUNZIONI DELL'ORGANISMO DI VIGILANZA *EX* D.LGS. 8 GIUGNO 2001, N. 231

NOVEMBRE 2025

Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

Composizione del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

Presidente

Elbano de Nuccio

Vice Presidente

Antonio Repaci

Consigliere Segretario

Giovanna Greco

Consigliere Tesoriere

Salvatore Regalbuto

Consiglieri

Gianluca Ancarani
Marina Andreatta
Cristina Bertinelli
Aldo Campo
Rosa D'Angiolella
Michele de Tavonatti
Fabrizio Escheri
Gian Luca Galletti
Cristina Marrone
Maurizio Masini
Pasquale Mazza
David Moro
Eliana Quintili
Pierpaolo Sanna
Liliana Smargiassi
Giuseppe Venneri
Gabriella Viggiano

Collegio dei revisori

Presidente

Rosanna Marotta

Componenti

Maura Rosano
Sergio Ceccotti

Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

A cura dell'Osservatorio Nazionale 231/2001

Presidente CNDCEC

Elbano de Nuccio

Consiglieri CNDCEC delegati

Fabrizio Escheri
Eliana Quintili

Presidente

Salvatore Sodano

Componenti

Ascensionato Raffaello Carnà
Federico Maurizio d'Andrea
Rossella De Bartolomeo
Michele Furlanetto
Claudia Gualtierotti
Renato Nitti
Daniele Piva
Ciro Santoriello
Paola Tagliavini
Paolo Vernero
Antonella Volpe

Staff tecnico

Annalisa De Vivo - *Ufficio Monitoraggio legislativo CNDCEC*

Sommario

INTRODUZIONE 1

PREMESSA 2

1. INIZIO E CESSAZIONE DELL'INCARICO 2

1.1. Conferimento dell'incarico 2
1.2. Autonomia e indipendenza 4
1.3. Onorabilità e professionalità 5
1.4. Durata e cessazione dell'incarico 7

2. ATTIVITÀ DI VIGILANZA: OBIETTIVI E FUNZIONI 8

2.1. Funzioni di vigilanza 8
2.2. Attività di vigilanza: obiettivi e funzioni 11
2.2.1. Pianificazione delle attività di verifica 11
2.2.2. Tipologie di riunioni 13
2.2.3. Modalità operative delle riunioni 14
2.2.4. Attività di verifica dell'OdV 15

3. FLUSSI INFORMATIVI 16

3.1. Flussi informativi verso l'OdV 16
3.1.1. Tipologie di flussi informativi 17
3.1.2. Modalità di comunicazione dei flussi informativi verso l'OdV 20
3.2. Flussi informativi dall'OdV 21
3.2.1. Tipologie di flussi informativi 21
3.2.2. Modalità di comunicazione dei flussi informativi dall'OdV 22

4. WHISTLEBLOWING E SEGNALAZIONI 24

4.1. Il D.lgs. 24/2023 (brevi cenni) 24
4.2. Le segnalazioni rilevanti e i canali di segnalazione 25
4.3. Il ruolo dell'Organismo di vigilanza 27
4.4. I flussi informativi in materia di segnalazioni 29

5. ATTIVITÀ DELL'ODV E COMPLIANCE INTEGRATA 30

5.1. Antiriciclaggio 30
5.2. Anticorruzione 32
5.3. Privacy 33
5.4. Adeguati assetti organizzativi 35
5.5. Sicurezza sul lavoro 36

5.6. Intelligenza artificiale (IA) e cybersicurezza 38
5.7. Ambiente 41
5.8. ESG (Environmental, Social, Governance) 44
5.9. Il regime dell'adempimento collaborativo e lo strumento del TCF (Tax Control Framework) 46

6. L'ORGANISMO DI VIGILANZA NEI GRUPPI SOCIETARI 47

6.1. La nomina dell'OdV 47
6.2. Funzionamento e problematiche condivise 49
6.3. Coordinamento tra OdV del gruppo 50

Introduzione

Con la pubblicazione delle *Linee Guida per lo svolgimento delle funzioni dell'Organismo di Vigilanza*, l'Osservatorio Nazionale sul D.lgs. 231/2001, istituito dal CNDCEC, intende mettere a disposizione dei professionisti e di tutti i soggetti interessati uno strumento aggiornato, concreto e facilmente applicabile, che consideri l'evoluzione della normativa, della prassi operativa e della giurisprudenza maturata in oltre vent'anni su questa materia.

Il ruolo dell'Organismo di vigilanza (OdV) si è progressivamente ampliato e consolidato, assumendo oggi un peso determinante nel sistema dei controlli interni e nella cultura della legalità delle organizzazioni. Ciò rende necessaria una guida che non si limiti a ripercorrere i contenuti della disciplina, ma che sappia interpretarla in chiave operativa, offrendo indicazioni chiare sia a chi ricopre la funzione di componente dell'OdV, sia ai professionisti e agli organi che con essa interagiscono quotidianamente.

Le Linee Guida nascono proprio con l'obiettivo di fornire un quadro sistematico e aggiornato delle attività dell'OdV, delineando requisiti, responsabilità e *best practice* in modo coerente con la complessità delle organizzazioni contemporanee. Ampio spazio è dedicato ai temi che oggi richiedono maggiore attenzione, dall'autonomia e indipendenza degli organismi ai criteri per la pianificazione delle verifiche, dalla strutturazione dei flussi informativi al *whistleblowing*, fino all'integrazione tra la vigilanza 231 e gli altri presidi di compliance, come *privacy*, sicurezza sul lavoro, anticorruzione, antiriciclaggio, sostenibilità, cybersicurezza e intelligenza artificiale

Il documento affronta, inoltre, questioni operative che spesso emergono nella prassi: la corretta verbalizzazione delle riunioni, l'utilizzo del budget, il ricorso a competenze specialistiche, la gestione dei rapporti con gli organi sociali e con le funzioni di controllo. Non meno rilevante è l'attenzione dedicata al funzionamento dell'OdV nei gruppi societari, realtà sempre più diffuse e caratterizzate da esigenze di coordinamento e omogeneità dei presidi di prevenzione dei rischi e di controllo

Abbiamo ritenuto fondamentale adottare un approccio equilibrato: rigoroso sotto il profilo metodologico, ma allo stesso tempo flessibile, affinché le indicazioni possano adattarsi alle diverse dimensioni e ai differenti modelli organizzativi degli enti. Le Linee Guida non intendono comprimere l'autonomia di giudizio degli organismi, bensì offrire un riferimento condiviso che renda più uniforme, trasparente e riconoscibile il modo in cui la nostra categoria e tutti gli altri soggetti interessati esercitano questa funzione.

Ringrazio i componenti dell'Osservatorio che, con competenze diversificate e spirito di collaborazione, hanno contribuito alla redazione del documento. Il risultato è frutto di un lavoro collettivo che valorizza esperienze maturate sul campo e che vuole mettere a disposizione di tutti un patrimonio comune di conoscenze.

Salvatore Sodano

Presidente dell'Osservatorio Nazionale 231/2001

Premessa

Le Linee guida per lo svolgimento delle funzioni dell'Organismo di vigilanza *ex* D.lgs. 8 giugno 2001, n. 231 (nel prosieguo anche: OdV) forniscono indirizzi professionali e metodologici per l'impostazione, la pianificazione e lo svolgimento dell'attività di vigilanza.

Le indicazioni contenute nel documento sono rivolte ai professionisti che svolgono l'attività di vigilanza nell'ambito di Organismi collegiali o monocratici in un ente che abbia adottato il Modello di organizzazione, gestione e controllo per la prevenzione dei reati *ex* D.lgs. 231/2001. Sono altresì rivolte al Collegio sindacale al quale siano attribuite le funzioni dell'OdV, ai sensi dell'art. 6, comma 4-*bis*, del D.lgs. 231/2001 (introdotto dalla legge 12 novembre 2011, n. 183).

Il documento si propone di fornire strumenti operativi di riferimento per lo svolgimento delle funzioni dell'OdV, anche mediante osservazioni utili per l'analisi delle scelte adottate, nonché per la valutazione delle problematiche interpretative che più spesso emergono nella prassi.

In tale prospettiva, il documento non ripercorre la disciplina della responsabilità amministrativa degli enti, la cui conoscenza si presume già posseduta dai lettori; l'attenzione si concentra piuttosto sugli aspetti pratici e applicativi che interessano l'operatività quotidiana degli Organismi di vigilanza.

1. Inizio e cessazione dell'incarico

1.1. Conferimento dell'incarico

L'art. 6, co. 1, lett. b) del D.lgs. 231/2001 richiede che un organismo indipendente, dotato di poteri autonomi, vigili sul funzionamento e l'osservanza dei modelli organizzativi e ne curi l'aggiornamento al fine di garantirne la conformità normativa ovvero l'adeguatezza a prevenire la commissione dei reati previsti dal citato Decreto. Dai riferimenti normativi appare evidente che, in mancanza di tale organismo, anche il più strutturato Modello organizzativo non potrà definirsi efficacemente attuato e non sarà in grado, pertanto, di evitare le sanzioni a carico dell'ente in caso di commissione di illeciti e in presenza degli ulteriori requisiti previsti dalla norma.

Il D.lgs. 231/2001 non definisce la composizione e i requisiti dell'Organismo di vigilanza, lasciando agli enti la facoltà di individuare le soluzioni più idonee. In ogni caso, la composizione dell'Organismo di vigilanza deve rispettare i requisiti normativi, nonché le indicazioni di dottrina, giurisprudenza e della prassi, potendo variare anche in base alle dimensioni e alle caratteristiche dell'ente.

L'OdV è generalmente nominato dall'organo amministrativo; può non escludersi, tuttavia, che la nomina dell'Organismo sia deliberata dall'assemblea. Ciò trova conferma nel disposto di cui all'art. 6, co. 4-*bis* del D.lgs. 231/2001, che ha introdotto la possibilità di attribuire la funzione dell'OdV al Collegio sindacale. Nelle società quotate la funzione di vigilanza viene attribuita all'organo di controllo - o a un

organismo appositamente costituito - dall'organo di amministrazione, con il supporto del Comitato controllo e rischi (vd. Codice di *corporate governance*, raccomandazione n. 33).

Nelle società a partecipazione pubblica la nomina dell'OdV può avvenire tramite scelta fiduciaria (*intuitu personae*) o procedura a evidenza pubblica. La questione centrale è se l'ente, in virtù della sua natura societaria, debba seguire la disciplina privatistica del Codice civile o se, essendo partecipato dalla Pubblica Amministrazione, sia invece soggetto ai principi pubblicistici e, in tal caso, entro quali limiti. Invero, il conferimento dell'incarico di componente dell'Organismo di vigilanza nelle società pubbliche dovrebbe seguire i principi di pubblicità, imparzialità e trasparenza previsti dall'art. 7, co. 6 del D.lgs. 165/2001, in linea con le normative anticorruzione e gli obiettivi di buona amministrazione, soprattutto per le società a controllo pubblico o *in house*. In base alla norma da ultimo citata, le amministrazioni pubbliche possono conferire incarichi individuali con contratti di lavoro autonomo solo in presenza di specifiche esigenze non soddisfabili con personale interno e solo ad esperti altamente qualificati, nel rispetto dei presupposti di legittimità previsti dalla normativa; gli incarichi conferiti devono essere temporanei e altamente qualificati, senza possibilità di rinnovo.

L'organo amministrativo, responsabile dell'assetto organizzativo dell'ente e della nomina dell'OdV, può scegliere tra una composizione monocratica e collegiale dello stesso, in ragione delle caratteristiche dimensionali e organizzative dell'ente, nonché della complessità del rischio da presidiare. La soluzione più efficace sembra essere quella di una composizione plurisoggettiva dell'Organismo, che combina soggetti interni (es. responsabile compliance, responsabile internal audit, funzione legale, amministratore indipendente, sindaco) ed esterni (consulenti, esperti), ferma restando la verifica dell'assenza di conflitti d'interesse e dell'adeguatezza delle competenze. Tale configurazione garantisce un equilibrio tra conoscenza interna dell'ente e competenza specialistica esterna.

Per le imprese di piccole dimensioni l'art. 6, co. 4, D.lgs. 231/2001 consente che i compiti dell'OdV siano svolti direttamente dall'organo dirigente. Il generico riferimento agli enti di "piccole dimensioni", però, non consente di individuare con certezza il perimetro di applicazione della previsione in commento. In ogni caso, si ritiene che questa soluzione possa generare un evidente conflitto di interessi, determinando una sovrapposizione tra controllore e controllato; di conseguenza, si raccomanda di limitarne l'applicazione esclusivamente all'ipotesi di enti con bassa complessità organizzativa e con una minima suddivisione delle funzioni gestionali.

A prescindere dalla tipologia di ente che procede alla nomina, l'Organismo di vigilanza accetta l'incarico mediante dichiarazione scritta con la quale attesta il possesso dei requisiti di autonomia, indipendenza, onorabilità e professionalità di seguito esaminati.

AI fini dell'adempimento degli obblighi antiriciclaggio, l'Organismo di vigilanza monocratico, ovvero il componente dell'OdV iscritto all'Albo dei Dottori Commercialisti e degli Esperti Contabili acquisisce una copia della delibera del CdA/determina dell'amministratore unico, ovvero del verbale assembleare, da conservare nel fascicolo intestato all'ente che ne ha deliberato la nomina (si vedano le Regole Tecniche *ex* art. 11, co. 2, D.lgs. 231/2007 emanate dal CNDCEC con Deliberazione n. 9 del 16 gennaio 2025).

1.2. Autonomia e indipendenza

Autonomia

Il requisito dell'autonomia, che è richiesto all'atto di nomina e deve sussistere per tutta la durata dell'incarico, è espressamente previsto dall'art. 6 del D.lgs. 231/2001, che attribuisce all'OdV autonomi poteri di iniziativa e controllo. L'autonomia può essere definita sia come libertà di azione e autodeterminazione dell'OdV, sia come disponibilità di strumenti adeguati al suo efficace funzionamento. L'OdV, quindi, deve essere libero da interferenze o condizionamenti interni, in particolare da parte dell'organo dirigente.

Per garantire la necessaria autonomia dell'OdV, è fondamentale che esso non svolga funzioni operative o gestionali; infatti, se fosse coinvolto nelle decisioni aziendali, esso rischierebbe di compromettere la propria obiettività nelle verifiche sul rispetto del Modello organizzativo.

Per essere realmente autonomo, l'OdV deve disporre di tutti i poteri necessari per svolgere le proprie funzioni in modo efficace, senza subire interferenze o condizionamenti da parte dell'ente. A tal fine, all'Organismo deve essere assegnato un *budget* adeguato del quale possa disporre per uno svolgimento indipendente ed efficace della propria attività, ovvero per ricorrere a consulenze specialistiche ove necessario. Il *budget* deve essere definito al momento del conferimento dell'incarico e approvato dall'organo amministrativo; l'OdV ha facoltà di richiedere integrazioni qualora le risorse assegnate risultino insufficienti per svolgere efficacemente le proprie funzioni di vigilanza, ovvero qualora emergano speciali necessità di verifiche addizionali e urgenti. Nell'ambito della propria relazione periodica all'organo amministrativo, l'OdV rendiconta l'eventuale utilizzo del budget.

Indipendenza

Il requisito dell'indipendenza, che deve essere richiesto all'atto di nomina e deve sussistere per tutta la durata dell'incarico, pur non essendo espressamente richiamato dal D.lgs. 231/2001, viene comunemente incluso tra quelli richiesti all'OdV in quanto individua la necessaria condizione di assenza di conflitto di interesse nei confronti dell'ente e, quindi, del suo management. L'indipendenza si basa quindi su un equilibrio psicologico e intellettuale, che consente ai membri dell'OdV di esercitare la propria funzione in modo imparziale, senza influenze interne che possano comprometterne l'efficacia. Se l'OdV ha una composizione collegiale mista, includendo sia soggetti interni che esterni, l'indipendenza assoluta non può essere richiesta a tutti i componenti interni: per questo, l'indipendenza dell'OdV deve essere valutata nel suo insieme. Si ritiene, in ogni caso, applicabile all'Organismo il disposto dell'art. 2399 c.c. relativo al Collegio sindacale e la prassi elaborata e codificata nelle norme di comportamento del Collegio sindacale di società non quotate emanate dal CNDCEC.

Nel caso di un OdV monocratico, si ritiene che il requisito dell'indipendenza sia soddisfatto affidando le relative funzioni preferibilmente a un soggetto esterno in possesso dei requisiti di professionalità necessari per l'espletamento dell'incarico (vedi § 1.3). In tal caso, la conoscenza diretta delle dinamiche aziendali da parte dell'Organismo e il raccordo con la struttura interna possono comunque essere garantiti attraverso l'individuazione di un supporto interno, ad esempio una segreteria tecnica.

Alla luce degli orientamenti giurisprudenziali più recenti, si ritiene che l'indipendenza dell'OdV risulti compromessa nel caso in cui i suoi membri – o la maggior parte di essi – siano subordinati gerarchicamente alla direzione generale o funzionalmente dipendenti dall'organo amministrativo, ossia dagli stessi soggetti che dovrebbero controllare.

Inoltre, l'indipendenza nell'espressione del proprio giudizio risulta minata anche quando l'OdV include professionisti retribuiti da società collegate per attività professionali diverse da quelle afferenti a funzioni di controllo e vigilanza e alle funzioni in esame, poiché ciò potrebbe influenzarne l'imparzialità.

Può non escludersi la presenza di amministratori indipendenti nell'OdV poiché, per loro natura e funzione, gli stessi svolgono un ruolo di controllo all'interno dell'organo amministrativo.

L'indipendenza dell'OdV è influenzata dalla corretta determinazione, da parte dell'organo amministrativo, del compenso previsto per la funzione. Quest'ultimo deve essere equilibrato: né troppo elevato, per evitare compromissioni dell'indipendenza, né troppo basso, per scongiurare il rischio di scarsa professionalità o un ruolo meramente onorifico. Il compenso deve quindi essere commisurato all'impegno, alle competenze professionali e al livello di responsabilità richiesto ai membri dell'OdV.

1.3. Onorabilità e professionalità

Onorabilità

Il requisito di onorabilità, che deve essere richiesto all'atto di nomina e deve sussistere per tutta la durata dell'incarico, riguarda la sfera personale dei membri dell'OdV, con particolare riferimento ai loro precedenti giudiziari. Sebbene non sia espressamente previsto dal D.lgs. 231/2001, tale requisito può essere desunto dalla logica del Decreto e dalla necessità di garantire la coerenza del sistema ed evitare contestazioni da parte dell'Autorità Giudiziaria. Per questo, è fondamentale che il Modello organizzativo preveda l'ineleggibilità nell'OdV di chi abbia riportato condanne penali definitive per i reati previsti dal D.lgs. 231/2001, indipendentemente dall'entità della pena, o per altri delitti dolosi con pene superiori a una soglia determinata. Si evidenzia che il D.lgs. 218/2012 (recante modifiche al Codice Antimafia di cui al D.lgs. 159/2011) ha esteso al Collegio sindacale e all'OdV l'obbligo di autocertificare l'assenza di misure di prevenzione antimafia, introducendo la prima codificazione legislativa del requisito di onorabilità.

Professionalità

L'OdV deve possedere un elevato livello di professionalità, combinando competenze tecniche e giuridiche per svolgere in modo efficace la propria funzione di controllo e prevenzione dei rischi-reato mappati nel Modello organizzativo adottato dall'ente, in conformità con il D.lgs. 231/2001.

L'OdV deve essere, quindi, un organismo altamente qualificato, in grado di assicurare lo svolgimento della funzione con la diligenza richiesta dalla natura dell'incarico.

A tal fine, esso deve essere capace di operare in modo autonomo, ma anche di interagire con le diverse

funzioni aziendali, assicurando un sistema di controllo efficace, che garantisca sia la prevenzione dei rischi sia la conformità alle normative di riferimento.

