AUGUSTO BALDASSARI

COMPLIANCE IN ITALIA

L'ANALISI DI CONFORMITA' LEGALE ED ORGANIZZATIVA DELL'AZIENDA

2023

COMPLIANCE IN ITALIA: L'ANALISI DI CONFORMITÀ LEGALE ED ORGANIZZATIVA DELL'AZIENDA

Come prevenire la responsabilità dell'imprenditore nel dedalo degli adempimenti legali e burocratici

Indice

La conformità in materia di salute e lavoro

La valutazione del rischio e la sua inferenza con le previsioni del d.lgs 231/2001

La conformità in materia di ambiente

Le procedure organizzative

Il modello organizzativo

Gli elementi del modello organizzativo
Identificazione dei rischi potenziali
I protocolli comportamentali nel rapporto con i partners, in particolare

Il sistema integrato della gestione del rischio

L'organismo di vigilanza

La composizione dell'organismo di vigilanza in particolare

La consulenza

L'impresa (o Ente) può disinteressarsi del fatto che un proprio dipendente (anche se di limitati poteri decisionali) abbia commesso un reato che di riflesso avvantaggia l'impresa?
La risposta è di segno negativo, poiché fin dal 2001, con l'entrata in vigore del d.lgs. n. 23, l'impresa ne risponde. In gergo si parla di responsabilità "penale" dell'ente o azienda, ma in modo corretto occorre invece riferirsi alla "responsabilità amministrativa (pecuniaria e interdittiva)" dell'impresa.
Per questo motivo l'imprenditore (o l'ente) deve rivedere il proprio modello organizzativo assicurandosi che:

1) sia conforme, nei vari processi produttivi, alle normative di settore;
2) valuti il rischio di violazioni legali, minimizzandone l'eventualità.

Il rischio di possedere modelli inadeguati e inadatti a prevenire determinati illeciti si definisce "rischio di compliance". E' oramai acquisito che il "*rischio di compliance*", ossia di non conformità alle norme, comporta per le imprese il pericolo di incorrere in sanzioni giudiziarie o amministrative, in perdite finanziarie rilevanti o danni reputazionali in conseguenza di violazioni di norme imperative

ovvero di autoregolamentazione, molte delle quali rientrano nel novero dei reati di cui al d.lgs. 231/2001.[1]
Qui di seguito, mantenendo un approccio schematico e non dottrinale, definiremo l'impatto della responsabilità, configurabili in difetto di compliance, per le imprese, per le associazioni e per gli Enti pubblici o privati.

1. Compliance: la nuova frontiera della consulenza legale ed amministrativa

C'è un termine anglosassone, "*accountability*", che non trova un'esatta traduzione nella nostra lingua, ma interessa sempre di più le imprese ed enti, economici e non, come paradigma della propria regolarità.
Nella complessità di oggi, caratterizzata da un proliferare di norme interne ed europee, regolamenti locali e nazionali e norme tecniche, ogni attività sul campo si confronta col problema della propria conformità alla regola, per evitare ogni tipo di responsabilità.
Il tema è divenuto ancora più stringente con l'introduzione della responsabilità delle persone giuridiche a fronte di alcuni reati piuttosto frequenti dalle cui conseguenze l'impresa si malleva solo a patto di aver previsto per tempo le giuste contromisure.
Accountability, grossomodo significa fare le cose inforcando le lenti del controllore: organizzarsi come se si fosse costantemente esaminati, concetto che, in sostanza, collima con l'autocontrollo e quindi con la massima "conformità" alle norme, alle prassi organizzative ed alla regola d'arte quando si tratta di produrre beni o servizi.
Questa conformità si chiama, mutuando ancora una volta dal dizionario inglese, "*compliance*".
In breve, per una credibile "accountability" (dimostrazione di aver concepito le proprie procedure con la massima responsabilità) è necessaria una corretta "compliance", ovvero una preventiva analisi di conformità dei propri modelli alle regole legali e tecniche vigenti.
Nella complessità del nostro mondo normativo la "compliance" è una attività difficile perché comprende conoscenze multiformi difficilmente abbordabili con le risorse interne all'azienda o all'amministrazione. Privacy, responsabilità amministrativa delle

aziende, sicurezza del lavoro, antiriciclaggio, anticorruzione, regole ambientali, correttezza nelle pratiche commerciali, rapporti con gli agenti di commercio ed altro, sono quindi oggi spesso oggetto di consulenza professionale esterna all'organizzazione aziendale. E' nata così e si sta notevolmente diffondendo la cosiddetta "*compliance consulting*". Vedremo nella seconda parte del testo in quali campi.