Poiché l'OdV può essere identificato con il Collegio sindacale, non vi sono ragioni per escludere la nomina di un sindaco all'interno dell'OdV. Anzi, la sua presenza in un organismo a composizione collegiale può favorire un migliore coordinamento e rafforzare i flussi informativi con il Collegio sindacale.

Continuità di azione

Per poter esercitare in modo corretto la funzione ad esso assegnata, l'OdV deve svolgere una costante attività di monitoraggio sul Modello. Dunque, con la locuzione "continuità d'azione" si vuole sottolineare la necessità che la vigilanza sul Modello non sia discontinua ma, al contrario, che sia svolta con una periodicità tale da consentire all'OdV di ravvisare in tempo reale eventuali situazioni anomale. Al fine di garantire l'effettività del Modello, l'OdV deve monitorare in modo costante la coerenza tra i comportamenti previsti nello stesso e le attività svolte in concreto dai suoi destinatari, svolgendo i propri compiti in modo sistematico (calendarizzazione delle attività, verbalizzazioni, flussi informativi, ecc.).

Compenso

Il compenso dei componenti dell'OdV è determinato dall'organo amministrativo o dall'assemblea all'atto della nomina per l'intero periodo di durata dell'incarico; esso è corrisposto al fine di remunerare la professionalità, l'esperienza e l'impegno richiesti dalla natura dell'incarico, anche in considerazione del rilievo della funzione.

La valutazione del compenso proposto e l'eventuale sua accettazione da parte dei componenti dell'OdV non possono prescindere dalla considerazione dei livelli di rischio e dalle responsabilità assunte dall'Organismo nell'assolvimento dell'incarico. A tal fine, rilevano i seguenti elementi:

- valutazione iniziale del rischio per l'adozione del Modello, in quanto più elevato è il pericolo di comportamenti illeciti, maggiori sono le potenziali responsabilità alle quali ciascun componente dell'OdV è esposto;
- complessità del Modello adottato, rilevabile dall'analisi di parametri quali la struttura organizzativa dell'ente, il numero di processi sensibili individuati, le aree e le funzioni coinvolte, le fattispecie di reato al cui rischio di commissione l'ente è esposto;
- livello dimensionale (es. fatturato, numero di dipendenti, attivo patrimoniale, capitale sociale) e organizzativo (es. esistenza di sedi diverse, anche all'estero) dell'azienda che conferisce l'incarico.

I componenti dell'OdV non accettano l'incarico, ove ritengano l'onorario non adeguato in relazione alle attività necessarie e alle modalità organizzative connesse alla funzione di vigilanza richiesta.

Si ritiene, inoltre, che in alcuni casi particolari debbano essere previste delle maggiorazioni del compenso ordinario alla luce del più elevato grado di "rischio 231" in cui versa l'azienda. Si pensi alle

ipotesi delineate dall'art. 12, co. 2, lett. b), ovvero dall'art. 17, co. 1, lett. b) del D.lgs. 231/2001: in entrambi i casi l'adozione del Modello da parte dell'ente avviene successivamente alla contestazione dell'illecito (*ex post*), ma prima dell'apertura del dibattimento di primo grado, al fine di ottenere rispettivamente la riduzione della sanzione pecuniaria da un terzo alla metà, ovvero la disapplicazione della sanzione interdittiva. Sembra logico ipotizzare che queste circostanze incidano sulla valutazione del compenso spettante ai componenti dell'OdV, stante il maggior grado di esposizione al rischio dell'ente il cui Modello è oggetto dell'attività di vigilanza. Appare opportuno che nella delibera di nomina si preveda, inoltre, la possibilità di un adeguamento del compenso inizialmente stabilito nel caso in cui aumenti il grado di complessità delle attività di vigilanza da svolgere, ad esempio in seguito ad un ampliamento del catalogo dei reati, a cambiamenti nell'assetto organizzativo dell'ente, ovvero ad una estensione delle attività svolte, con conseguente variazione dei profili di rischio.

La ripartizione del compenso fra i componenti dell'Organismo avviene sulla base di quanto stabilito all'atto della nomina, generalmente con una maggiorazione a favore del Presidente; si ritiene applicabile la normativa sull'equo compenso di cui alla L. 21 aprile 2023, n. 49.

1.4. Durata e cessazione dell'incarico

Durata

Per quanto riguarda la durata in carica dell'OdV, è preferibile la nomina per un periodo temporale determinato (ad esempio per tre anni); salvo che si verifichi una causa di cessazione anticipata, i membri dell'OdV rimangono in carica fino alla data della naturale scadenza.

In alternativa alla durata in anni, la nomina dell'OdV può essere riferita a un numero determinato di esercizi sociali, generalmente tre, con efficacia dalla data di insediamento fino all'approvazione del bilancio relativo all'ultimo dei tre esercizi.

Per evitare discontinuità temporale della funzione di vigilanza, il Modello dovrebbe prevedere l'applicabilità del regime di *prorogatio*, consentendo all'OdV uscente di restare in carica fino alla nomina del successivo, garantendo così il rispetto dei requisiti previsti dall'art. 6 del D.lgs. 231/2001 ai fini dell'esimente da responsabilità, seppur nell'ambito di un periodo limitato, la cui durata auspicabilmente dovrebbe essere prevista nel Modello.

Revoca e decadenza

La revoca dell'Organismo non è espressamente disciplinata; tuttavia, è possibile fare riferimento a diverse figure giuridiche e tipi contrattuali al fine di identificare le fattispecie che integrano la possibilità di revocare i membri dell'OdV.

Si deve in ogni caso ritenere che la revoca dell'Organismo e di ciascun componente competa all'organo amministrativo o all'assemblea, in caso di nomina assembleare.

Per ciò che concerne le cause di decadenza dalla funzione di componente dell'OdV, esse si configurano nel caso in cui un componente perda il possesso di uno dei requisiti precedentemente menzionati.

La decadenza è, quindi, generalmente legata al venir meno di uno tra i requisiti di autonomia, indipendenza, onorabilità e professionalità, oppure all'interdizione o inabilitazione, o a prolungate assenze non giustificate dalle riunioni. Il Modello organizzativo può includere specifiche cause di ineleggibilità, individuando espressamente l'organo amministrativo quale soggetto legittimato a dichiarare la decadenza, nonché le modalità del relativo accertamento.

Rinuncia

Il componente dell'OdV è libero di rinunciare in qualsiasi momento all'incarico, ad esempio mediante dimissioni volontarie. È opportuno che la rinuncia sia redatta in forma scritta ovvero risulti negli atti sociali, sia motivata e avvenga con un congruo preavviso. La comunicazione deve essere indirizzata con qualsiasi mezzo che consenta la certezza della ricezione da parte dell'organo amministrativo anche, ad esempio, attraverso la conferma da parte dei destinatari.

La rinuncia del componente dell'OdV ha effetto immediato. Nel caso in cui le dimissioni riguardino più membri, per stabilirne l'ordine di efficacia farà fede il momento nel quale esse sono state ricevute dall'ente.

In caso di rinuncia, l'organo amministrativo provvede tempestivamente a sostituire il membro dimissionario. Per garantire la continuità operativa dell'OdV in caso di cessazione dell'incarico di uno o più membri, il Modello organizzativo può prevedere anche la nomina di membri supplenti.

2. Attività di vigilanza: obiettivi e funzioni

2.1. Funzioni di vigilanza

Ai sensi dell'art. 6, co. 1, lett. b) - anche in combinato disposto con l'art. 7, co. 4, D.lgs. 231/2001 - all'Organismo di vigilanza spetta il compito di vigilare sul funzionamento e l'osservanza dei modelli e di curare il loro aggiornamento.

a) Per quanto riguarda le funzioni di vigilanza l'Organismo deve, in particolare:

- valutare, nel tempo, l'attualità, l'adeguatezza e la funzionalità del Modello, specialmente in relazione:
    - all'effettiva conformità alla natura, alle dimensioni, al sistema di amministrazione e controllo, alla struttura organizzativa (articolazione delle competenze e dei poteri gestori) e alla tipologia delle attività dell'ente;
    - all'individuazione delle attività a rischio reato (cd. mappatura dei rischi) e delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;
    - alla previsione di specifici protocolli diretti a programmare l'elaborazione e l'attuazione delle decisioni in relazione ai reati da prevenire;

- alla previsione di obblighi di informazione nei confronti dell'Organismo medesimo;
- alla previsione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
- all'attivazione e al funzionamento di adeguati canali di segnalazione interna;

- monitorare l'efficace attuazione del Modello, con riferimento all'effettività dei controlli, al rispetto dei protocolli di comportamento e delle misure in esso indicate, allo scambio dei flussi informativi, all'inserimento di apposite clausole nei contratti con i terzi e all'eventuale applicazione di sanzioni disciplinari nel caso di violazione da parte degli organi competenti;
- monitorare lo svolgimento di periodiche attività di formazione o informazione degli apicali e del personale aziendale e la relativa formalizzazione attraverso appositi documenti, promuovendo iniziative per la diffusione della conoscenza e della comprensione delle misure indicate nel Modello;
- invitare l'organo amministrativo ad avviare l'azione disciplinare a fronte di riscontrate violazioni del Modello da parte del personale aziendale o di terzi, ovvero esprimere il proprio parere ove interpellato dagli organi societari competenti all'irrogazione delle medesime sanzioni disciplinari.

Le funzioni di vigilanza, da pianificarsi e rendicontarsi periodicamente, si attuano principalmente mediante:

- analisi dei flussi informativi (periodici o ad evento);
- acquisizioni documentali;
- richieste di informazione o audizioni (periodiche o ad evento) del personale responsabile di attività a rischio o di funzioni di controllo (es. *compliance, audit*, ecc.);
- verifiche su singole operazioni o attività societarie;
- scambi informativi (periodici o ad evento) con l'organo amministrativo e con altri organi di controllo (es. Collegio Sindacale e Società di revisione) ovvero con il gestore delle segnalazioni interne.

b) Per quanto riguarda le funzioni di cura dell'aggiornamento del Modello, l'OdV deve, in particolare:

- segnalare all'organo amministrativo la necessità di apportare modifiche o aggiornamenti del Modello, eventualmente formulando anche proposte in merito, a fronte di:
  - significative violazioni delle relative prescrizioni da intendersi come quelle che, per qualità, gravità, modalità di commissione o reiterazione, a prescindere dall'applicazione di sanzioni disciplinari, evidenzino la necessità di apportare modifiche al Modello al fine di garantirne adeguatezza e/o funzionalità;
  - mutamenti nell'organizzazione o nell'attività che incidono su natura, tipologia o intensità

dei rischi-reato e/o sul funzionamento dei presidi di controllo (es. acquisizioni o trasformazioni societarie, fusioni per incorporazione, apertura di nuove aree di *business,* assunzione o dimissione di personale impiegato in attività a rischio e/o responsabile di funzioni di controllo, ecc.);

- mutamenti normativi, direttamente o indirettamente rilevanti ai sensi del D.lgs. 231/2001 (es. introduzione o modifica di reati-presupposto ovvero di normative di settore dagli stessi esplicitamente o implicitamente richiamati).

La cura dell'aggiornamento del Modello si attua attraverso:

- il costante monitoraggio della normativa;
- l'analisi delle risultanze delle attività di vigilanza;
- la motivata segnalazione all'organo amministrativo circa la necessità di apportare modifiche o aggiornamenti al Modello;
- la verifica dell'adeguatezza dell'aggiornamento del Modello prima della sua approvazione da parte dell'organo amministrativo;
- la verifica dello svolgimento di adeguata attività informativa e formativa al personale sulle modifiche e/o sugli aggiornamenti del Modello.

Quanto al perimetro applicativo di dette funzioni è importante rilevare come, essendo l'OdV privo di poteri impeditivi e di reazione, ad esso non possono essere attribuiti compiti operativi che inevitabilmente ne comprometterebbero l'indipendenza di giudizio.

Proprio per tale ragione deve essere evitata la prassi, purtroppo diffusa in molte realtà, di considerare l'OdV come un organo "onnicomprensivo" al quale rivolgersi per ogni esigenza di chiarimento o attività di verifica, incluse quelle di natura gestionale o organizzativa che non rientrano nei suoi compiti istituzionali. Un simile approccio, oltre a compromettere l'indipendenza e la neutralità di giudizio dell'OdV, rischierebbe di snaturarne la funzione primaria. È pertanto necessario ribadire che l'OdV non è titolare di poteri di indirizzo o di gestione, ma esclusivamente di funzioni di controllo, valutazione e segnalazione.

Ciò significa che, una volta individuata l'esistenza di violazioni del Modello, l'OdV dovrà limitarsi ad informare l'organo amministrativo affinché adotti le misure consequenziali. Il perimetro delle funzioni dell'OdV è, infatti, rigorosamente limitato alla vigilanza sul Modello organizzativo adottato ai sensi del D.lgs. 231/2001, essendo escluse dal suo ambito operativo eventuali attività di monitoraggio su qualsiasi ulteriore elemento del sistema di controllo interno dell'ente.

Nel caso in cui fossero necessarie specifiche professionalità in relazione alla materia oggetto del controllo, che non si riscontrino all'interno dell'OdV (es. perché il catalogo dei reati si è ampliato e le nuove fattispecie delittuose riguardano ambiti differenti rispetto a quelli in precedenza mappati), è possibile ricorrere ad un consulente specializzato a valere sul budget dell'OdV.

2.2. Attività di vigilanza: obiettivi e funzioni

L'attività di verifica, quale strumento operativo della funzione di vigilanza affidata all'OdV, si configura come una leva fondamentale nell'attuazione delle funzioni istituzionali affidate all'OdV. Essa contribuisce ad istituire un presidio sistemico – e non meramente formale – volto a garantire l'effettiva attuazione, la costante adeguatezza e l'idoneità del Modello, in una prospettiva di prevenzione integrata della responsabilità dell'ente.

Tali attività assolvono una funzione tripartita: preventiva, diagnostica e correttiva. Sotto il profilo preventivo, esse mirano ad anticipare eventuali disfunzioni organizzative e a mitigare l'esposizione ai rischi-reato; in chiave diagnostica, consentono di rilevare deviazioni operative, scostamenti procedurali e criticità strutturali rispetto alle disposizioni del Modello; in ottica correttiva, rappresentano un'occasione per proporre misure migliorative, sia sul piano delle procedure interne che della cultura organizzativa.

In tale contesto, l'OdV: *i*) esercita un controllo costante sul grado di conformità dei comportamenti aziendali alle prescrizioni del Modello, *ii*) monitora l'efficacia dei controlli interni in relazione alle aree di rischio identificate e *iii*) propone soluzioni tecniche e organizzative per la revisione del sistema dei presidi. Centrale è anche la funzione di tracciabilità: ogni attività deve poter essere ricostruita *ex post* in un'ottica di *accountability* sostanziale, a garanzia della trasparenza e della difendibilità delle scelte adottate.

La vigilanza dell'OdV si sviluppa, altresì, secondo il principio di continuità, che si esplica attraverso la regolare pianificazione delle riunioni, lo svolgimento sistematico di verifiche documentali e "sul campo", il dialogo con le funzioni aziendali a rischio e l'analisi critica dei flussi informativi ricevuti. Tale approccio è ulteriormente potenziato da una lettura proporzionale dell'intensità dei controlli, calibrata in base alla complessità dell'organizzazione, alla sensibilità dei processi gestionali e al quadro normativo e giurisprudenziale di riferimento.

L'efficacia del sistema di vigilanza risiede, infine, nel rispetto di principi fondanti quali l'autonomia, l'indipendenza e la competenza tecnica dell'OdV. La produzione e conservazione ordinata delle evidenze documentali – resa possibile attraverso la verbalizzazione delle riunioni e la protocollazione delle attività – rappresenta una condizione imprescindibile per l'effettività della funzione di controllo e per la sua successiva valorizzazione, anche in sede giudiziaria.

Si evidenzia che nelle realtà più complesse alcune attività di vigilanza sono affidate a una funzione interna e indipendente (internal audit) o anche a consulenti esterni, laddove necessario e/o opportuno.

2.2.1. Pianificazione delle attività di verifica

La pianificazione delle attività di verifica costituisce il fulcro metodologico attraverso cui l'OdV esercita la propria funzione di controllo in modo sistematico, proporzionato e documentabile. Essa consente di assicurare la continuità e la coerenza dell'azione di vigilanza con i principi di autonomia, indipendenza

e professionalità sanciti dal D.lgs. 231/2001 e dal Modello 231. Il processo di pianificazione, in tale prospettiva, assume natura strategica, poiché definisce *ex ante* l'insieme delle attività di presidio, le relative priorità, le modalità di attuazione e gli strumenti di verifica, garantendo che l'azione dell'OdV non si riduca a un controllo episodico, ma si configuri come un presidio strutturale e permanente di legalità aziendale.

Il piano delle verifiche è elaborato annualmente o - più raramente - su base pluriennale, in coerenza con la mappatura dei rischi-reato e con l'evoluzione organizzativa dell'ente. Nella sua predisposizione, l'OdV tiene conto dei risultati delle attività pregresse, delle eventuali non conformità rilevate, delle segnalazioni ricevute, nonché delle modifiche normative o procedurali che incidono sul perimetro dei rischi. Tale impostazione dinamica garantisce che la vigilanza si mantenga aderente al contesto operativo e all'effettivo profilo di rischio dell'organizzazione, in linea con i principi di proporzionalità e di adeguatezza propri del sistema 231.

L'attività di pianificazione si sviluppa in più fasi. In primo luogo, l'OdV individua le aree e i processi oggetto di verifica, selezionandoli sulla base di criteri di priorità che tengono conto della gravità potenziale dei reati presupposto, della frequenza e dell'impatto dei processi, nonché del grado di maturità dei presìdi interni di controllo. Successivamente, vengono definiti gli obiettivi specifici di ciascun intervento, le modalità operative (analisi documentale, colloqui, controlli a campione, accessi diretti), la periodicità e le responsabilità esecutive. L'approvazione del piano da parte dell'OdV avviene in seduta collegiale, previa discussione dei criteri adottati e formalizzazione nel verbale di riunione, a garanzia della tracciabilità decisionale.

Il piano delle verifiche si accompagna a un calendario operativo delle riunioni, articolato in sessioni ordinarie e straordinarie (vd. § 2.2.2). Le prime assicurano il monitoraggio sistematico dello stato di attuazione del Modello 231 e dei flussi informativi; le seconde sono attivate in presenza di eventi anomali, segnalazioni rilevanti o modifiche organizzative di impatto significativo. Tale doppio livello di pianificazione - strategica e operativa - permette di mantenere un equilibrio tra controllo preventivo e capacità reattiva, elementi entrambi essenziali per un sistema di vigilanza effettivo.

Elemento qualificante della pianificazione è la previsione di momenti di riesame periodico, finalizzati a valutare l'attuazione delle verifiche, la coerenza dei risultati con gli obiettivi fissati e la necessità di eventuali rimodulazioni. In tale fase, l'OdV procede anche all'analisi comparativa tra le attività programmate e quelle effettivamente realizzate, individuando le cause di eventuali scostamenti e adottando misure correttive per migliorare l'efficacia complessiva del sistema di vigilanza. Ogni aggiornamento del piano viene formalizzato mediante delibera e comunicato agli organi sociali di riferimento.

La pianificazione delle verifiche non si esaurisce nella dimensione procedurale, ma rappresenta uno strumento di indirizzo culturale e gestionale in grado di orientare le funzioni aziendali verso una maggiore consapevolezza dei rischi di reato e promuovere un approccio preventivo fondato su trasparenza, tracciabilità e responsabilità diffusa. L'adozione di criteri di selezione documentati, l'utilizzo di check-list standardizzate, l'integrazione con gli strumenti digitali di compliance

management e la conservazione ordinata delle evidenze rafforzano il valore probatorio delle attività svolte e la loro difendibilità in sede ispettiva o giudiziaria.

In tale cornice, la pianificazione dell'OdV assume il significato di presidio metodologico del Modello 231, funzionale a garantire non solo la regolarità dei controlli, ma anche la loro effettiva capacità di prevenire, individuare e correggere tempestivamente comportamenti a rischio. Essa rappresenta, in ultima analisi, l'asse portante di un sistema di vigilanza che traduce la compliance normativa in pratica organizzativa, integrando la prevenzione della responsabilità penale dell'ente con una gestione consapevole e proattiva dei rischi.

2.2.2. Tipologie di riunioni

L'architettura delle riunioni dell'OdV costituisce un elemento cardine per l'attuazione efficace della funzione di vigilanza. Esse devono rispondere a logiche di proporzionalità, tempestività e rilevanza strategica, in relazione alla finalità perseguita e alla natura dei soggetti coinvolti.

Le principali tipologie di riunioni possono essere così articolate:

a) Riunioni interne dell'OdV

Si tratta di incontri riservati ai soli membri dell'Organismo e dedicati alla valutazione delle evidenze acquisite, alla calibrazione del piano delle verifiche, alla discussione dei casi emersi e all'elaborazione delle eventuali proposte correttive. Tali riunioni, quindi, costituiscono il momento di sintesi e riflessione critica dell'attività di vigilanza; in tal senso, è buona prassi includere l'analisi comparata tra quanto pianificato e quanto effettivamente realizzato, anche ai fini del miglioramento continuo.

b) Riunioni con le funzioni aziendali

Sono incontri con i responsabili delle unità organizzative coinvolte nei processi aziendali a rischio reato, finalizzati all'approfondimento di specifici aspetti operativi, all'analisi dei flussi informativi e alla verifica dell'allineamento tra le procedure applicate e quanto previsto dal Modello. Possono essere calendarizzate (pianificazione ordinaria) oppure attivate in via straordinaria, a fronte di segnali di criticità o eventi anomali. Tali momenti rappresentano anche un'opportunità per promuovere una cultura della prevenzione e responsabilizzazione diffusa.

c) Riunioni con gli organi societari (CdA, Collegio Sindacale, Revisore legale)

Questi incontri rispondono all'esigenza di consolidare un sistema di governance integrata e multilivello. L'OdV presenta relazioni periodiche sulle attività svolte, proponendo – ove necessario – correttivi organizzativi, aggiornamenti al Modello o interventi disciplinari. Il dialogo con tali organi deve essere strutturato e costante, al fine di garantire una circolazione efficace delle informazioni e una coerente gestione dei rischi-reato a livello apicale.

d) Riunioni con consulenti esterni o soggetti terzi

In talune circostanze, la complessità tecnica delle verifiche richiede il coinvolgimento di esperti qualificati esterni (ad es. per tematiche ambientali, informatiche, giuslavoristiche). Le riunioni con tali

soggetti devono essere formalizzate e finalizzate alla produzione di report tecnici o alla definizione condivisa di azioni correttive. Il loro apporto si integra con la funzione valutativa dell'OdV in una prospettiva di specializzazione e rigore metodologico.

e) Riunioni ad hoc

Convocate a fronte di eventi straordinari – quali procedimenti penali, gravi inadempimenti, segnalazioni *whistleblowing* significative in ambito 231 o incidenti critici – queste riunioni sono orientate alla tempestiva presa d'atto dell'accaduto, all'analisi degli impatti potenziali e alla definizione di misure immediate di contenimento. Esse costituiscono un presidio reattivo e strategico volto a rafforzare la resilienza organizzativa del sistema 231.

2.2.3. Modalità operative delle riunioni

L'efficacia delle riunioni dell'OdV dipende anche dalla definizione di modalità operative chiare e coerenti con i principi di tracciabilità, trasparenza, riservatezza e verificabilità. Tali modalità rappresentano non soltanto uno strumento organizzativo, ma anche una garanzia metodologica dell'idoneità delle attività di vigilanza a produrre valore probatorio e difensivo, in conformità con il principio dell'evidenza documentale.

In quest'ottica, è opportuno che l'OdV disciplini tali attività mediante un Regolamento interno che ne definisca le modalità attuative, la frequenza, le responsabilità e i criteri di selezione degli ambiti di verifica. Tale regolamentazione rafforza la continuità dell'azione di controllo e ne garantisce la coerenza con la mappatura dei rischi e il piano di attività dell'Organismo. È buona prassi che Il Regolamento sia oggetto di informativa da parte dell'OdV e di mera presa d'atto da parte dell'organo amministrativo.

La convocazione delle riunioni deve avvenire secondo tempistiche e procedure definite dal Regolamento dell'OdV e può essere disposta dal Presidente o da altro componente delegato, anche su sollecitazione delle funzioni aziendali o degli organi sociali. È preferibile che la convocazione sia accompagnata dall'ordine del giorno, predisposto dal Presidente, al fine di assicurare un confronto mirato e consapevole.

Durante la riunione il coordinamento spetta al Presidente dell'OdV o, in sua assenza, al componente individuato nel Regolamento dell'OdV, tipicamente il membro più anziano, e la conduzione deve rispettare criteri di sintesi, completezza e oggettività. Il dibattito deve consentire l'emersione delle diverse posizioni e la formalizzazione delle decisioni assunte. È opportuno che il segretario dell'OdV o un componente delegato provveda alla redazione del verbale, il quale deve contenere almeno: data, orario e luogo della riunione, nominativi dei presenti e degli assenti, ordine del giorno, sintesi delle posizioni espresse, decisioni adottate, azioni previste e soggetti responsabili dell'attuazione, dettaglio dei punti aperti dalle precedenti verifiche (con relativo *follow up*), calendario delle verifiche e stato delle stesse, aggiornamenti normativi, variazioni organizzative intervenute, segnalazioni *whistelblowing*, stato del piano di audit.

Il verbale riveste un valore essenziale ai fini della prova dell'effettività dell'azione di vigilanza. Esso deve essere redatto in modo chiaro, coerente, completo e inalterabile e deve essere approvato mediante apposita sottoscrizione. A fini di trasparenza e controllo, è raccomandabile l'adozione di un libro delle riunioni numerato progressivamente e gestito in modalità conforme ai requisiti di integrità e conservazione previsti dalla normativa vigente e dalle *best practice* di settore. La preventiva vidimazione, sebbene non obbligatoria, può essere eventualmente valutata come buona prassi di controllo.

La gestione dei verbali e della documentazione a supporto deve prevedere la conservazione in un archivio sicuro, accessibile solo ai soggetti autorizzati e conforme alle disposizioni in materia di protezione dei dati personali e di sicurezza informatica. Il set documentale prodotto – composto da verbali, relazioni, materiali condivisi, corrispondenza e ogni altro elemento rilevante – costituisce un presidio fondamentale non solo per la continuità operativa dell'OdV, ma anche per la sua funzione difensiva nell'ambito di eventuali procedimenti giurisdizionali.

La verbalizzazione rileva anche quale strumento di sintesi delle attività svolte e di raccordo tra i membri dell'OdV e tra l'OdV e gli organi dell'ente. In tale prospettiva, si sottolinea l'opportunità di una verbalizzazione che documenti, con rigore, anche le eventuali divergenze emerse in sede di riunione, le astensioni motivate e le osservazioni dei partecipanti.

I verbali redatti dall'Organismo di vigilanza costituiscono documentazione interna e riservata, destinata a comprovare l'attività svolta. È opportuno che essi siano trasmessi all'organo amministrativo esclusivamente per le parti che richiedano specifici interventi o determinazioni da parte di quest'ultimo. Non appare invece opportuno trasmettere i verbali ad altri soggetti, quali il Collegio sindacale, la Società di revisione o consulenti esterni (ad esempio, in caso di indagini, perizie, svolgimento di *due diligence* per operazioni societarie), anche in presenza di eventuali richieste, al fine di preservare la riservatezza delle attività di vigilanza. A tale esigenza di informazione verso gli altri organi societari e i soggetti sopra indicati provvede la relazione periodica dell'Organismo di vigilanza, che costituisce il documento riepilogativo dell'attività svolta e il canale formale di comunicazione previsto dal Modello di organizzazione, gestione e controllo. Resta salva la possibilità di trasmettere i verbali, o parti di essi, laddove vi sia una richiesta debitamente motivata – da parte dei soggetti menzionati – di approfondimento/maggiore *disclosure* e previa comunicazione immediata all'OdV.

2.2.4. Attività di verifica dell'OdV

L'attività di verifica rappresenta il principale strumento attraverso cui l'OdV accerta, con metodo autonomo e sistematico, la tenuta del sistema dei controlli interni e la conformità dell'operato aziendale al Modello 231. Essa si affianca e si integra con i flussi informativi ricevuti dalle funzioni aziendali, configurandosi come una forma di controllo diretto, potenzialmente anche ispettivo, finalizzato a rilevare carenze procedurali, inadempienze organizzative e rischi latenti.

Senza pretesa di esaustività, rientrano tra le modalità attuative delle verifiche: *i*) l'analisi di documentazione amministrativa, gestionale e tecnica; *ii*) l'effettuazione di interviste e colloqui con i

referenti delle aree a rischio; *iii*) l'esame di report operativi e gestionali (e della relativa documentazione di supporto); *iv*) la somministrazione di questionari; *v*) la verifica sul campo di specifiche attività o processi; *vi*) la disamina delle relazioni che altre funzioni di controllo debbano rendere all'organo di governo (ad es: risk management, compliance, internal audit, ecc.).

In funzione della complessità dell'ente, del livello di rischio rilevato e delle risorse disponibili, l'OdV può avvalersi – quando necessario – della funzione di internal audit e/o di consulenti o professionisti esterni per svolgere accertamenti di natura specialistica, in particolare su ambiti tecnici, informatici o ambientali. Tali soggetti agiscono sotto il coordinamento dell'OdV che mantiene la piena titolarità delle attività svolte e dell'elaborazione delle risultanze.

L'esperienza applicativa mostra l'utilità di affiancare ai flussi informativi "passivi" una strategia di verifica "attiva", ad esempio mediante controlli a campione, anche a sorpresa e non programmati, mirati su procedure o atti di particolare rilevanza. Tale approccio consente di testare la tenuta del sistema di prevenzione in condizioni operative reali, offrendo un riscontro puntuale sull'efficacia e sull'effettiva attuazione del Modello.

Affinché tali attività siano efficaci e valorizzabili anche in un'eventuale prospettiva giudiziaria, esse devono essere accuratamente pianificate, documentate e archiviate. L'OdV, pertanto, è tenuto a predisporre un set informativo di supporto, comprensivo di piani di verifica, evidenze raccolte, verbali di colloquio, check-list adottate, conclusioni formulate e – ove del caso – raccomandazioni o richieste di adeguamento rivolte alle funzioni aziendali coinvolte.

Le verifiche condotte devono altresì confluire in una relazione informativa periodica, redatta secondo la cadenza stabilita nel Regolamento e/o nel Modello, destinata agli organi apicali dell'ente, ivi inclusi gli organi di controllo, con l'obiettivo di favorire una piena integrazione tra la funzione di vigilanza e il sistema complessivo di governance.

Tale approccio rafforza la funzione dell'OdV quale presidio di secondo o terzo livello, contribuendo alla costruzione di un sistema di controllo multilivello, dinamico e coerente con le finalità del D.lgs. 231/2001.

3. Flussi informativi

3.1. Flussi informativi verso l'OdV

L'art. 6, co. 2, lett. d) del D.lgs. 231/2001 dispone che i Modelli 231 prevedano "*obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli*". Il Decreto e la Relazione di accompagnamento non forniscono ulteriori disposizioni specifiche in tema di flussi informativi; nondimeno, gli stessi possono essere considerati uno dei principali strumenti di riscontro sull'adeguatezza e l'efficace attuazione del Modelli 231 e rappresentano, pertanto, un elemento essenziale per il corretto funzionamento dell'OdV.

In sintesi, un sistema di flussi informativi ben strutturato deve consentire all'OdV di:

- verificare l'efficace attuazione del Modello;
- rilevare tempestivamente situazioni di rischio o possibili violazioni del Modello;
- svolgere in maniera più efficiente la propria attività di vigilanza anche al fine di pianificare controlli mirati su ambiti maggiormente a rischio;
- assicurare la tracciabilità delle informazioni per tutelare l'ente in caso di accertamenti da parte dell'Autorità giudiziaria.

Per un effettivo espletamento dei compiti e delle funzioni attribuitegli, l'OdV ha accesso a tutte le informazioni e alla documentazione aziendale funzionali all'espletamento dell'incarico. Tali dati e informazioni sono trattati nel rispetto di quanto stabilito dalla normativa in materia di protezione dei dati personali. L'omissione degli obblighi di informazione verso l'OdV deve essere considerata all'interno del Modello 231 quale inadempimento alle obbligazioni derivanti dal rapporto di lavoro ai sensi dell'art. 2104 c.c. e dell'art. 2106 c.c. e, pertanto, sanzionabile in via disciplinare.

3.1.1. Tipologie di flussi informativi

I flussi informativi possono essere distinti in:

- periodici: flussi informativi da inviare all'OdV entro una determinata scadenza;
- ad evento: flussi informativi che avvengono al verificarsi di un determinato evento, che è necessario segnalare tempestivamente all'OdV.

Frequenza, contenuti essenziali, canali e responsabilità di invio sono definiti in coerenza con l'assetto organizzativo e con la mappatura dei rischi-reato, nel rispetto dei principi di proporzionalità, riservatezza e tracciabilità; l'OdV può richiedere integrazioni motivate.

A) Flussi informativi periodici

Si tratta di informazioni trasmesse all'OdV con una determinata periodicità (ad esempio trimestrale, semestrale o annuale in considerazione delle specifiche esigenze dell'OdV riferite alle peculiarità organizzative dell'ente) dalle funzioni aziendali, che consentono all'OdV di monitorare l'efficace attuazione del Modello 231 e di individuare eventuali aree di miglioramento. La loro configurazione dipende dalle specificità dell'ente, come le dimensioni o il business in cui opera.

Le principali fonti di provenienza di tali flussi possono essere:

- funzioni che operano in processi ritenuti a rischio reato 231 (a titolo esemplificativo: HR, procurement, IT, finance, ecc.);
- funzioni di controllo (internal audit, compliance, risk management, ecc.);
- organi sociali;

- altri interlocutori (ad esempio, consulenti esterni strutturati).

Di seguito si forniscono alcune esemplificazioni di flussi informativi periodici suddivisi per aree, fermo restando che gli stessi sono conseguenti anche a valutazioni in merito alle caratteristiche dimensionali e di business dell'ente.

In ambito sicurezza (si veda anche il § 5.5), viene trasmesso annualmente il piano di formazione del personale in materia di salute e sicurezza sul lavoro, unitamente al consuntivo della formazione erogata nell'anno precedente nonché la relazione *ex* art. 35 del D.lgs. 81/2008 (Testo Unico Sicurezza).

Con riferimento alla funzione HR, con periodicità da definirsi, deve essere predisposto un report sui provvedimenti disciplinari adottati nei confronti dei dipendenti, specificando sanzioni irrogate, archiviazioni e relative motivazioni. Analogamente, sul versante della formazione, l'OdV riceve un resoconto periodico delle attività di formazione erogate al personale in materia di D.lgs. 231/2001.

Per l'area *finance*, con la medesima cadenza annuale, l'OdV riceve copia del fascicolo di bilancio, così da poter valutare eventuali profili critici per la vigilanza di competenza.

Nell'area dei sistemi certificati, l'Organismo deve essere informato periodicamente attraverso report predisposti dall'Organismo di Certificazione circa lo stato dei sistemi di gestione aziendale certificati. Ancora, l'area legale deve inviare con una cadenza periodica definita un elenco dei contenziosi attivi e passivi, comprensivo di quelli chiusi nel periodo di riferimento, in modo da consentire all'OdV di monitorare il contenzioso legale dell'ente e i rischi correlati.

Con cadenza periodica, l'OdV riceve un report di sintesi sul presidio 231 nell'area acquisti, proporzionato alle dimensioni e al rischio dell'ente, che includa almeno: (*i*) deroghe o eccezioni alle procedure di approvvigionamento, (*ii*) gli affidamenti diretti o di urgenza sopra la soglia interna, (*iii*) le variazioni contrattuali rilevanti (per importo e/o oggetto) ed eventuali frazionamenti di fornitura atipici, (*iv*) l'uso di intermediari e/o consulenti in ambiti sensibili o nuovi rispetto agli esistenti, (*v*) le eventuali controversie o rilievi ispettivi o segnalazioni attinenti al processo di acquisto, (*vi*) i fornitori per i quali sia intervenuta una variazione negli Iban di appoggio e (*vi*), per gli enti che partecipano a gare pubbliche, una sintesi delle principali procedure e dei relativi esiti.

Per quanto concerne l'ambito delle autorizzazioni, deve essere previsto un flusso periodico che descriva le richieste di autorizzazioni, licenze, concessioni o provvedimenti amministrativi necessari per l'esercizio delle attività aziendali, con indicazione degli esiti conseguiti.

L'area internal audit, compliance e risk management, a sua volta, contribuisce periodicamente con report di follow up sugli audit effettuati su processi a rischio reato 231, evidenziando i rilievi e le azioni correttive intraprese.

Per la funzione marketing, sempre con periodicità da definirsi, l'OdV riceve un rendiconto riepilogativo delle sponsorizzazioni, donazioni e omaggi concessi, così da monitorarne la conformità rispetto al Modello 231.

In aggiunta, nell'ambito dei progetti finanziati, l'Organismo riceve periodicamente un elenco tabellare

dei soggetti erogatori, dell'oggetto dei contributi o sovvenzioni e delle erogazioni ricevute, oltre a un report sullo stato di avanzamento dei progetti di innovazione sostenuti da fondi di terzi.

Sul fronte IT, l'OdV può richiedere un report periodico sugli accessi dei dipendenti al Modello 231, qualora ad esempio pubblicato su intranet aziendale, utile per valutare il livello di utilizzo e conoscenza dello strumento.

Infine, con riferimento al *whistleblowing*, l'Organismo riceve con la periodicità valutata opportuna (tipicamente la cadenza potrebbe essere annuale o semestrale, ma nulla vieta una maggiore frequenza) un'informativa relativa a tutte le segnalazioni pervenute, anche nel caso in cui la loro istruttoria non sia di diretta competenza dell'OdV stesso.

B) Flussi informativi ad evento

Si tratta di informazioni che devono essere trasmesse tempestivamente all'OdV in caso di potenziali criticità o eventi specifici che potrebbero sfociare nella realizzazione di un reato presupposto *ex* D.lgs. 231/2001.

Di seguito si forniscono alcune esemplificazioni di flussi informativi ad evento suddivisi per area.

In primo luogo, nell'ambito della sicurezza sul lavoro, devono essere comunicati all'OdV gli infortuni con prognosi iniziale superiore a quaranta giorni, nonché gli infortuni mortali che coinvolgano dipendenti, personale somministrato o personale di imprese appaltatrici. Nondimeno, appare opportuna anche la segnalazione di infortuni di minore gravità o dei *near miss* utili ai fini dell'identificazione di eventuali criticità.

Parimenti, rientrano tra gli eventi rilevanti le eventuali modifiche, conferimenti o revoche di deleghe e sub-deleghe *ex* art. 16 del D.lgs. 81/2008, così come le visite ispettive e le prescrizioni impartite dagli organi di vigilanza pubblici competenti in materia di sicurezza (A.S.L., Ispettorato del Lavoro, Pubblica Amministrazione o Polizia Giudiziaria).

Sul versante *finance*, devono essere prontamente trasmesse le comunicazioni relative a visite, ispezioni e accertamenti avviati dagli enti preposti (quali Agenzia delle Entrate, Guardia di Finanza e ogni altra Autorità di vigilanza) e, all'esito, gli eventuali rilievi o sanzioni comminate.

Con riguardo all'area HR, è oggetto di flusso informativo l'aggiornamento o la variazione del Codice disciplinare aziendale.

Analogamente, sotto il profilo organizzativo, devono essere comunicati i cambiamenti e gli aggiornamenti dell'organigramma societario.

Nell'ambito dei sistemi certificati, l'OdV deve essere informato di ogni sospensione delle certificazioni rilasciate dagli Organismi di certificazione, nonché delle relative cause.