2. La necessità di un sistema integrato dei sistemi di gestione: organizzarsi in modo da evitare responsabilita'

Per andare alle origini, possiamo dire che la cosiddetta "*funzione di compliance*" (adeguamento ai vari modelli normativi e tecnici) è nata inizialmente in un sistema molto complesso, come quello della finanza, per poi diffondersi a macchia d'olio, soprattutto nell'ultimo decennio, in settori di minore complessità, anche in concomitanza con la costituzione di Autority di controllo e con la previsione di sanzioni rilevanti in tutto il mondo produttivo di beni e servizi.
In buona sostanza, dotarsi di un sistema di conformità **alle norme non è più solo un fatto etico**, ma rappresenta il **modo di prevenire le sanzioni** che la legge infligge all'impresa (o all'amministrazione) per non avere fatto prevenzione.
Le radici della predetta funzione risalgono agli anni 2000, inizialmente in diretta correlazione con i mercati finanziari. Nei settori creditizi e di investimento, all'epoca, si avvertì l'esigenza di affiancare ad un fisiologico sistema di controlli esterni anche un sistema interno di verifica di "conformità" nell'ambito di una analisi di previsione e minimizzazione dei rischi.[2]
Per agevolare i processi di compliance, nel senso predetto, nello stesso settore – quello finanziario - è intervenuta la Banca d'Italia con una propria direttiva del 12 luglio 2007, intitolata appunto "*Disposizioni di vigilanza: funzione di conformità (compliance)*". Sulla stessa scia e con le medesime finalità di promuovere l'assessment di prevenzione dei rischi ed una organizzazione conforme alle normative, capace anche di svolgere una azione di controllo interno, sono poi stati emanati schemi di riferimento e

direttive anche in ambito CONSOB (per la borsa) e ISVAP (per le attività assicurative).
Ne è seguita prima in quel settore, poi in altri, la proliferazione di "linee guida", direttive e norme tecniche, volte ad agevolare la funzione di *compliance,* divenuta sempre più importante e diffusa per la necessità di adeguarsi ad un sistema stratificato di regole. Il tutto in un contesto articolato, contrassegnato dalle direttive e dai regolamenti UE, dalla normazione nazionale primaria e secondaria ed dagli standards tecnici.
La stratificazione di norme e i relativi adempimenti, la necessità per il soggetto economico di dimostrare a priori di aver valutato i rischi connessi all'esercizio della propria impresa o della propria attività professionale, ha reso centrale l'attività di *compliance* e la relativa consulenza in materia. Questo, a supporto della capacità di esprimere valutazioni basate sulla consapevole gestione dei rischi e di saper tradurre tali valutazioni in modelli organizzativi adeguati a prevenirli.
Niente di astratto, dunque. Anzi, nulla di più concreto: la *compliance* implica la conformità ed il rispetto delle regole, soprattutto di quelle che disciplinano gli aspetti più sostanziali della vita aziendale o professionale.
Per questo sono nate nel tempo – e talvolta imposte direttamente dalla legge – due necessità per l'imprenditore e in parte anche per il professionista:

a) quella di valutare i rischi legali connessi alla propria attività;
b) quella di creare modelli organizzativi e di vigilanza interna, conformi ai paradigmi legali.

Nella "gabbia di norme" che circoscrive l'impresa, l'esenzione di responsabilità è rimessa alla valutazione autonoma dell'imprenditore o del professionista. In altre parole, alla sua *accountability*.

3. **Un po' di casistica:**

Non c'è nulla di più concreto della responsabilità aziendale o professionale, nel momento in cui detta responsabilità si traduce in pesanti sanzioni economiche, se non peggio. Sanzioni che non derivano direttamente dalle attività illecite, ma piuttosto dal non averne previsto un sistema atto a prevenirle. Per usare una banale

metafora non si punisce il furto, ma il fatto di non aver chiuso la porta con la serratura.
Per averne un'idea plastica conviene affidarsi ai casi che hanno fatto registrare le più eclatanti sanzioni, con l'avvertenza, però, che anche in casi di ben minore consistenza tanti imprenditori se la sono dovuta vedere con multe significative di inferiore entità ma di non minore afflittività.