Per quanto riguarda il profilo societario, è necessario trasmettere estratti dei verbali dell'organo amministrativo qualora affrontino specifiche tematiche connesse al D.lgs. 231/2001, oltre alle modifiche riguardanti la compagine sociale, la proprietà e la composizione degli organi sociali (CdA,

Collegio sindacale).

Sul piano legale, devono essere segnalati i provvedimenti o le notizie provenienti da autorità giudiziarie, di polizia giudiziaria o altre autorità competenti, dai quali si evinca lo svolgimento di indagini – anche nei confronti di ignoti – in relazione ad ipotesi di reato rilevanti ai sensi del D.lgs. 231/2001 anche se riferibili a persone fisiche, ma potenzialmente incidenti sull'ente.

Dal punto di vista dell'internal audit, compliance e risk management, devono essere trasmessi all'OdV i report relativi ai processi a rischio reato 231, nonché il Piano di Audit approvato dall'organo amministrativo.

In ambito IT, l'OdV deve ricevere informazioni su eventi significativi connessi all'andamento delle attività rispetto alle fattispecie di reato considerate dal Modello 231, ivi compresi *data breach*, segnalazioni al Garante della Privacy e, più in generale, i risultati dei test operati in applicazione delle normative vigenti (ad esempio normativa Nis2 e Dora).

Infine, nell'area *whistleblowing*, devono essere comunicate le segnalazioni ricevute che siano rilevanti ai sensi della normativa 231 (vd. par. 4.4).

3.1.2. Modalità di comunicazione dei flussi informativi verso l'OdV

Al fine di agevolare i flussi informativi previsti dal Modello e rafforzare l'efficacia del proprio sistema di vigilanza, l'OdV deve richiedere, ove non abbia ricevuto in tal senso comunicazione all'atto della nomina, all'organo amministrativo l'attivazione di una casella di posta elettronica dedicata, che può essere istituita sia come indirizzo di posta elettronica ordinaria sia come casella di posta elettronica certificata. La scelta tra le due soluzioni dipende dalle esigenze organizzative e dal livello di formalizzazione che l'ente intende assicurare alle comunicazioni: l'utilizzo della posta ordinaria può risultare più agile nella gestione quotidiana dei flussi informativi, mentre la PEC garantisce una maggiore certezza della trasmissione e della ricezione dei messaggi, oltre a un valore probatorio superiore. In ogni caso, è fondamentale che la casella sia accessibile esclusivamente ai componenti dell'OdV, o a soggetti appositamente delegati dallo stesso, e che siano adottate misure idonee a garantire la riservatezza e la tracciabilità delle comunicazioni ricevute.

È inoltre opportuno che l'OdV adotti una specifica procedura che regolamenti la gestione dei flussi informativi. In particolare, per il buon esito dell'informativa, occorre definire:

- il responsabile del flusso;
- il contenuto del flusso;
- la modalità di invio del flusso;
- la tempistica dell'invio del flusso.

La procedura dovrà essere adattata alla struttura organizzativa dell'ente; pertanto, è opportuno che l'OdV analizzi le aree e i processi sensibili e identifichi le funzioni aziendali a rischio reato a cui – tra gli altri – dovrà essere rivolto l'obbligo di trasmissione dei flussi. La procedura può altresì prevedere che i

flussi informativi possano essere rappresentati dal responsabile della trasmissione con specifica relazione o rappresentati all'OdV nel caso di convocazione in una specifica riunione.

Occorre tenere presente che l'elencazione dei flussi, per quanto esaustiva e accurata, non può prevedere tutti quei flussi ad evento, di carattere eccezionale, ritenuti idonei ad integrare un rischio reato o altra notizia rilevante secondo la discrezionalità del soggetto responsabile del flusso. Per tale motivazione, occorre prevedere all'interno del Modello 231 l'obbligo di informazione all'OdV per tutti i dipendenti che vengano a conoscenza di notizie relative a comportamenti non in linea con quanto previsto dal Modello 231 e dal Codice Etico adottati dall'ente.

La procedura può, altresì, prevedere la trasmissione all'OdV, su base periodica, di una specifica scheda di autocertificazione da parte dei responsabili dei flussi che attesti il rispetto, nell'ambito dei processi sensibili da questi gestiti, delle regole previste dal Modello 231 e segnali eventuali eccezioni o situazioni che richiedono un aggiornamento del medesimo.

È opportuno che la procedura, una volta approvata dall'OdV, venga trasmessa all'organo amministrativo dell'ente con richiesta di diffonderla ai diretti riporti, responsabili dei flussi informativi; per una maggiore diffusione, l'OdV può altresì richiedere all'ente che la stessa venga resa disponibile nel *repository* aziendale delle procedure.

3.2. Flussi informativi dall'OdV

Un'efficace architettura dei flussi informativi richiede che, in aggiunta ai flussi dalle strutture aziendali competenti nei confronti dell'OdV, siano previsti altresì flussi da quest'ultimo verso l'organo amministrativo e gli organi di controllo.

I flussi "in uscita" dall'OdV contribuiscono alla regolare attuazione del sistema di controllo interno e di gestione dei rischi e permettono al vertice, responsabile dell'adeguatezza del sistema di controllo interno di gestione dei rischi e del sistema organizzativo, di effettuare un monitoraggio sull'attività svolta dall'Organismo con riferimento al funzionamento e all'osservanza del Modello 231 e al suo costante aggiornamento.

3.2.1. Tipologie di flussi informativi

I flussi informativi dall'OdV possono essere continuativi, periodici e ad evento.

Flussi continuativi

L'Organismo deve mantenere uno scambio informativo continuativo con:

- il vertice aziendale, in particolare con riferimento alle occasioni in cui sia necessario l'aggiornamento del Modello 231 per il sopravvenire di novità normative, giurisprudenziali e/o dottrinali di rilievo;
- il Collegio sindacale;
- il Comitato controllo e rischi (e sostenibilità), in caso di società quotata;

- la Società di revisione e/o il Revisore legale;
- il Responsabile della prevenzione della corruzione e della trasparenza, in caso di società a partecipazione pubblica;
- il Responsabile della funzione antiriciclaggio, in caso di ente destinatario degli obblighi di cui al D.lgs. 21 novembre 2007, n. 231.

Flussi periodici

L'Organismo deve riferire periodicamente all'organo amministrativo e agli organi di controllo dell'ente sulle attività svolte per far fronte ai doveri derivanti dal D.lgs. 231/2001.

Potrebbe essere utile prevedere, per questo tipo di flussi, riunioni congiunte con il Collegio sindacale e il Comitato controllo e rischi (e Ssostenibilità) e, più in generale, con il Comitato per il controllo interno e la revisione legale di cui alla direttiva 2006/43/CE (nel caso di Enti di Interesse Pubblico - EIP), anche al fine di consentire agli organi di controllo di chiedere approfondimenti all'Organismo di vigilanza e di condividere, nel rispetto delle reciproche prerogative e responsabilità, ulteriori temi di interesse comune, quali, a titolo esemplificativo, l'esame di interventi di audit o di documenti normativi interni in materia di governance e di sistema di controllo.

Flussi ad evento

Si tratta di flussi dall'Organismo di vigilanza all'organo amministrativo da attivarsi qualora si verifichino fatti di particolare significatività per l'attuazione del "sistema 231" dell'ente.

In particolare, tali flussi possono essere determinati da:

i. emersione, nel corso dello svolgimento delle attività di vigilanza, di criticità rilevanti nell'attuazione del Modello 231, incluse violazioni gravi e/o reiterate del Modello o del Codice Etico di cui l'Organismo potrebbe venire a conoscenza mediante attività di audit, ovvero segnalazioni aventi rilevanza in materia di responsabilità amministrativa di impresa, ovvero flussi provenienti da altre strutture aziendali competenti, per esempio in ipotesi di procedimenti disciplinari per violazioni del Modello 231 e/o del Codice etico dell'ente;

ii. inadempimento delle strutture aziendali tenute a informative nei confronti dell'Organismo di vigilanza: compito dell'OdV in questo caso è segnalare l'inadempimento all'organo gestorio, proponendo le misure ritenute opportune (es. richiami, correttivi organizzativi, attivazione delle funzioni competenti).

3.2.2. Modalità di comunicazione dei flussi informativi dall'OdV

Come anticipato, l'Organismo di vigilanza deve predisporre una relazione periodica per iscritto all'organo amministrativo. La Relazione, redatta su base annuale o semestrale, deve essere altresì trasmessa, per opportuna conoscenza, anche agli organi di controllo.

Quanto al contenuto, l'attività di reporting dell'OdV si sviluppa lungo diverse direttrici, ciascuna delle

quali risponde all'esigenza di assicurare una vigilanza effettiva e completa sul funzionamento e sull'aggiornamento del Modello 231.

In primo luogo, particolare rilievo assume la rendicontazione delle riunioni svolte nel periodo di riferimento. L'OdV fornisce puntuale indicazione del numero complessivo di incontri tenuti, delle rispettive date e della tipologia delle riunioni, segnalando altresì quelle effettuate in sessione congiunta con gli organi di controllo societari, quali il Collegio sindacale o il Revisore legale. Questa parte del reporting consente di documentare in modo trasparente la continuità operativa e la regolarità di funzionamento dell'Organismo, oltre a evidenziare i momenti di confronto interfunzionale che rafforzano il sistema di controllo complessivo. A tali dati quantitativi si accompagna una sezione dedicata agli *highlights* delle riunioni, che riassume in forma discorsiva i principali temi affrontati, le criticità emerse, le decisioni assunte e le eventuali attività di *follow up* programmate.

Un ulteriore capitolo riguarda la gestione dei flussi informativi previsti dal Modello 231; in questa sede l'OdV descrive le informative ricevute dalle diverse strutture aziendali, richiamando eventualmente la data di trasmissione, i soggetti responsabili coinvolti, l'oggetto dell'informativa e l'esito delle valutazioni effettuate. La rendicontazione non si limita alla mera ricezione del flusso, ma dà conto di eventuali problematiche riscontrate, dei rilievi mossi e delle richieste di chiarimento o di documentazione integrativa avanzate dall'Organismo. In tal modo si rende evidente la funzione attiva e dinamica dell'OdV nel monitoraggio dei processi aziendali a rischio reato.

A ciò si affianca l'attività di audizione dei responsabili di processo, programmata anche secondo una logica *risk based* che privilegia le aree di maggiore esposizione. Il reporting illustra le audizioni svolte, sintetizzandone i contenuti principali, gli elementi di attenzione emersi e le ulteriori richieste di approfondimento o di verifica documentale eventualmente formulate.

Un'attenzione specifica è rivolta alla vigilanza sulla tenuta del Modello 231, ossia alle verifiche condotte per accertare che i presidi di controllo delineati nel Modello siano effettivamente coerenti con le procedure interne aziendali. In parallelo, viene data rendicontazione delle attività di vigilanza pianificata, svolte direttamente dall'OdV o con il supporto di strutture interne ed esterne. In questa sezione sono indicate le tipologie e il numero degli interventi effettuati, le carenze organizzative e procedurali rilevate, le azioni di miglioramento suggerite e l'esito dei successivi *follow up* volti a verificare la chiusura dei *gap* individuati. Non mancano, inoltre, riferimenti alle verifiche extra piano operativo, ossia alle attività ispettive condotte al di fuori della programmazione ordinaria per fronteggiare esigenze sopravvenute o eventi anomali.

Il reporting comprende anche la sezione dedicata al *whistleblowing*, nella quale sono riportati i dati sulle segnalazioni ricevute in ambito 231, l'esito delle indagini interne condotte, le misure correttive eventualmente adottate e le azioni disciplinari o organizzative conseguenti (si veda il § 4.4). Ciò consente di evidenziare come il canale di segnalazione costituisca uno strumento concreto di presidio della legalità e di prevenzione dei rischi.

Altrettanto significativa è l'attività di vigilanza sull'adeguatezza del Modello 231, che riguarda sia la Parte Generale sia le Parti Speciali. In questo contesto, l'OdV riferisce sugli aggiornamenti effettuati,

sulle attività di *risk assessment* condotte, sugli eventuali *gap* riscontrati rispetto al contesto normativo o organizzativo di riferimento e sui piani di azione predisposti per colmare tali lacune, con l'indicazione dei relativi *follow up*.

Accanto a tali attività, l'Organismo dedica un focus al monitoraggio delle novità normative e giurisprudenziali rilevanti per il sistema 231. Vengono analizzati sia i provvedimenti legislativi e regolamentari, anche se non direttamente collegati a nuovi reati presupposto, sia le più recenti pronunce giurisprudenziali in materia di responsabilità amministrativa degli enti. Tale monitoraggio consente di valutare l'adeguatezza del sistema di controllo interno e di proporre eventuali aggiornamenti.

Un ulteriore fronte di impegno riguarda le attività di formazione e informazione in materia 231. Nel reporting, l'OdV dà conto dei dati relativi alla formazione pianificata e a quella effettivamente erogata, degli eventuali scostamenti riscontrati e delle iniziative intraprese per il recupero.

La relazione dà evidenza delle informazioni e degli approfondimenti condotti in merito ad eventuali procedimenti giudiziari 231 che coinvolgano l'ente. In tali casi, l'OdV documenta le informative ricevute, gli eventuali atti acquisiti e le attività di monitoraggio poste in essere, in modo da presidiare tempestivamente ogni possibile ricaduta in termini di responsabilità amministrativa dell'ente.

In chiusura, l'Organismo di vigilanza esprime un giudizio motivato sull'effettività e sull'adeguatezza del Modello 231 rispetto al profilo di rischio dell'ente, fondato sulle attività svolte nel periodo. Sulla base di tale valutazione, l'OdV formula - ove necessario - proposte di aggiornamento del Modello e dei relativi presìdi, evidenziandone urgenza e impatto.

4. Whistleblowing e segnalazioni

4.1. Il D.lgs. 24/2023 (brevi cenni)

Con il D.lgs. 24/2023, l'Italia ha recepito la Direttiva (UE) 2019/1937 del 23 ottobre 2019 «riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione». Il Decreto, nel solco della normativa europea, mira a rafforzare la tutela delle persone che segnalano violazioni di disposizioni normative nazionali o del diritto UE, lesive degli interessi e/o dell'integrità dell'ente pubblico o privato di appartenenza e di cui siano venute a conoscenza nello svolgimento dell'attività lavorativa. Più in generale, la nuova disciplina intende promuovere la cultura della legalità e della compliance nei contesti organizzativi, in accordo alle indicazioni delle Istituzioni euro-unitarie e alle *best practices* internazionali in tema di *whistleblowing* e prevenzione della criminalità d'impresa.

A tal fine, il Decreto è intervenuto sulle norme interne che già regolavano la materia, le quali in precedenza distinguevano nettamente le tutele del *whistleblower* in base all'inquadramento lavorativo/professionale nel contesto pubblico o privato. Per quest'ultimo, la protezione era demandata in via diretta al D.lgs. 231/2001, il cui art. 6, co. 2-*bis* e ss., in relazione al contenuto

"minimo" dei Modelli, esigeva la previsione di: *i*) canali di segnalazione interna; *ii*) divieti di ritorsione e discriminazione nei confronti del segnalante; *iii*) un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure di protezione e delle procedure di segnalazione.

Anche il D.lgs. 24/2023, nel riformare la disciplina del *whistleblowing*, è intervenuto sul D.lgs. 231/2001. In particolare, è stato previsto quanto segue:

- art. 4, co. 1: *«i modelli di organizzazione e di gestione, di cui all'art. 6, comma 1, lettera a), del decreto legislativo n. 231 del 2001, prevedono i canali di segnalazione interna di cui al presente decreto»*;
- art. 21, co. 2: i modelli organizzativi *«prevedono nel sistema disciplinare adottato ai sensi dell'articolo 6, comma 2, lettera e), del decreto n. 231 del 2001, sanzioni nei confronti di coloro che accertano essere responsabili degli illeciti di cui al comma 1»;*
- art. 24, co. 5, che sostituisce il co. 2-*bis* dell'art. 6 del D.lgs. 231/2001: *«i modelli di cui al comma 1, lettera a) prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e)».*

Il legislatore del 2024 ha quindi confermato, per il settore privato, la responsabilità dell'organo dirigente in ordine alla previsione, all'interno dei Modelli, di canali di segnalazione interna conformi alle indicazioni del D.lgs. 24/2023. Di più, la norma ha posto a carico degli enti una serie di adempimenti collegati all'attivazione del sistema di *whistleblowing*, tra i quali:

- predisposizione di canali che soddisfino i parametri di sicurezza e affidabilità descritti dalla legge e dalle indicazioni dell'Autorità Nazionale Anticorruzione (ANAC);
- nomina di un "Responsabile della gestione delle segnalazioni" (di seguito anche "gestore"), specificamente formato in materia e dotato del requisito dell'autonomia;
- adozione di una procedura che regoli l'iter per l'esame delle segnalazioni pervenute e che sia conforme alle scadenze temporali dettate sia dalla Direttiva (UE) 2019/1937 sia dal D.lgs. 24/2023, a garanzia dell'effettività del sistema di reporting;
- adeguamento dei sistemi disciplinari mediante la previsione di sanzioni nei confronti di chi violi le misure di protezione del segnalante: anzitutto, la riservatezza della sua identità e il divieto di ritorsioni e discriminazioni.

La disciplina sinteticamente descritta, incidendo sui modelli organizzativi e sulle modalità di segnalazione degli illeciti, richiede un'attenzione particolare da parte dell'Organismo di vigilanza, che deve ricomprendere tra le proprie attività anche quella relativa alla vigilanza sul sistema di *whistleblowing*.

4.2. Le segnalazioni rilevanti e i canali di segnalazione

Preliminarmente, giova rammentare che le tutele previste dal D.gs. 24/2023 sono assicurate soltanto

nei confronti dei *whistleblowers* - che agiscono in buona fede - che abbiano presentato segnalazioni ammissibili secondo i requisiti di legge. In generale, possono essere segnalati quei comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'ente di appartenenza. Più in particolare, l'art. 2, lett. a) del D.lgs. 24/2023 precisa che le «violazioni» oggetto di segnalazione consistono in:

1. illeciti amministrativi, contabili, civili o penali;
2. condotte illecite rilevanti ai sensi del D.lgs. 231/2001 o violazioni dei Modelli di organizzazione, gestione e controllo adottati ai sensi di detto decreto (nel cui ambito i canali di segnalazione sono previsti);
3. illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea (riguardanti, a titolo esemplificativo, le seguenti materie: appalti pubblici; mercati finanziari e prevenzione del terrorismo; sicurezza e conformità dei prodotti; tutela dell'ambiente);
4. altri atti od omissioni che ledono gli interessi finanziari dell'Unione europea e/o riguardanti il mercato interno.

Rispetto quanto precede, merita evidenziare che l'adozione (volontaria) di un Modello organizzativo *ex* D.lgs. 231/2001 amplia il novero dei comportamenti che i soggetti dell'organizzazione potranno segnalare e/o divulgare pubblicamente, così esponendo l'ente – di nuovo – a un più alto rischio di infrazione della disciplina del *whistleblowing*. Tra le violazioni potenzialmente rilevanti rientreranno, infatti, quelle dei principi del Codice etico, dei principi di comportamento e delle altre procedure interne delineate dal Modello, indipendentemente dalla loro rilevanza quali "reati 231" o quali illeciti penali, civili, contabili e amministrativi *ex* dell'art. 2, lett. a), n. 1, oppure dalla circostanza che all'ente si applichi detto articolo nella sua interezza.

Esulano, dunque, dall'ambito di applicazione del Decreto in commento le contestazioni, le rivendicazioni o le richieste legate a un interesse di carattere personale del soggetto segnalante o che concernono esclusivamente i propri rapporti individuali di lavoro o di impiego pubblico anche con le figure gerarchicamente sovraordinate. Pertanto, la normativa in questione non si applica, a titolo esemplificativo, alle segnalazioni relative a cause di lavoro, discriminazioni tra colleghi, conflitti interpersonali tra il segnalante e un altro lavoratore o con i superiori gerarchici. A tal proposito, non si ravvisa una segnalazione di *whistleblowing* nel caso in cui il segnalante agisca per scopi essenzialmente personali o per contestazioni o rivendicazioni afferenti al rapporto di lavoro nei confronti dei superiori.

Per presentare la segnalazione il soggetto interessato può avvalersi, nei casi e nei modi previsti dal D.lgs. 24/2023, dei seguenti canali:

- canale di segnalazione interna;
- canale di segnalazione esterna gestito dall'ANAC;
- divulgazione pubblica;
- denuncia all'Autorità giudiziaria.

Il primo ha una valenza preferenziale in quanto si ritiene che si possano contrastare più facilmente i

fenomeni segnalati agendo sul fronte interno, tant'è che al canale di segnalazione esterna presso ANAC si ricorre quando si ravvisa una delle seguenti condizioni:

- non è prevista l'attivazione obbligatoria del canale di segnalazione interna o quest'ultimo, pur essendo obbligatorio, non è attivo o pur essendo attivo non è conforme alle prescrizioni di legge;
- la segnalazione interna non ha avuto seguito;
- vi sono fondati motivi per ritenere che alla segnalazione interna non verrà dato efficace seguito o che vi sia il rischio di ritorsione o, infine, che la violazione possa rappresentare un pericolo imminente o palese per il pubblico interesse.

L'interessato può avvalersi della divulgazione pubblica quando alle segnalazioni interna ed esterna non sia stato dato riscontro o abbia fondato motivo di ritenere che la violazione possa rappresentare un pericolo imminente o palese per il pubblico interesse o, ancora, perché ritiene in maniera fondata che a seguito della segnalazione esterna possano manifestarsi ritorsioni o non venga dato efficace seguito alla stessa. Infine, vi è la possibilità di rivolgersi direttamente all'Autorità giudiziaria, precisando che qualora il *whistleblower* abbia la qualifica di pubblico ufficiale, sussiste in capo a quest'ultimo un obbligo di denunciare all'autorità anzidetta i fatti penalmente rilevanti. Anche in tal caso, devono essere garantite le regole sulla tutela della riservatezza previste dal D.lgs. 24/2023, cui si rinvia.

4.3. Il ruolo dell'Organismo di vigilanza

Ai sensi dell'art. 5 del D.lgs. 24/2023, spetta all'organo di direzione dell'ente, in aggiunta all'attivazione dei canali di segnalazione interna, la nomina del responsabile della gestione del sistema di *whistleblowing*.

Il responsabile della gestione delle segnalazioni deve essere dotato di specifica formazione (i.e. professionalità) in materia di *whistleblowing* e discipline collegate e/o potenzialmente rilevanti in rapporto all'ambito oggettivo delineato dal D.lgs. 24/2023; per esempio, oltre al D.lgs. 231/2001, anche la normativa europea di riferimento, la disciplina del settore di attività dell'ente (bancaria, farmaceutica, sportiva, lavori pubblici, distribuzione, ecc.) la cui violazione può integrare illeciti amministrativi, civili, contabili, ecc. Il responsabile della gestione, inoltre, deve possedere il requisito dell'autonomia che, ad avviso dell'ANAC, deve essere inteso nel senso dell'imparzialità e indipendenza rispetto all'ente di cui gestisce il sistema; quindi, come connotazioni *prima facie* soggettive, oltre che di posizionamento organizzativo.

Nell'ambito del proprio ruolo, come detto, tale soggetto è responsabile di specifiche attività di "gestione" delle segnalazioni. Tra queste: *i*) invio dell'avviso di ricezione della segnalazione al segnalante, entro sette giorni a decorrere dal ricevimento; *ii*) riscontro al segnalante sull'esito dell'indagine interna, entro un termine ragionevole e comunque non superiore a tre mesi a far data dell'invio dell'avviso di ricezione della segnalazione; *iii*) mantenimento e cura delle interlocuzioni con il segnalante, così concorrendo a garantire un "corretto seguito" alle segnalazioni ricevute. In particolare, un corretto seguito implica – nel rispetto di tempistiche ragionevoli e della riservatezza dei

dati nel corso dell'accertamento dei fatti – una valutazione sulla sussistenza dei requisiti essenziali della segnalazione per valutarne l'ammissibilità e poter quindi accordare, al segnalante e agli altri soggetti garantiti, le tutele previste.

Una volta valutata l'ammissibilità della segnalazione, il gestore è tenuto ad avviare l'istruttoria interna sui fatti riportati nella stessa per valutarne la sussistenza e la fondatezza. Ove la segnalazione non sia adeguatamente circostanziata, il gestore potrà richiedere al segnalante elementi integrativi tramite il canale a ciò dedicato, o anche di persona, qualora il segnalante abbia richiesto e/o accettato, su iniziativa del gestore, un incontro diretto. Diversamente, il gestore potrà procedere all'archiviazione delle segnalazioni inammissibili, manifestatamente infondate o impossibili da accertare.

All'esito dell'istruttoria, nel fornire il riscontro finale al segnalante sull'esito della segnalazione, il gestore è tenuto a dare conto delle misure previste, adottate o da adottare affinché l'ente dimostri di voler dare seguito alla segnalazione, nonché dei motivi alla base della scelta.

Alla luce della delicatezza delle attività ora descritte, nonché delle caratteristiche di formazione e autonomia richieste dalla legge in capo al gestore delle segnalazioni, ci si è interrogati circa la possibilità di affidare tale ruolo all'OdV. È noto che nel contesto della previgente disciplina in materia di *whistleblowing* (L. 179/2017), la prevalenza dei Modelli organizzativi attribuisse proprio all'OdV l'esame delle segnalazioni e l'eventuale impulso all'adozione di misure rimediali a carico dell'ente, anche di tipo sanzionatorio/disciplinare nei confronti delle persone segnalate ovvero responsabili di atti di ritorsione e discriminazione ai danni del segnalante.

Nel settore privato la scelta del soggetto a cui affidare l'incarico di gestore delle segnalazioni è rimessa all'autonomia organizzativa di ciascun ente, tenendo in considerazione le esigenze legate alle dimensioni, alla natura dell'attività svolta e alla realtà organizzativa concreta. Tale ruolo, in linea teorica, può essere affidato agli organi di controllo interno, tra cui anche l'Organismo di vigilanza. Peraltro, tramite l'introduzione dell'obbligo di istituire i canali di segnalazione interna, il legislatore ha inteso incentivare i segnalanti a rivolgersi, innanzitutto, all'organizzazione alla quale sono "collegati", in quanto l'accertamento delle violazioni si gioverebbe, in termini di effettività, della vicinanza tra il gestore della segnalazione e il "fatto" (incontro orale con il segnalante, trasmissione di documenti, flussi informativi con le funzioni aziendali coinvolte, interviste delle persone informate, ecc.).

Giova evidenziare, però, che l'attività affidata all'OdV è in un certo senso "sensibile", in quanto potenzialmente impegnativa della responsabilità dell'ente in caso di inottemperanza alle prescrizioni di legge, ovvero di violazione di talune specifiche disposizioni (ad esempio, ritardi nel riscontro al segnalante, violazioni della riservatezza dell'identità del segnalante, altre violazioni in tema di privacy da parte del titolare del trattamento dei dati personali, inadeguato accertamento della fondatezza dei fatti segnalati, ecc.). La gestione delle segnalazioni è, cioè, un'attività rientrante nell'ambito dei rischi d'impresa, il cui processo andrebbe affidato a una funzione interna dell'ente ovvero a un consulente/professionista esterno che possa essere chiamato a rispondere del corretto adempimento dell'attività/consulenza di fronte all'organo dirigente.

In sintesi, una posizione difficilmente compatibile con l'indipendenza e la terzietà che l'OdV deve

mantenere nei confronti dell'ente ai sensi del D.lgs. 231/2001; in caso contrario, l'OdV rivestirebbe allo stesso tempo il ruolo di controllore e controllato, almeno rispetto a una attività "sensibile".

4.4. I flussi informativi in materia di segnalazioni

Il fatto che l'OdV non debba essere necessariamente (o almeno: è preferibile che non sia) il gestore del sistema di *whistleblowing* non significa che lo stesso debba rimanere estraneo e/o ignaro in merito alle segnalazioni ricevute e alle attività svolte per dare alle stesse un corretto seguito. Al contrario, è opportuno che l'OdV riceva specifici flussi informativi:

- da parte del gestore delle segnalazioni, in merito alle attività di gestione dei canali e alla ricezione di segnalazioni di violazioni rilevanti ai sensi del D.lgs. 231/2001;
- da parte dell'ente, in relazione alle misure rimediali e sanzionatorie adottate a valle delle segnalazioni e all'accertamento di eventuali comportamenti di discriminazione e ritorsione.

Anche in seguito all'entrata in vigore del D.lgs. 24/2023, resta dunque immutato il compito dell'OdV sul Modello complessivamente inteso e, dunque, anche sul sistema di *whistleblowing*.

I canali di segnalazione e le relative policy, infatti, rappresentano una parte essenziale del Modello, sia in virtù della nuova formulazione dell'art. 6 del D.lgs. 231/2001 sui contenuti minimi degli stessi, sia alla luce del fatto che il D.lgs. 24/2023 prevede espressamente, quali condotte illecite rilevanti, anche le violazioni del Modello organizzativo.

Con l'entrata in vigore della nuova disciplina sul *whistleblowing* spettano all'Organismo verifiche ulteriori, relative al corretto adempimento, da parte dell'ente, dei nuovi obblighi posti dalla disciplina: attivazione di adeguati canali interni di segnalazione (con specifico riguardo alle esigenze di riservatezza dell'identità dei segnalanti); nomina di un gestore formato in materia e autonomo; monitoraggio del corretto svolgimento delle attività di gestione, inteso come una vera e propria verifica di secondo livello (sempre nel rispetto della riservatezza dei dati relativi alle segnalazioni, che l'OdV non potrà conoscere se non espressamente autorizzato); monitoraggio delle comunicazioni/sanzioni da parte dell'autorità competente (ANAC per gli ambiti di propria competenza); svolgimento, da parte dell'ente, della formazione dei dipendenti e di audit sulla tenuta dei canali interni; monitoraggio sull'aggiornamento della documentazione privacy, ecc.

Emerge, dunque, con ulteriore evidenza non solo l'inopportunità di affidare all'Organismo di vigilanza il ruolo di gestore delle segnalazioni, ma anche la necessità di assicurare, nei suoi confronti, un effettivo e costante flusso informativo (periodico e a evento) da parte del gestore, in relazione alle segnalazioni di potenziale rilevanza ai sensi del D.lgs. 231/2001 e delle altre discipline idonee a impegnare la responsabilità dell'ente. In tal modo, si salvaguardano l'indipendenza, la terzietà e l'efficacia dei controlli richiesti dal D.lgs. 231/2001.

5. Attività dell'ODV e compliance integrata

5.1. Antiriciclaggio

L'attività di vigilanza dell'OdV assume particolare rilievo anche con riferimento agli obblighi derivanti dalla normativa in materia di prevenzione del riciclaggio e del finanziamento del terrorismo di cui al D.lgs. 231/2007. Sebbene la titolarità e la responsabilità degli adempimenti antiriciclaggio ricadano sui soggetti obbligati specificamente individuati dal legislatore – quali banche, intermediari finanziari, professionisti e operatori non finanziari in determinati settori – non può trascurarsi il fatto che la normativa antiriciclaggio e quella sulla responsabilità amministrativa degli enti condividono un comune obiettivo: la costruzione di un sistema di controllo interno idoneo a prevenire comportamenti illeciti che possano compromettere la legalità e l'integrità dell'attività aziendale. In questa prospettiva, l'Organismo è chiamato ad assumere un ruolo di raccordo e di verifica, pur senza sostituirsi agli organi e alle funzioni aziendali a ciò deputati, per garantire che il Modello 231 risulti coerente e integrato con i presidi previsti dal D.lgs. 231/2007.

Il contributo dell'OdV in questo ambito si manifesta anzitutto nella capacità di promuovere una cultura della compliance che tenga conto non solo delle esigenze derivanti dal Modello 231, ma anche delle misure organizzative e procedurali richieste dalla normativa antiriciclaggio. Occorre tuttavia chiarire che, nelle società e negli enti destinatari del D.lgs. 231/2007, l'OdV non è tenuto – né potrebbe esserlo – a vigilare sul corretto adempimento degli obblighi antiriciclaggio da parte dei soggetti obbligati, in quanto tale funzione non rientra tra le sue attribuzioni e rimane di esclusiva competenza delle funzioni aziendali appositamente preposte. Il ruolo dell'OdV si concentra invece sulla verifica che il presidio antiriciclaggio, già delineato dall'ente in adempimento agli obblighi di legge, risulti adeguatamente coordinato e coerente con i presidi previsti dal Modello 231, così da evitare sovrapposizioni, lacune o disallineamenti. In tale prospettiva, l'OdV non interviene nel merito degli adempimenti operativi (quali l'adeguata verifica della clientela, la conservazione documentale e le segnalazioni di operazioni sospette), ma vigila affinché il sistema di controlli predisposto dall'ente nel suo complesso garantisca un livello di protezione integrato ed efficace contro il rischio di riciclaggio e i reati presupposto previsti dal D.lgs. 231/2001.

Va peraltro evidenziato che il ruolo dell'OdV assume connotazioni differenti a seconda che l'ente sia o meno destinatario della normativa antiriciclaggio. Nel primo caso, le considerazioni appena esposte trovano piena applicazione, essendo necessario garantire un efficace coordinamento tra il presidio AML (*Anti Money Laundering*) e il Modello 231. Nel secondo caso, invece, pur mancando obblighi specifici di legge, restano comunque rilevanti ai fini della responsabilità amministrativa gli illeciti di riciclaggio, autoriciclaggio e impiego di denaro, beni o utilità di provenienza illecita, espressamente inclusi tra i reati presupposto dal D.lgs. 231/2001. Ne consegue che anche gli enti non soggetti agli obblighi di cui al D.lgs. 231/2007 devono predisporre adeguati presidi organizzativi per prevenire tali rischi. Nella prospettiva descritta, l'OdV può stimolare l'adozione di misure volontarie di mitigazione, suggerendo di trarre spunto – pur con i necessari adattamenti – dalle procedure e dai presidi previsti

dalla disciplina antiriciclaggio, così da rafforzare l'efficacia complessiva del Modello 231 e assicurare un più elevato livello di protezione dell'ente.

In entrambi i casi la predisposizione di un Modello 231 realmente efficace non può prescindere dall'integrazione con i presidi previsti dalla disciplina antiriciclaggio, pena il rischio di lasciare scoperta un'area di esposizione significativa. L'OdV, in quanto organo deputato alla vigilanza sull'attuazione e sull'osservanza del Modello, deve dunque garantire che quest'ultimo contempli misure specifiche e proporzionate per prevenire tali fattispecie di reato, verificandone la concreta operatività e proponendo gli opportuni aggiornamenti in caso di evoluzione normativa o giurisprudenziale.

Un ulteriore profilo di rilievo attiene alla capacità dell'OdV di favorire un coordinamento tra i diversi presidi interni. In molte realtà aziendali, infatti, la funzione antiriciclaggio è affidata a un ufficio dedicato o a un responsabile interno AML, mentre il Modello 231 assegna specifici compiti di prevenzione e controllo a vari organismi e funzioni. L'OdV, in tale contesto, assume un ruolo di "snodo" che consente di garantire una visione complessiva e integrata del sistema dei controlli, verificando che non vi siano sovrapposizioni, lacune o incoerenze tra quanto previsto dalla normativa antiriciclaggio e quanto stabilito dal Modello 231. Attraverso l'attività di audit, l'esame della documentazione e la raccolta di informazioni dalle funzioni aziendali competenti, l'OdV è in grado di individuare eventuali aree di rischio non adeguatamente presidiate e di proporre, ove necessario, interventi correttivi e migliorativi.

Particolare importanza riveste, inoltre, la vigilanza dell'OdV sulla gestione dei flussi informativi. La normativa antiriciclaggio prevede, infatti, un sistema articolato di obblighi di comunicazione interna ed esterna: dalle segnalazioni di operazioni sospette all'Unità di Informazione Finanziaria per l'Italia (UIF), fino alla trasmissione di dati e informazioni alle autorità di vigilanza. L'Organismo, nel rispetto delle competenze proprie dei soggetti obbligati, è chiamato a verificare che l'ente abbia adottato procedure che consentano un'adeguata circolazione delle informazioni, anche verso lo stesso OdV, ogniqualvolta emergano criticità o anomalie potenzialmente rilevanti ai fini 231. In tal senso, la collaborazione e il dialogo tra l'OdV e il responsabile antiriciclaggio aziendale rappresentano un elemento essenziale per assicurare la tempestiva individuazione e gestione dei rischi.

Non va infine trascurato l'aspetto culturale e formativo: l'OdV, in collaborazione con le funzioni aziendali competenti, può contribuire alla diffusione di una cultura della legalità anche attraverso la supervisione dei programmi di formazione in materia di prevenzione del riciclaggio e del finanziamento del terrorismo. L'attenzione deve essere rivolta non solo al personale direttamente coinvolto negli adempimenti AML, ma a tutti coloro che nello svolgimento della propria attività potrebbero entrare in contatto con operazioni o comportamenti a rischio. Nei confronti di questi ultimi si rende senz'altro opportuna un'attività formativa specifica finalizzata alla diffusione e alla conoscenza degli indicatori di anomalia emanati e periodicamente aggiornati dall'UIF.

5.2. Anticorruzione

Le funzioni dell'OdV assumono un'importanza significativa anche in rapporto alla normativa anticorruzione e trasparenza che, seppur nata con finalità autonome, condivide con il sistema 231 l'obiettivo di rafforzare la legalità e l'integrità dell'azione aziendale. La Legge 190/2012, con i suoi provvedimenti attuativi, ha introdotto un articolato sistema di prevenzione della corruzione nelle pubbliche amministrazioni, estendendo nel tempo alcuni dei suoi principi anche agli enti di diritto privato in controllo pubblico. Parallelamente, il D.lgs. 33/2013 ha posto al centro il principio di trasparenza, intesa non soltanto come accessibilità alle informazioni, ma anche come strumento di prevenzione dei fenomeni corruttivi. In tale contesto, sebbene la responsabilità primaria della gestione dei rischi corruttivi sia attribuita ad altre figure (in particolare al Responsabile della Prevenzione della Corruzione e della Trasparenza – RPCT – negli enti pubblici e negli organismi ad essi equiparati), l'OdV è chiamato a esercitare un ruolo complementare e di coordinamento, volto a garantire la coerenza e l'integrazione tra il Modello 231 e le misure previste dalla normativa anticorruzione e trasparenza.

Occorre chiarire che l'OdV non si sovrappone al RPCT o agli uffici preposti, né è chiamato a verificare l'assolvimento puntuale degli obblighi di legge in materia di trasparenza (quali, ad esempio, la pubblicazione di dati sul sito istituzionale), che rimangono di esclusiva competenza delle funzioni dedicate. L'OdV, tuttavia, vigila affinché il sistema dei controlli interni non presenti lacune o incoerenze e che le misure di prevenzione del rischio corruttivo e i meccanismi di trasparenza risultino adeguatamente coordinati con i presidi previsti dal Modello 231. La corruzione e i reati contro la pubblica amministrazione, infatti, rientrano a pieno titolo tra i reati presupposto rilevanti ai fini della responsabilità amministrativa dell'ente e, pertanto, un Modello di organizzazione e gestione realmente efficace deve contemplare presidi specifici per mitigare tali rischi.

Il ruolo dell'OdV, in questo ambito, si articola quindi su più livelli: da un lato, esso verifica che le procedure aziendali siano coerenti con le regole di correttezza, trasparenza e imparzialità imposte dalla normativa anticorruzione e dal Modello 231, evitando il rischio di comportamenti opportunistici o collusivi nei rapporti con la pubblica amministrazione o con altri soggetti privati; dall'altro, promuove una cultura aziendale orientata all'etica e alla legalità, verificando che l'ente abbia adottato misure organizzative idonee a prevenire situazioni di conflitto di interessi, favoritismi, pratiche di *mala gestio* o di gestione non trasparente. A tal fine l'OdV riceve flussi informativi periodici, svolgendo delle verifiche mirate secondo un piano di audit basato su un adeguato *risk assesment* e segnalando al vertice aziendale eventuali carenze e suggerendo le conseguenti azioni correttive. In tale prospettiva, il compito dell'OdV non si esaurisce in un controllo formale della documentazione, ma richiede una costante attività di monitoraggio e di dialogo con le funzioni aziendali, così da cogliere eventuali segnali di rischio e sollecitare l'adozione di correttivi tempestivi.

Anche in questo ambito, come già osservato in materia antiriciclaggio, il ruolo dell'OdV assume connotazioni differenti a seconda della natura dell'ente. Per gli enti pubblici e per le società a partecipazione pubblica, destinatari diretti della normativa anticorruzione e trasparenza, l'OdV è chiamato a vigilare sul corretto coordinamento tra il Modello 231 e il Piano Triennale di Prevenzione

della Corruzione e della Trasparenza (PTPCT), verificando che le due architetture di controllo non siano sviluppate in modo separato e incoerente, ma dialoghino tra loro, rafforzandosi reciprocamente. Per gli enti privati non direttamente soggetti alla L. 190/2012 e al D.lgs. 33/2013, invece, l'OdV ha il compito di assicurare che il Modello 231 preveda presidi adeguati a prevenire i reati corruttivi previsti dal D.lgs. 231/2001. In tali casi, pur non sussistendo obblighi normativi specifici, può risultare opportuno che l'ente adotti misure volontarie ispirate alle *best practice* pubblicistiche e ai presidi previsti per gli enti pubblici, così da rafforzare la propria reputazione e credibilità, oltre che ridurre in concreto l'esposizione al rischio corruttivo.

La vigilanza dell'OdV si estende inoltre alla gestione dei flussi informativi, che rappresentano un elemento essenziale tanto nel sistema 231 quanto nella normativa anticorruzione e trasparenza. L'Organismo è chiamato a verificare che vi sia un adeguato sistema di comunicazioni interne e di reporting, idoneo a garantire la tempestiva circolazione delle informazioni su eventuali anomalie o criticità, comprese quelle che possano riguardare possibili condotte corruttive o violazioni degli obblighi di trasparenza. Anche in questo caso, l'OdV non si sostituisce alle funzioni aziendali dedicate, ma vigila sulla effettiva operatività dei flussi e sulla loro capacità di fornire all'ente un quadro chiaro e aggiornato dei rischi.

Infine, l'OdV, in collaborazione con le funzioni competenti, può contribuire a orientare i programmi di formazione e sensibilizzazione, vigilando che essi siano calibrati sulle specificità dell'ente e rivolti non solo alle figure apicali, ma anche al personale operativo che, nei rapporti quotidiani, potrebbe trovarsi esposto a tentativi di condizionamento o indebite pressioni.

Nelle società in controllo pubblico, come definite dal D.lgs. 175/2016, l'Organismo di vigilanza assume un ruolo significativo anche nella verifica del rispetto degli obblighi di trasparenza. Tale funzione, nelle amministrazioni pubbliche, è attribuita per legge agli Organismi Indipendenti di Valutazione (OIV); poiché le società in controllo pubblico di norma non dispongono di un OIV, l'ANAC – con delibera n. 1134/2017 e successivamente con delibera n. 141/2018 – ha chiarito che tali compiti devono essere attribuiti all'organo interno di controllo più idoneo, individuabile anche nell'Organismo di vigilanza, i cui riferimenti vanno indicati nella sezione "Società trasparente" del sito web istituzionale.

5.3. Privacy

Il legame tra la disciplina in materia di protezione dei dati personali e le funzioni attribuite all'OdV si presenta come particolarmente significativo, in quanto le attività di vigilanza e controllo esercitate dall'OdV comportano spesso la necessità di accedere, trattare e conservare informazioni che rientrano nella nozione di "dato personale" ai sensi del Regolamento (UE) 2016/679 (GDPR) e del Codice per la protezione dei dati personali (D.lgs. 196/2003 e ss.mm.ii.). Si tratta, ad esempio, di informazioni relative a dipendenti, collaboratori, fornitori e altri *stakeholder*, che possono includere dati identificativi, dati connessi a procedimenti disciplinari, dati contenuti nelle segnalazioni interne (anche di natura anonima o riservata) e, talvolta, persino categorie particolari di dati ai sensi dell'art. 9 del GDPR (es. dati sanitari connessi a infortuni sul lavoro o dati sindacali in relazione a dinamiche

aziendali).

Proprio in ragione del ruolo di rilievo nell'ambito del trattamento di dati personali svolto dall'OdV nell'esercizio delle proprie funzioni, l'Autorità Garante per la protezione dei dati personali è intervenuta per chiarire che l'OdV, pur dotato di autonomi poteri di iniziativa e controllo, non può essere qualificato né come titolare né come responsabile del trattamento dei dati personali. Esso deve, piuttosto, essere considerato quale soggetto autorizzato al trattamento dei dati personali e, di conseguenza, i trattamenti effettuati dai suoi componenti devono essere ricondotti al titolare del trattamento, ovvero l'ente stesso. I componenti dell'OdV agiscono come soggetti autorizzati al trattamento, operando sotto l'autorità e secondo le istruzioni del titolare, nel rispetto dei principi di *accountability* e minimizzazione dei dati.

In sintesi, nello svolgimento della propria attività, con riferimento alla disciplina privacy, l'OdV deve tenere debitamente conto del sottile equilibrio tra autonomia funzionale e subordinazione gerarchica rispetto all'ente titolare del trattamento. L'OdV non è un soggetto autonomo nel trattamento dei dati, bensì un'articolazione interna dell'ente, la cui attività deve essere svolta nel rispetto delle regole del GDPR, con particolare attenzione alla riservatezza, alla sicurezza e alla liceità dei trattamenti effettuati.

Tale impostazione determina rilevanti conseguenze pratiche: in primo luogo, l'ente deve garantire che i componenti dell'OdV ricevano un'adeguata formazione in materia di protezione dei dati personali, affinché siano pienamente consapevoli dei limiti, delle cautele e delle responsabilità connesse ai trattamenti da loro effettuati. Le attività dell'OdV sono svolte nel rispetto dei principi di minimizzazione, integrità e riservatezza dei dati personali. L'ente assicura idonee procedure che garantiscano tracciabilità dei flussi informativi, corretta conservazione dei documenti e accesso esclusivamente da parte dei soggetti autorizzati; l'OdV opera su basi giuridiche adeguate, con poteri di accesso proporzionati e nel rispetto delle istruzioni del titolare del trattamento.

Ulteriore aspetto di rilievo è il coordinamento tra OdV e *Data Protection Officer* (DPO), laddove nominato dall'ente. Pur trattandosi di figure dotate di compiti e finalità distinte, la cooperazione tra OdV e DPO rappresenta un elemento essenziale per garantire la coerenza e l'efficacia complessiva del sistema dei controlli interni. Se l'OdV vigila sulla corretta attuazione e sull'efficacia del Modello 231, il DPO monitora l'osservanza del GDPR e delle disposizioni nazionali in materia di protezione dei dati. Un dialogo strutturato e continuo tra i due organismi consente di individuare tempestivamente criticità, evitare sovrapposizioni o lacune e assicurare che le verifiche svolte nell'ambito della compliance 231 siano condotte nel pieno rispetto della normativa privacy.

Particolare attenzione deve inoltre essere riservata alla gestione dei flussi informativi verso l'OdV, che costituiscono il canale principale attraverso il quale l'ente alimenta l'attività di vigilanza. Tali flussi possono contenere dati personali sensibili e, pertanto, devono essere trasmessi secondo modalità che ne garantiscano la riservatezza, la pertinenza e la proporzionalità rispetto alle finalità perseguite.

Il rispetto delle regole in materia di protezione dei dati personali si inserisce, dunque, come componente essenziale dell'efficacia del Modello 231. In tal senso, la tutela della privacy non rappresenta un limite, ma piuttosto un elemento di rafforzamento del sistema dei controlli interni,

contribuendo a garantire la legittimità, la trasparenza e la sostenibilità dell'attività di vigilanza dell'OdV.

5.4. Adeguati assetti organizzativi

L'OdV rappresenta uno snodo fondamentale nel sistema di governance aziendale, collocandosi come presidio di legalità e strumento di garanzia della corretta implementazione e dell'efficace attuazione del Modello organizzativo. Tale ruolo assume una portata più ampia in relazione agli obblighi posti dall'art. 2086, secondo comma, c.c., secondo cui gli amministratori sono tenuti a istituire assetti organizzativi, amministrativi e contabili adeguati alla natura e alle dimensioni dell'impresa, nonché idonei a rilevare tempestivamente i segnali di crisi e la perdita di continuità aziendale.

In tale contesto, l'attività dell'OdV non può essere circoscritta a un mero controllo formale della conformità al Modello 231, ma si inserisce come parte integrante di un sistema più ampio di presidi. L'adeguatezza degli assetti organizzativi, infatti, presuppone la presenza di procedure interne chiare, di un organigramma coerente con la struttura e le dimensioni aziendali, di flussi informativi attendibili e tempestivi, nonché di strumenti di risk management che consentano di individuare e anticipare possibili situazioni di disfunzione o criticità.

Sotto tale aspetto, l'azione dell'OdV assume rilievo in quanto lo stesso verifica che i protocolli e i presidi previsti dal Modello 231 siano effettivamente attuati e aggiornati in relazione all'evoluzione dell'organizzazione e dei rischi aziendali, segnalando agli organi competenti eventuali criticità rilevate nell'ambito delle proprie funzioni di vigilanza.

Il contributo dell'OdV si manifesta in primo luogo attraverso il costante aggiornamento e la verifica della mappatura delle attività sensibili e delle procedure interne correlate, attività che non solo tutela l'impresa dal rischio reato, ma favorisce anche una più generale cultura del controllo e della compliance, elementi imprescindibili per definire un assetto organizzativo proporzionato, funzionale ed efficace. Tale attività si traduce, ad esempio, nella verifica periodica della coerenza tra l'assetto organizzativo e i protocolli previsti dal Modello 231, nell'esame delle modalità di tracciabilità dei processi rilevanti ai fini del modello e nella valutazione dell'adeguatezza dei sistemi di delega e responsabilità in relazione alle aree di "rischio 231" individuate.

Un ulteriore profilo di rilievo riguarda la gestione dei flussi informativi. L'OdV è destinatario di segnalazioni, report e comunicazioni da parte delle diverse funzioni aziendali, che analizza per individuare anomalie o segnali di rischio. Lo scambio di flussi informativi consente all'OdV di svolgere in modo più efficace le proprie funzioni di vigilanza sul Modello 231, fornendo agli organi aziendali informazioni utili a garantire l'aggiornamento e il miglioramento continuo dei presidi di controllo previsti. In tal senso, i flussi informativi gestiti dall'OdV possono contribuire, seppure indirettamente, al rafforzamento complessivo del sistema di governance e alla tempestiva individuazione di eventuali anomalie rilevanti ai fini del Modello.

La documentazione prodotta dall'OdV, come le relazioni periodiche e le segnalazioni rivolte all'organo amministrativo o al Collegio sindacale, costituisce parte integrante del sistema di reporting interno.

Questi strumenti forniscono agli organi di vertice elementi ulteriori per valutare l'adeguatezza degli assetti, consentendo di intervenire tempestivamente in presenza di carenze o criticità, rafforzando l'efficacia del sistema di controllo interno e contribuendo, in via indiretta, alla continuità aziendale.

È inoltre importante sottolineare come l'azione dell'OdV, pur distinta da quella del Collegio sindacale e del Revisore legale, si inserisce in un sistema integrato di controlli che opera a diversi livelli e con finalità complementari. Se il Collegio sindacale ha il compito di vigilare sull'adeguatezza degli assetti ai sensi dell'art. 2403 c.c. e il Revisore legale è chiamato a esprimere un giudizio sulla correttezza contabile e sulla rappresentazione veritiera e corretta del bilancio, l'OdV aggiunge a questo quadro una prospettiva ulteriore, fondata sulla prevenzione del rischio reato e sulla verifica della compliance. Tale funzione, se correttamente esercitata, contribuisce ad alimentare la cultura della legalità, della trasparenza e della responsabilizzazione diffusa, che sono alla base di assetti realmente adeguati.

L'attività di vigilanza dell'OdV, fondata su indipendenza, autonomia e continuità d'azione, concorre a garantire che il sistema aziendale sia coerente con i principi sanciti dall'art. 2086 c.c. Operativamente, tale attività può essere svolta attraverso:

- la pianificazione di riunioni periodiche congiunte tra OdV, Collegio sindacale e Revisore legale, finalizzate al confronto sugli esiti delle rispettive attività di vigilanza e all'individuazione di aree di rischio comuni;
- lo scambio di flussi informativi, formalizzati in procedure interne, che disciplinino le modalità di trasmissione e condivisione di dati, segnalazioni e report;
- il coordinamento delle attività di audit, al fine di evitare duplicazioni e assicurare una copertura omogenea delle aree a rischio, sia sotto il profilo organizzativo sia sotto quello economico-finanziario.

In tale assetto integrato, l'OdV contribuisce ad arricchire il monitoraggio aziendale con la propria specifica prospettiva di vigilanza sul rischio reato che, per la natura stessa delle aree presidiate (rapporti con la P.A., gestione della sicurezza sul lavoro, fiscalità, ambiente, ecc.), intercetta spesso fenomeni rilevanti che si riflettono anche sull'equilibrio economico-finanziario dell'ente.

5.5. Sicurezza sul lavoro

Nel perimetro della salute e sicurezza sul lavoro, l'Organismo esercita vigilanza di secondo livello sull'effettiva attuazione dei presìdi del Modello 231 rilevanti ai fini dei reati di cui all'art. 25-*septies*. L'OdV non dispone di poteri decisionali o gestionali in materia di D.lgs. 81/2008 e non garantisce l'adempimento degli obblighi prevenzionistici, che restano in capo ai soggetti titolari.

In materia, l'Organismo è chiamato a svolgere una funzione di "alta vigilanza" sulla idoneità e l'efficace attuazione del Modello di cui all'art. 30 D.lgs. 81/2008 che consiste, in particolare, nel:

- verificare nel tempo, tenuto conto della natura e delle dimensioni dell'organizzazione nonché del tipo di attività svolta, l'idoneità del Modello a garantire, in termini di effettuazione e registrazione,

l'adempimento degli obblighi previsti dalla normativa come nel tempo vigente a carico dell'ente, con particolare riguardo alla previsione di:

  - un'articolazione di funzioni che assicuri competenze tecniche e poteri necessari per la verifica, la valutazione, la gestione e il controllo del rischio;
  - un adeguato sistema di flussi informativi (ad es. da parte del datore di lavoro all'organo amministrativo e all'Organismo medesimo, di delegati/subdelegati di funzioni rispettivamente al proprio delegante);
  - un adeguato e tempestivo sistema di circolazione in azienda delle informazioni sull'organizzazione, sui rischi e sulle misure di prevenzione e protezione nel tempo adottate;
  - un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello;
  - un sistema di controllo sull'attuazione del Modello e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate;

- monitorare l'attuazione del Modello, con riferimento all'effettività dei controlli, al rispetto delle misure in esso indicate in relazione all'adempimento degli obblighi prevenzionali, all'attuazione dei flussi informativi e all'eventuale applicazione di sanzioni disciplinari nel caso di violazione da parte degli organi competenti;
- monitorare il riesame e l'eventuale modifica del Modello ove siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico, eventualmente segnalandone la necessità all'organo amministrativo e proponendo azioni in merito.

L'Organismo può adempiere le predette funzioni di vigilanza attraverso le seguenti attività:

- monitoraggio della normativa direttamente o indirettamente rilevante in materia di sicurezza sul lavoro;
- analisi dei flussi informativi periodici (ad esempio su valutazione dei rischi, mutamenti dell'organigramma della sicurezza, modifica del datore di lavoro o conferimento, modifica o revoca di deleghe o sub-deleghe di funzioni *ex* art. 16 D.lgs. 81/2008, applicazione di sanzioni disciplinari; verbale delle riunioni periodiche *ex* art. 35 D.lgs. 81/2008; report audit degli enti di certificazione; verbali di riesame dell'alta direzione) o ad evento (ad esempio reportistica su infortuni sul lavoro; verbali ispettivi o di contestazione degli organi di vigilanza; report audit interni o esterni sulla sicurezza sul lavoro);
- eventuali acquisizioni documentali (ad esempio nomine, deleghe/sub-deleghe, DVR, DUVRI, protocolli, procedure, policy, istruzioni operative, piani di emergenza, certificazioni e, nell'ambito di cantieri temporanei mobili, PSC o POS);
- richieste di informazione o audizioni (periodiche o ad evento) del personale aziendale titolare di obblighi o attribuzioni in materia di sicurezza sul lavoro (datore/i di lavoro, delegati o subdelegati

di funzioni, dirigenti, preposti, medico competente, RSPP, RLS, coordinatori per la progettazione e per l'esecuzione dei lavori in cantieri temporanei o mobili) ovvero di funzioni di controllo (compliance, audit, ecc.);

- verifiche su singole attività e relativa documentazione (ad esempio in tema di formazione o informazione dei lavoratori, sorveglianza sanitaria, gestione delle emergenze, prove di evacuazione, operazioni di primo soccorso, prescrizioni impartite dagli organi di vigilanza, valutazioni di idoneità tecnico-funzionale, cooperazione e coordinamento in caso di contratti di appalto, opera o somministrazione, nomine e reportistiche apertura di cantieri temporanei o mobili);
- scambi informativi (periodici o ad evento) con l'organo amministrativo e con il datore di lavoro (ove non coincidente con l'organo amministrativo) ovvero con il gestore delle segnalazioni interne.

In sintesi, l'OdV esercita alta vigilanza sulla conformità e sull'effettiva attuazione del Modello ai sensi dell'art. 30 D.lgs. 81/2008 e del D.lgs. 231/2001, senza compiti gestionali o poteri decisionali. Esso verifica che i flussi informativi, i meccanismi di controllo e le misure di prevenzione siano non solo formalmente adottati, ma anche concretamente attuati e costantemente aggiornati rispetto all'evoluzione normativa, organizzativa e tecnologica e, in presenza di criticità, attiva il coinvolgimento del vertice aziendale monitorando l'attuazione dei correttivi e la revisione del Modello 231.

5.6. Intelligenza artificiale (IA) e cybersicurezza

Il rapido sviluppo delle tecnologie digitali e l'integrazione crescente dell'IA nei processi aziendali costringono gli Enti a rafforzare i presidi di controllo interno, a ripensare la tradizionale assegnazione di ruoli e funzioni ai decisori umani e, di conseguenza, a ridisegnare il perimetro delle responsabilità e delle verifiche sulla gestione delle imprese, anche ai fini della responsabilità 231 e delle correlate attività di vigilanza sulla tenuta del Modello. Ciò comporta un ampliamento delle attività dell'OdV, che deve essere in grado, anzi tutto, di conoscere le trasformazioni tecnologiche del mondo del lavoro, di interpretare i rischi legati alla cybersicurezza e all'IA, non solo come minacce operative, ma anche come potenziali fonti di responsabilità dell'ente, di monitorare le attività per le quali si fa ricorso alle "macchine".

In tale contesto, la capacità dell'OdV di anticipare i cambiamenti, contribuire al rafforzamento delle attività di controllo (anche collaborando attivamente con le altre funzioni aziendali) e promuovere una cultura della cybersicurezza, rappresenta un elemento cruciale: *i*) per assicurare l'adeguatezza e l'efficacia del Modello 231 nell'ambito del sistema di controllo interno; *ii*) per la protezione dell'ente dai rischi di incorrere – anche colposamente – in situazioni da cui possa discendere la responsabilità di cui al Decreto 231.

Con riferimento a quest'ultima, la cybersicurezza ha assunto un rilievo crescente in relazione tanto ai c.d. *computer crimes* (attacchi informatici a computer, *device* e infrastrutture digitali dell'azienda,

anche tramite virus, *malware*, ecc.), quanto ai c.d. *computer facilitated crimes* (reati comuni realizzati attraverso l'impiego di strumenti informatici, per esempio: furto, trattamento illecito di dati, appropriazione indebita, clonazione di strumenti di pagamento, riciclaggio, estorsione, falsi e contraffazione, frode informatica, *phishing*, ecc.).

Il D.lgs. 231/2001 prevede, sin dalla sua prima introduzione, la responsabilità amministrativa agli enti per le frodi informatiche perpetrate in danno dello Stato o di un Ente pubblico (art. 640-*ter* c.p., incluso nell'art. 24 del Decreto). A seguire, la responsabilità è stata estesa alle ipotesi espresse di commissione dei delitti informatici e trattamento illecito di dati (art. 24-*bis*). Da ultimo, la legge sulla cybersicurezza (L. 90/2024, recante «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici») ha apportato diverse modifiche ai reati informatici previsti dal Codice penale e al citato art. 24-*bis* del Decreto 231, che li richiama ai fini della responsabilità amministrativa.

Va ricordato che nell'ambito più ampio della cybersicurezza devono considerarsi anche l'art. 25-*octies*.1 del Decreto 231, dedicato ai delitti in materia di strumenti di pagamento diversi dai contanti e, come detto, i c.d. *computer facilitated* (o *related*) *crimes* previsti agli artt. 25-*sexies* (Abusi di mercato), 25-*octies* (Ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita) e 25-*nonies* (Delitti in materia di violazione del diritto d'autore), reati che assumono rilevanza in questa sede nella misura in cui vengano commessi con l'impiego degli strumenti informatici o sui mercati virtuali.

Il tema della cybersicurezza, quindi, non è solo tecnico, ma diventa un ambito strategico anche per la corretta programmazione delle attività di vigilanza, la prevenzione dei reati e l'efficacia del sistema 231 nel suo complesso.

Per le ragioni esposte, nell'esecuzione delle attività di vigilanza sull'efficacia e sull'adeguatezza del Modello 231, con specifico riferimento alle misure e ai protocolli di sicurezza informatica, l'OdV è chiamato a:

- verificare l'esistenza e l'aggiornamento di policy di cybersicurezza coerenti con le normative nazionali ed europee (es. GDPR, NIS2, D.lgs. 24/2023 in materia di *whistleblowing*, normativa Dora);
- verificare la mappatura dei rischi informatici e la corretta implementazione di controlli organizzativi (essendo l'idoneità tecnica in capo alle funzioni IT), tenendo conto delle caratteristiche del business e della sua eventuale modifica all'insegna dell'evoluzione tecnologica (per esempio, vendite online, raccolta dei dati personali dei clienti, quotazione/investimenti sui mercati regolamentati, ecc.);
- accertarsi che il personale sia adeguatamente formato sui rischi cyber e sulle modalità di segnalazione di eventuali incidenti;
- monitorare gli aggiornamenti tecnologici e la resilienza dei sistemi, anche attraverso audit periodici e reportistica interna;
- segnalare carenze e raccomandare l'avvio di interventi da parte delle funzioni competenti in

merito ai presidi tecnologici che assicurino, per quanto possibile, la "difesa" dell'ente dal pericolo di subire violazioni informatiche e, più in generale, l'ammodernamento tecnologico dell'impresa, a beneficio del business e del sistema di controllo interno.

In modo parzialmente correlato a quanto detto rispetto ai rischi informatici, anche l'intelligenza artificiale sta trasformando profondamente il modo in cui le imprese operano, introducendo sia vantaggi competitivi sia nuove aree di rischio, in costante evoluzione. Le applicazioni di IA, infatti, possono incidere su decisioni critiche, sulla gestione dei dati e sull'automazione di processi che coinvolgono responsabilità legali ed etiche, anche in tema di rispetto dei diritti umani, della sicurezza e della dignità dei lavoratori. Si pensi, a quest'ultimo proposito, alle nuove forme di manifestazione dello sfruttamento lavorativo, mediante l'affidamento della gestione dei dipendenti ad algoritmi e piattaforme informatiche; o ancora, all'impiego di immagini e altri dati sensibili "rubati" in rete per la creazione di contenuti falsi, alle violazioni della privacy dei consumatori e alle frodi perpetrate ai loro danni.

Sotto il profilo normativo, con la Legge 23 settembre 2025, n. 132, l'Italia ha adottato un quadro organico di norme sull'intelligenza artificiale, finalizzato a promuovere un uso sicuro, etico, trasparente e affidabile dell'IA, in coerenza con i principi del Regolamento (UE) 2024/1689 ("AI Act"). La nuova disciplina introduce principi fondamentali - tra cui trasparenza, supervisione umana, responsabilità, tracciabilità, non discriminazione e sicurezza - e stabilisce obblighi differenziati in funzione del livello di rischio del sistema IA (approccio *risk-based*).

Muovendo da tali premesse, l'impiego dell'IA da parte delle organizzazioni è soggetto a diversi obblighi, per lo più attinenti alla valutazione e riduzione del rischio, al monitoraggio e alla trasparenza sui processi decisionali. Ne discende che l'introduzione dell'IA in azienda rappresenta un fattore di rischio che va valutato con attenzione, soprattutto da parte dell'organo di indirizzo. Infatti, il tema dei reati informatici, della cybersicurezza e dell'IA non riguarda più l'iniziativa criminale del singolo o della "macchina", bensì la colpa d'organizzazione, ossia il malgoverno dei rischi derivanti dall'affidamento delle attività gestorie e dei controlli all'IA, allorquando detti sistemi siano impreparati o non adeguatamente formati e controllati circa i divieti e le violazioni che potrebbero realizzare o i principi etici che dovrebbero guidare l'attività d'impresa; oppure, nello scenario peggiore, siano intenzionalmente addestrati alla commissione di reati "in nome e per conto" dell'impresa ovvero "nel suo interesse e a suo vantaggio".

Gli organi di controllo - e l'OdV in particolare - devono dunque vigilare con scrupolo almeno sui seguenti aspetti dell'organizzazione aziendale:

- trasparenza e tracciabilità delle decisioni automatizzate, per evitare discriminazioni, abusi o mancanze di accountability (si pensi in particolare al tema della sicurezza sul lavoro nel caso di macchinari che agiscono secondo algoritmi di intelligenza artificiale, ma anche alle verifiche in materia di antiriciclaggio);
- rispetto dei principi di intervento e sorveglianza umana delle piattaforme digitali e degli algoritmi impiegati per l'esecuzione di talune attività (c.d. "*human-in-the-loop*" o "*human-in-command*"),

soprattutto quelle relative alla gestione del personale e all'organizzazione della logistica;

- sicurezza degli algoritmi, per prevenire manipolazioni, attacchi informatici o utilizzi non autorizzati;
- monitoraggio dei sistemi di IA e aggiornamento degli stessi;
- formazione del personale sui limiti e i rischi dell'IA;
- aggiornamento dei Modelli 231 con specifici focus sull'IA.

Il ruolo dell'OdV, in questo contesto, si estende alla verifica che l'adozione di tecnologie basate su IA sia accompagnata da un'adeguata analisi dei rischi, dalla definizione di regole di governance e dalla predisposizione di controlli efficaci. È inoltre opportuno che l'OdV collabori con le funzioni IT, compliance e legale per integrare questi aspetti nel Modello 231, aggiornandolo rispetto alle nuove minacce e innovazioni.

5.7. Ambiente

L'inserimento dell'art. 25-*undecies* nel D.lgs. 231/2001, a seguito del D.lgs. 121/2011, ha segnato un passaggio cruciale nell'estensione del perimetro di vigilanza dell'OdV, richiedendo una crescente attenzione ai profili ambientali dell'attività d'impresa.

I reati oggi ricompresi nella categoria ambientale sono numerosi e complessi. Si va dalle condotte legate all'inquinamento e alla gestione illecita dei rifiuti, fino a fattispecie più gravi come il disastro ambientale e i reati in materia di commercio di specie protette. Tale articolazione richiede che l'OdV sviluppi una competenza trasversale, capace di integrare aspetti normativi, tecnici e gestionali.

L'art. 25-*undecies* D.lgs. 231/2001, infatti, include una serie eterogenea di fattispecie penali, tra cui a titolo meramente esemplificativo:

- inquinamento ambientale (art. 452-*bis* c.p.);
- disastro ambientale (art. 452-*quater* c.p.);
- omessa bonifica (art. 452-*terdecies* c.p.);
- attività organizzate per il traffico illecito di rifiuti (art. 452-*quaterdecies* c.p.);
- abbandono di rifiuti pericolosi (art. 255-*ter* D.lgs. 152/2006);
- gestione illecita di rifiuti (art. 256 D.lgs. 152/2006);
- combustione illecita di rifiuti (art. 256-*bis* D.lgs. 152/2006);
- superamento dei limiti di emissione (art. 279, co. 5, D.lgs. 152/2006);
- violazioni in materia di protezione delle acque, aria e suolo, commercio di specie protette (artt. 727-*bis* e 733-*bis* c.p.).

Tali reati si caratterizzano per la loro elevata complessità tecnico-normativa e per la sovrapposizione tra il diritto penale ambientale e la disciplina amministrativa settoriale. È dunque necessario che l'OdV si doti di competenze specifiche o si avvalga, se del caso, di consulenti tecnici ambientali.

In materia ambientale (art. 25-*undecies*), l'OdV comprende il perimetro dei processi esposti a rischio, come la produzione industriale, lo smaltimento dei rifiuti, l'impiego di sostanze pericolose o la gestione degli scarichi idrici e verifica, in chiave di seconda linea, che l'ente li abbia mappati e presidiati tramite protocolli, responsabilità, autorizzazioni e registrazioni idonee, evitando approcci meramente formali. L'OdV valuta che le misure organizzative, procedurali e tecnologiche previste dal Modello 231 siano effettivamente implementate, aggiornate, comunicate e conosciute da chi opera nelle aree a rischio. In quest'ottica, l'OdV non svolge verifiche tecniche di tipo operativo, ma effettua controlli e audit, segnalando la necessità di adeguare il Modello alle nuove esigenze normative, organizzative o giurisprudenziali.

Un presidio efficace dei reati ambientali richiede che l'OdV vigili sui flussi informativi rilevanti, inclusi i report ambientali interni, le segnalazioni di eventi critici, le comunicazioni con le autorità ambientali (ARPA, ISPRA, ecc.) e gli esiti delle eventuali ispezioni o contestazioni ricevute informando, se del caso, gli organi di vertice e monitorando il completamento degli interventi.

Un momento cruciale per l'attività dell'OdV è rappresentato dalla mappatura dei rischi ambientali, che deve essere condotta in stretta collaborazione con le funzioni tecniche competenti, come l'HSE Manager o il Responsabile Ambientale o altro soggetto a ciò preposto o delegato.

La mappatura deve identificare le aree operative maggiormente esposte (ad esempio, impianti di trattamento, laboratori chimici, aree di stoccaggio rifiuti), le responsabilità, le autorizzazioni e le procedure in essere, i controlli in essere e la loro efficacia con una stima del rischio residuo attraverso criteri oggettivi e documentati. Questa analisi rappresenta la base per definire le priorità di vigilanza e per calibrare il piano annuale delle attività dell'OdV.

Un aspetto fondamentale consiste nell'integrazione della mappatura con altri strumenti già presenti in azienda: il Documento di Valutazione dei Rischi (DVR), i piani di gestione ambientale certificati (ISO 14001, EMAS) e gli audit interni.

In funzione dei risultati dell'analisi dei rischi e dell'evoluzione normativa l'OdV adotta un piano annuale di vigilanza che, con approccio di secondo livello, può prevedere, ad esempio:

- *site visit* su impianti o reparti ad alto impatto ambientale per esaminare lo stato di gestione dei rifiuti e la presenza di eventuali criticità operative;
- interviste ai responsabili di funzione;
- verifiche documentali su autorizzazioni (AIA, AUA), registri e formulari rifiuti, MUD, report di monitoraggio e non conformità;
- verifica del corretto monitoraggio delle scadenze e degli adempimenti normativi;
- verifica a campione della formazione del personale su tematiche ambientali e procedurali (esame dei registri e attestati di partecipazione);
- verifica che i report di monitoraggio (scarichi/emissioni) siano disponibili e valutati dalle funzioni competenti e che eventuali superamenti e/o irregolarità siano tracciati, comunicati

all'OdV e gestiti con azioni correttive e tempi assegnati;

- riesame delle segnalazioni ricevute tramite i canali *whistleblowing* relativi a potenziali illeciti ambientali.

È consigliabile che queste attività siano documentate puntualmente in appositi verbali e report e che gli esiti siano oggetto di confronto periodico con l'organo amministrativo, anche per valutare eventuali azioni correttive o migliorative.

Inoltre, l'OdV può:

- sollecitare simulazioni di gestione delle emergenze ambientali (con verifica della prontezza del personale e dell'efficacia delle procedure) alle quali partecipare in qualità di osservatore;
- svolgere audit sui conferimenti dei rifiuti e la loro tracciabilità (in collaborazione con operatori terzi);
- richiedere analisi di *benchmark* normativo e giurisprudenziale, anche su casi giudiziari recenti;
- verificare l'effettiva attuazione dei piani di miglioramento ambientale previsti da certificazioni ISO o da provvedimenti prescrittivi;
- verificare il rispetto delle prescrizioni contenute nei provvedimenti delle autorità ambientali (ARPA, ISPRA, Ministero dell'Ambiente, ecc.), anche in fase di post-ispezione.

Uno dei presidi più rilevanti nella prevenzione dei reati ambientali è rappresentato dai flussi informativi tra l'OdV e le diverse funzioni aziendali. È fondamentale che l'OdV riceva, con regolarità, secondo una tempistica individuata, e completezza:

- le comunicazioni di eventi anomali con impatto ambientale,
- i rapporti di ispezione delle autorità competenti,
- le segnalazioni di non conformità interne o di comportamenti difformi.

L'istituzione di canali di segnalazione dedicati – anche anonimi – e l'adozione di procedure di *whistleblowing* rappresentano strumenti sempre più diffusi e raccomandati.

In caso di incidente ambientale rilevante, l'OdV deve essere prontamente informato e può valutare l'attivazione di un'indagine interna o la revisione urgente del Modello, oltre a monitorare la gestione della crisi da parte delle strutture aziendali competenti.

L'efficacia dell'azione dell'OdV si accresce quando si realizza un dialogo strutturato e continuativo con gli altri organi di controllo presenti in azienda. Con il Collegio sindacale o il Revisore legale è opportuno condividere i profili ambientali che possano avere riflessi economico-patrimoniali o reputazionali. Con l'HSE Manager e il RSPP si deve operare in stretta sinergia per evitare sovrapposizioni e per valorizzare le competenze tecniche specifiche. Nei gruppi strutturati, anche il Comitato ESG o il Responsabile della sostenibilità possono costituire interlocutori rilevanti, specie in chiave di rendicontazione non finanziaria.

5.8. ESG (Environmental, Social, Governance)

L'evoluzione del contesto economico, normativo e culturale ha portato i fattori ESG (Environmental, Social, Governance) a incidere profondamente sul modo di operare delle imprese, estendendo la prospettiva del controllo e della compliance oltre i confini della mera osservanza normativa. Al riguardo, nel 2025 la Commissione Europea ha intrapreso un'azione di revisione significativa delle normative ESG, adottando il cosiddetto "Regolamento Omnibus", un pacchetto di modifiche e aggiornamenti avente come obiettivo la semplificazione e rimodulazione degli obiettivi di rendicontazione della sostenibilità a livello comunitario, con impatto su quattro regolamenti europei fondamentali:

- CSRD (Corporate Sustainability Reporting Directive) e gli ESRS (European Sustainability Reporting Standards);
- CSDDD (Corporate Sustainability Due Diligence Directive);
- Tassonomia Europea;
- CBAM (Carbon Border Adjustment Mechanism).

La sostenibilità incide su processi e controlli aziendali e può riflettersi sui rischi reato 231. In tale prospettiva, l'OdV considera gli esiti e i flussi ESG come input del proprio *risk assessment* limitatamente ai profili 231 (es. ambiente - art. 25-*undecies*; salute e sicurezza - art. 25-*septies*; anticorruzione - artt. 24-25; reati societari - art. 25-*ter*; impiego di cittadini di Paesi terzi - art. 25-*duodecies*; delitti informatici e trattamento dati - art. 24-*bis*). L'OdV non assume compiti di governance ESG né di rendicontazione: utilizza tali informazioni per verificare l'adeguatezza e l'effettiva attuazione del Modello 231 e per proporne l'aggiornamento quando i rischi ESG entrano nel perimetro 231.

Invero, l'integrazione dei fattori ESG nel sistema 231 non introduce un nuovo ambito di vigilanza, ma amplia la prospettiva dell'Organismo, chiamato a verificare la coerenza tra i principi dichiarati e i comportamenti concreti dell'organizzazione, soprattutto con riferimento al Codice etico. Attraverso un approccio basato sul rischio, una lettura unitaria dei sistemi di controllo e una costante attenzione all'evoluzione normativa e di mercato, il Modello 231, pur restando finalizzato alla prevenzione dei reati e alla tutela dell'ente ai sensi del Decreto, può contribuire, se effettivamente attuato, a rafforzare la cultura della legalità e della responsabilità, elementi che concorrono alla sostenibilità complessiva dell'impresa.

Il ruolo dell'OdV rispetto ai fattori ESG si inserisce nel più ampio ambito della compliance integrata, volta a garantire un presidio unitario e coerente dei diversi ambiti di rischio aziendale. L'Organismo non assume funzioni operative nella gestione della sostenibilità, ma vigila affinché le politiche, le procedure e i comportamenti aziendali siano coerenti con i principi del Modello 231 e con i valori di trasparenza e correttezza che ispirano la normativa. L'obiettivo è accertare che l'integrazione dei fattori ESG non resti un adempimento formale o comunicativo, ma si traduca nell'adozione di effettivi presidi organizzativi e procedurali, idonei a prevenire comportamenti illeciti o non conformi.

In questa prospettiva, l'OdV assume un ruolo di "cerniera" tra il Modello 231 e gli altri sistemi di

gestione presenti in azienda, come quelli ambientali, di salute e sicurezza, anticorruzione, parità di genere, sicurezza informatica e protezione dei dati personali. L'OdV può quindi valorizzare le informazioni e gli esiti derivanti da tali sistemi, integrandoli nella propria analisi dei rischi e nel piano di verifiche periodiche. Attraverso l'esame dei flussi informativi, la valutazione dei report di audit e la verifica dell'aggiornamento del Modello, l'Organismo può monitorare la reale incorporazione dei fattori ESG nelle procedure aziendali e nei comportamenti organizzativi.

Un'attenzione particolare deve essere dedicata al collegamento tra i fattori ESG e le categorie di reato previste dal Decreto.

Sul versante ambientale (E), l'OdV vigila sui rischi connessi alle violazioni delle norme in materia di gestione dei rifiuti, scarichi, emissioni, uso di sostanze pericolose e tutela del territorio, che rientrano tra i reati ambientali di cui all'art. 25-*undecies*. La vigilanza potrà estendersi anche alla veridicità delle comunicazioni ambientali e alle eventuali dichiarazioni o certificazioni non conformi alla realtà, che possono integrare ipotesi di frode, truffa ai danni dello Stato o false comunicazioni sociali. L'Organismo, in tale ambito, potrà esaminare i flussi informativi provenienti dalle funzioni tecniche, valutare la regolarità delle autorizzazioni, il rispetto delle scadenze e la gestione delle non conformità ambientali.

Sul piano sociale (S), l'OdV deve considerare i rischi legati alla tutela della salute e sicurezza dei lavoratori, che trovano corrispondenza nei reati di cui all'art. 25-*septies*, nonché quelli relativi a discriminazioni, molestie o violazioni della dignità personale, che possono essere ricondotti ai delitti contro la persona o alla violazione della normativa in materia di parità di trattamento. Anche il rispetto delle regole in materia di contratti di appalto, somministrazione e intermediazione di manodopera può presentare profili di rischio sotto l'aspetto penale, ma anche reputazionale. L'OdV, attraverso i flussi HR, gli esiti degli audit e le segnalazioni *whistleblowing*, può verificare la coerenza delle politiche aziendali con i principi di tutela del lavoro e di inclusione sociale dichiarati dall'impresa.

Per quanto concerne il fattore di governance (G), l'Organismo deve vigilare sulla correttezza dei processi decisionali e sulla trasparenza della rappresentanza dell'ente nei confronti dei terzi e della pubblica amministrazione. Rientrano in tale ambito i reati contro la pubblica amministrazione (artt. 24 e 25), le ipotesi di corruzione tra privati, i reati societari (art. 25-*ter*) e quelli tributari (art. 25-*quinquiesdecies*), oltre ai reati informatici e di trattamento illecito dei dati (art. 24-*bis*). La vigilanza dell'OdV può quindi comprendere la verifica della tracciabilità delle decisioni, del corretto utilizzo dei poteri di rappresentanza, della coerenza tra dati gestionali, bilanci civilistici e informazioni di sostenibilità. Particolare attenzione va riservata ai rischi di *greenwashing*, che possono derivare da comunicazioni non veritiere o fuorvianti su obiettivi e risultati ESG: in tali casi, l'OdV può verificare l'esistenza di procedure di validazione dei dati e la congruità dei controlli interni.

Il Modello 231 rappresenta oggi un tassello del più ampio sistema di governance aziendale, volto a integrare la prevenzione dei reati con la tutela della sostenibilità e dell'etica d'impresa, nella logica di un controllo interno fondato su legalità, trasparenza e responsabilità. In tal senso l'evoluzione dei fattori ESG contribuisce a ridefinire i confini dei rischi reato 231, rafforzando la necessità di un

approccio integrato tra risk management, compliance e vigilanza, e richiede il presidio dell'OdV sul periodico e continuo aggiornamento della mappatura dei rischi, con particolare riguardo ai nuovi ambiti di attenzione (transizione ecologica, economia circolare, benessere organizzativo, etica digitale, gestione dei dati) e alle modalità con cui essi possano incidere sulla responsabilità dell'ente. Ciò implica anche l'esigenza di competenze multidisciplinari: l'Organismo dovrà comprendere le interrelazioni tra rischio legale, operativo e reputazionale, avvalendosi - quando necessario - di consulenti o specialisti interni all'organizzazione. La digitalizzazione dei flussi informativi, l'utilizzo di indicatori di performance ESG e la tracciabilità delle segnalazioni rappresentano strumenti utili per rafforzare la capacità di analisi e di intervento.

Pur in assenza di funzioni operative, l'OdV può svolgere un'importante funzione di impulso culturale, contribuendo a diffondere la consapevolezza che sostenibilità e legalità sono dimensioni complementari della buona gestione. L'Organismo, attraverso il dialogo con gli organi sociali e le funzioni aziendali, può favorire l'evoluzione del Modello 231 in un senso più ampio, tale da rappresentare non solo uno strumento di prevenzione dei reati, ma anche una piattaforma di riferimento per l'etica e la responsabilità d'impresa. Tale contributo, pur nel rispetto della posizione di indipendenza e di non ingerenza, rafforza la cultura del controllo e la credibilità dell'intero sistema di governance.

5.9. Il regime dell'adempimento collaborativo e lo strumento del TCF (Tax Control Framework)

L'inclusione dei reati tributari tra i reati presupposto del D.lgs. 231/2001, già avviata con il D.lgs. 75/2020 e ulteriormente rafforzata dal D.lgs. 87/2024, ha esteso il perimetro della responsabilità amministrativa degli enti e ha reso necessario un presidio strutturato del rischio fiscale. La gestione consapevole di tale rischio si colloca nel più ampio quadro degli obblighi di adeguatezza organizzativa previsti dall'art. 2086 c.c., come modificato dal D.lgs. 14/2019, e si fonda sui principi di corretta amministrazione, trasparenza e tracciabilità dei processi.

In tale contesto, il Tax Control Framework (TCF) - istituito con il D.lgs. 128/2015, successivamente modificato dal D.lgs. 221/2023 e disciplinato dal D.M. 2012/2024 - rappresenta un valido strumento operativo attraverso cui l'impresa struttura la gestione del rischio fiscale, rafforza la compliance tributaria, garantisce la tracciabilità delle operazioni e integra il presidio fiscale nel sistema dei controlli interni e nel Modello. Costruito sulla base della mappatura delle attività e dei processi sensibili, il TCF identifica le aree a rischio fiscale diretto e indiretto e prevede misure quali la segregazione delle funzioni, l'attribuzione di responsabilità, la regolamentazione formalizzata, la tracciabilità dei flussi informativi, controlli di linea efficaci e aggiornamento costante.

Per l'Organismo di vigilanza, il TCF è una fonte informativa utile a leggere processi e flussi che impattano sui rischi reato 231, ai soli fini di verificare l'attuazione dei protocolli e la tracciabilità dei flussi previsti dal Modello. Il ruolo dell'OdV non si esaurisce nella verifica formale dell'esistenza dei presidi, ma si estende alla valutazione della loro concreta attuazione, della loro idoneità a prevenire il

rischio fiscale e della capacità dell'ente di aggiornare tempestivamente il modello in funzione dell'evoluzione normativa e organizzativa.

La valutazione dell'efficacia del TCF da parte dell'OdV si basa su criteri sostanziali e strumenti operativi che garantiscano un presidio strutturato, tracciabile e coerente con il profilo di rischio fiscale dell'ente. Il TCF deve tradursi in protocolli operativi concreti, proporzionati e aggiornabili, costruiti in funzione delle attività sensibili e dei rischi tributari individuati nella mappatura. Tali protocolli devono prevedere l'attribuzione di responsabilità sui processi a rischio, la regolamentazione formalizzata delle attività, la tracciabilità dei flussi informativi, l'efficacia dei controlli di linea e la segregazione delle funzioni, al fine di evitare concentrazioni di potere e conflitti di interesse.

Nel presidio del rischio fiscale, l'OdV collabora in modo strutturato e continuativo con la funzione fiscale, con i consulenti e con i revisori legali, al fine di garantire un monitoraggio efficace del TCF e una vigilanza integrata sul Modello 231. Con la funzione fiscale l'interazione è sistematica e si basa sulla condivisione di aggiornamenti normativi e procedurali, sull'analisi congiunta delle criticità e sull'allineamento rispetto alle misure correttive e ai presidi di controllo. L'OdV può inoltre richiedere evidenze documentali, chiarimenti su anomalie e output di audit, valutando la coerenza tra il TCF e il Modello 231. Tale collaborazione si estende anche alla promozione di attività formative congiunte, rivolte sia ai soggetti apicali che alle funzioni operative, con l'obiettivo di rafforzare la cultura della compliance tributaria e promuovere comportamenti coerenti con i principi di legalità e trasparenza.

Parallelamente, i revisori costituiscono una fonte informativa autorevole a disposizione dell'OdV. Le risultanze delle attività di audit, comprese eventuali non conformità o gap di controllo, vengono condivise e analizzate in chiave 231, consentendo di evitare sovrapposizioni, pianificare interventi coordinati su aree a rischio e integrare le attività di audit nel piano di vigilanza. Le segnalazioni di criticità rilevate dai revisori sono trasmesse all'OdV tramite flussi formalizzati, nel rispetto dei principi di tracciabilità e tempestività. L'OdV, a sua volta, valuta l'impatto delle segnalazioni sul sistema di controllo, attiva eventuali approfondimenti e monitora l'attuazione delle misure correttive, contribuendo così a una governance efficace, integrata e orientata alla prevenzione dei rischi fiscali.

6. L'Organismo di vigilanza nei gruppi societari

6.1. La nomina dell'OdV

Le scarne disposizioni esistenti in materia di "gruppo di imprese" inducono l'interprete a soffermarsi sulle norme dettate in materia di "direzione e coordinamento" (art. 2497 e seguenti del Codice civile), non mancando, ovviamente, di considerare l'art. 2359 dello stesso Codice in tema di società controllate e collegate. Preliminare a ogni valutazione è, tuttavia, la necessaria riflessione sull'impostazione della normativa civilistica, improntata a una concezione atomistica e singola delle società: in altre parole, il "gruppo di imprese", che pure esiste a livello economico, a livello giuridico sconta un deficit definitorio che incide anche sulla disciplina 231 applicabile.

Se le società sono considerate singolarmente, i Modelli di organizzazione, gestione e controllo non possono che essere singoli per società, ritagliati su ogni società e, soprattutto nella Parte Generale di ciascun Modello, idonei a rappresentare compiutamente l'organizzazione societaria della singola società, dando atto del suo inserimento nel gruppo di appartenenza. Tale circostanza, peraltro, non deve confliggere con i principi di autonomia e indipendenza della società stessa, che devono essere chiari ed effettivi e la cui mancanza sostanziale porterebbe a configurare un gruppo solo "apparente", dando luogo e vita a tematiche differenti, che presuppongono differenti impostazioni e comporterebbero ancor più differenti conclusioni, in quanto le società del gruppo sarebbero da considerare, nei fatti, unità organizzative della controllante che, di conseguenza, dovrebbe essere considerata l'unico centro di imputazione della responsabilità da reato *ex* D.lgs. 231/2001.

L'esistenza di questo problema, comunque, impone all'interprete la ricerca di tutti quegli elementi organizzativi che, coordinati tra loro in modo armonioso, permettano di coniugare l'appartenenza a un gruppo con l'autonomia finanziaria e operativa delle singole società del gruppo stesso, al fine di evitare che del reato commesso nell'ambito di una società del gruppo possano essere chiamate a rispondere le altre società, in particolare la capogruppo.

L'evoluzione giurisprudenziale, oltre che dottrinale, consente oggi di considerare consolidato l'orientamento in base al quale la responsabilità dell'ente, di ciascun ente, deve essere dimostrata in concreto e certo non può inferirsi dalla semplice appartenenza a un gruppo.

Ne discende che, in assenza di ingerenza continuativa e sistematica degli apicali di una società (massimamente, la controllante) nella vita della controllata, non si può parlare di un allargamento della responsabilità, prescindendo dall'esame concreto, oltre che dell'interesse o del vantaggio della controllata, anche della sua effettiva operatività.

Se l'assunto di cui sopra è condiviso, ne discende che ogni società, oltre a disporre di un proprio specifico Modello, deve nominare, in relazione alle proprie peculiarità (dimensionali e non solo) un proprio Organismo di vigilanza e ogni componente di quest'ultimo deve essere in possesso di tutti i requisiti previsti per farne parte, tra cui, massimamente, quelli dell'indipendenza (che dovrebbe connotare chiunque sia chiamato a svolgere funzioni di controllo) e della professionalità (anche calibrata sul mercato di riferimento della società).

La nomina degli Organismi deve avvenire ad opera di ciascun organo amministrativo e, pur non esistendo un principio consolidato al riguardo, si ritiene preferibile evitare la costituzione, nell'ambito del gruppo, di un unico OdV con competenze su tutto il gruppo, così come si reputa utile evitare che lo stesso OdV in composizione unica sia formalmente nominato in ogni società.

Questo principio, peraltro, non deve essere spinto fino al punto da considerare necessario che gli OdV delle singole società debbano essere composti da persone sempre diverse, dovendosi ritenere inibita esclusivamente l'ipotesi di OdV di fatto "unici", seppur formalmente propri di ciascun ente facente parte del gruppo. Anzi, la contemporanea presenza di alcune figure in più OdV dello stesso gruppo potrebbe agevolare la conoscenza più completa delle tematiche attinenti al controllo, purché vi sia sempre un'attenzione specifica sulle singole società. Tale conoscenza può essere altresì garantita

mediante l'attribuzione delle funzioni dell'Organismo di vigilanza, anche monocratico, a soggetti riconducibili per funzioni e competenze ad altre società del gruppo (ad es. la capogruppo).

In definitiva, il principio che deve essere salvaguardato è sempre e solo quello dell'autonomia operativa degli Organismi delle singole società, che deve risultare dalla concreta operatività degli stessi e che, soprattutto, deve essere tracciato e documentato, in modo tale da garantire sempre una agevole e completa ricostruibilità degli accadimenti.

6.2. Funzionamento e problematiche condivise

Nei gruppi di società in cui ogni *legal entity* ha adottato il proprio Modello 231 e nominato il rispettivo OdV, si pone la necessità di regolare l'interazione della vigilanza tra l'OdV della società controllante e gli OdV delle società controllate. Tale esigenza assume rilevanza laddove si consideri l'apporto positivo che tali interazioni possono arrecare in termini di efficacia delle attività dei singoli OdV. Un altro aspetto da considerare è l'opportunità di condivisione dell'esperienza dell'OdV di una società con gli altri OdV del gruppo su una determinata criticità riscontrata, che potrebbe consentire l'individuazione di lacune nel sistema di controllo comuni a più società del gruppo.

Alla luce di tali considerazioni, è auspicabile che tra l'OdV della capogruppo e gli OdV delle società controllate – nel rispetto della reciproca autonomia e indipendenza – si instaurino periodici scambi di flussi comunicativi, che potranno essere opportunamente disciplinati all'interno del Regolamento di funzionamento dei singoli OdV (vd. § 6.3).

È altresì auspicabile prevedere incontri periodici congiunti tra l'OdV della capogruppo e gli OdV delle società controllate, con cadenza annuale o semestrale, in cui trattare, tra le altre, le tematiche comuni legate all'attività di vigilanza, le eventuali criticità emerse nel corso del periodo di riferimento, gli aggiornamenti normativi intercorsi e gli orientamenti giurisprudenziali in materia, definendo una metodologia comune, con particolare attenzione al tema del distacco di lavoratori tra società del gruppo. Naturalmente, tale attività non deve comportare alcuna ingerenza nella gestione operativa da parte degli OdV, dovendo piuttosto essere indirizzata esclusivamente alla vigilanza da svolgere insieme alla funzione competente interna alle singole realtà aziendali (ad es. HR).

Ancora, con riguardo alle specifiche esigenze degli OdV delle società controllate di vigilare sui processi sensibili che vengono svolti dalla capogruppo in virtù di contratti *intercompany*, sussiste la tematica afferente alla possibilità di prevedere periodici incontri congiunti tra i responsabili delle funzioni aziendali di riferimento e gli OdV delle società che ricevono il *service*.

Si ribadisce che tali forme di raccordo tra gli OdV delle società del gruppo non devono trasformarsi in ingerenza: ciascun OdV dovrà sempre esercitare le proprie funzioni in totale autonomia e indipendenza, tenendo conto delle esigenze concrete della realtà aziendale in cui svolge i propri compiti.

6.3. Coordinamento tra OdV del gruppo

L'attività di coordinamento tra OdV deve essere puntualmente disciplinata, in quanto è fondamentale un bilanciamento tra le diverse esigenze rilevanti nei vari ambiti.

Da una parte, infatti, l'istituzione di adeguati flussi informativi tra Organismi di vigilanza di società facenti parte del medesimo gruppo di imprese consente di avere una visione globale dei rischi e delle eventuali carenze nel sistema di controllo interno, riuscendo a conseguire anche una maggiore efficacia nell'espletamento delle attività istituzionali attribuite all'OdV dal Decreto 231. La possibilità di interazioni con l'OdV della capogruppo consente, inoltre, agli OdV delle società controllate di sfruttare le maggiori competenze tecniche solitamente allocate a livello della holding.

Dall'altra parte, tale attività di coordinamento deve essere correttamente gestita e svolta in ottica paritetica, per evitare di attribuire un potere di ingerenza o un controllo "di fatto" all'OdV della capogruppo. In tal caso, infatti, si potrebbe incorrere in un duplice rischio: quello di minare l'indipendenza dei singoli Organismi, rendendo dunque inefficace la loro attività di vigilanza e, di conseguenza, l'intero impianto del sistema 231; e quello di "favorire" la risalita della responsabilità alla holding, in ragione di un coinvolgimento diretto di soggetti facenti capo alla stessa in attività di competenza della società controllata.

I flussi comunicativi tra Organismi di vigilanza devono avere finalità conoscitiva, essendo mirati a sottoporre all'attenzione degli Organismi del gruppo aspetti rilevanti per l'efficacia e l'adeguatezza dei sistemi di controllo interni delle società.

Con riferimento all'opportunità di una comunicazione nei confronti dell'OdV della capogruppo, i flussi dovrebbero riguardare:

- la definizione delle attività programmate e compiute;
- le eventuali criticità riscontrate nell'attività di vigilanza;
- i possibili riflessi delle criticità sulle altre società del gruppo;
- le iniziative assunte dai singoli OdV;
- le misure predisposte in concreto.

A titolo esemplificativo, dunque, gli OdV delle società controllate potrebbero inviare all'Organismo della *holding* i macro-ambiti dei piani di vigilanza programmati e gli *highlights* delle relazioni periodiche destinate alla valutazione degli organi amministrativi delle società di appartenenza sulle attività di vigilanza svolte, incluse le eventuali azioni correttive proposte e il *follow up* sul completamento delle stesse.

Quanto ai temi di interesse trasversale a tutte le società del gruppo, potrebbe essere utile mettere a fattor comune:

- l'inventariazione delle attività sensibili, sia specifiche con riferimento a processi di business comuni tra le società, sia trasversali all'interno del gruppo;

- la messa a disposizione di strumenti di controllo unitari, idonei alla rilevazione di eventuali criticità;
- l'utilizzo di applicativi e piattaforme per la gestione dei processi comuni;
- la condivisione di contromisure adottate in caso di violazione del Modello 231, al fine di prevenire situazioni analoghe;
- le linee guida del programma formativo in materia 231.

I menzionati punti di contatto potrebbero avvenire anche in occasione di riunioni congiunte tra gli OdV del gruppo, con cadenza periodica, che potrebbe essere annuale o semestrale, dedicate anche all'esame, per esempio, di:

- recenti novità normative e/o orientamenti giurisprudenziali impattanti in materia di responsabilità amministrativa d'impresa;
- linee guida o documenti di approfondimento emanati dalle associazioni di settore;
- strategie per l'implementazione di un sistema adeguato ai fini del conseguimento di una certificazione;
- interventi o revisioni nei processi gestiti dal gruppo a livello centralizzato;
- formulazione di indirizzi comuni riguardo alle attività di vigilanza;
- programmi di aggiornamento dei Modelli 231 delle società del gruppo, da avviare anche a seguito di una preliminare attività di analisi svolta da parte della capogruppo.

L'attività di coordinamento tra gli OdV del gruppo potrebbe essere "delegata" dalle società controllate alle funzioni centrali della *holding*, al fine di avere una visione integrata delle tematiche comuni, consentendo una maggiore efficacia nel conseguimento di obiettivi unitari e negli scambi informativi tra gli OdV.

In particolare, alla funzione competente per il coordinamento degli Organismi del gruppo potrebbero essere attribuite:

- la formulazione di linee guida riguardo alle attività di vigilanza degli OdV del gruppo;
- il supporto alle attività di modifica e integrazione dei Modelli 231 nell'ottica dell'adozione di una metodologia unitaria di gruppo;
- la creazione di un *repository* di raccolta e aggiornamento dei Modelli 231 delle società controllate, nonché di ulteriori documenti informativi di interesse;
- l'elaborazione di "format" standard utili come basi per la redazione delle relazioni periodiche predisposte dai singoli Organismi per l'organo amministrativo delle rispettive società, con l'obiettivo di armonizzare gli elementi minimi utili nell'ottica del rafforzamento del sistema di controllo interno;
- le informative ad evento aventi ad oggetto eventi giudiziari rilevanti;
- la segreteria societaria per l'organizzazione degli audit e dei controlli.

Potrebbe essere opportuno, infine, indicare anche all'interno del Modello 231 i principi seguiti nell'attività di coordinamento tra gli Organismi di Vigilanza del gruppo.

Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili
Piazza della Repubblica, 59 00185 Roma