PRIVACY:

- *Qualificato per errore cliente "moroso" da A. spa, società che distributrice l'energia elettrica, Tizio non riesce a passare ad un altro fornitore e perde così il potenziale risparmio derivante dai vantaggi della liberalizzazione del mercato. Si rivolge allora al Garante per la privacy che, al termine di una articolata attività istruttoria, dichiara illecito il trattamento di dati effettuato dal distributore e ingiunge alla società il pagamento di una sanzione di 1 milione di euro. Dagli accertamenti ispettivi svolti dall'Autorità è emerso che l'illecito trattamento ha riguardato altre migliaia di clienti. L'impossibilità per l'utente di cambiare fornitore era derivata da un trattamento di dati inesatti e non aggiornati, dovuto a un disallineamento dei sistemi interni della società che ha comportato l'errata comunicazione in ordine ad una morosità in corso al Sistema informativo integrato (SII), la banca dati consultata dai fornitori prima di sottoscrivere un nuovo contratto (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9834373). Oltre all'erronea applicazione della query per l'estrazione del dato sulla morosità, il Garante ha contestato anche tempistiche inadeguate nella conservazione dei dati, migrazione di dati non esatti nell'ambito dei propri sistemi e inidoneo riscontro all'istanza con la quale il reclamante aveva esercitato i propri diritti. Ad A. E' stata contestata altresì la violazione del principio di accountability, poiché le misure tecniche e organizzative adottate per conformare*

il trattamento dei dati al Regolamento europeo non sono risultate adeguate alla natura, al contesto e ai rischi del trattamento effettuato.

- *Il trattamento di dati biometrici sul posto di lavoro è consentito solo se necessario per adempiere gli obblighi ed esercitare i diritti del datore di lavoro previsti da una disposizione normativa e con adeguate garanzie. Questo il principio ribadito dal Garante che ha sanzionato per 20.000 euro una società sportiva che aveva introdotto un sistema di rilevazione delle impronte digitali per accertare la presenza dei dipendenti presso i club in gestione. L'Autorità è intervenuta a seguito di una segnalazione di un'organizzazione sindacale, che lamentava l'introduzione del sistema biometrico da parte della società, nonostante la richiesta del sindacato di adottare mezzi di rilevazione meno invasivi. Nel corso dell'istruttoria e degli accertamenti ispettivi, effettuati dal Nucleo speciale tutela privacy e frodi tecnologiche della Guardia di Finanza, è emerso che la società aveva effettuato, per quasi quattro anni, la rilevazione delle impronte digitali dei 132 dipendenti senza un'adeguata base normativa.*
- *Se l'utente dice "no" alla telefonata commerciale indesiderata il call center o la società che lo ha contattato deve annotare subito la sua volontà e cancellare il nominativo dalle liste utilizzate per il telemarketing. L'opposizione espressa nel corso della telefonata non deve essere confermata con email o altre modalità, come invece viene spesso richiesto di fare da parte degli operatori, ed è valida anche per le campagne promozionali future. Il principio è stato affermato dal Garante privacy che, al termine di una complessa attività istruttoria, ha rilevato diverse condotte illecite messe in atto da E. E. spa nei confronti di un numero rilevante di utenti. L'Autorità ha quindi ingiunto alla società l'adozione di una serie di misure per mettersi in regola e le ha ordinato il pagamento di una sanzione di 4 milioni e 900 mila euro. (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9857857)*

- *Il legittimo interesse a trattare dati personali per difendere un proprio diritto in giudizio non annulla il diritto dei lavoratori alla protezione dei dati personali. Tanto più se riguarda una forma di corrispondenza, come i messaggi di posta elettronica, la cui segretezza è tutelata anche costituzionalmente. È una delle motivazioni con cui il Garante privacy ha sanzionato un'azienda che, dopo l'interruzione della collaborazione con un'esponente di una cooperativa, ne aveva mantenuto attivo l'account di posta elettronica, prendendo visione del contenuto e impostando un sistema di inoltro verso un dipendente della società. (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9864136)*

SICUREZZA SUL LAVORO:

- *I carabinieri di (...), con il supporto dei loro colleghi del Nucleo Ispettorato del Lavoro di (...), nell'attuazione di un piano di controllo delle attività produttive esercenti nel territorio, hanno proceduto alla verifica di un'attività specializzata nel settore delle confezioni tessili. Durante l'indagine ispettiva si accertava come l'amministratore dell'azienda de quo aveva disatteso l'obbligo d'inviare i propri dipendenti alla visita medica preventiva e/o periodica entro la scadenza prevista dal programma di sorveglianza sanitaria. Si appurava altresì l'omissione di custodia presso la sede di lavoro del documento di valutazione dei rischi. Violazioni, queste, contestate all"amministratore della società, per le quali venivano irrogate sanzioni per un importo complessivo di 5.700 euro circa (CataniaToday 27/5/2020).*

- *La IV Sezione penale della Corte di Cassazione pronunciandosi con sentenza 5975/2020, su un caso di lesioni colpose connesse alla violazione della disciplina dettata in materia di prevenzione antinfortunistica, conferma l'orientamento giurisprudenziale secondo il quale la generica ed insufficiente redazione del documento*

di valutazione dei rischi costituisce addebito di responsabilità per colpa in capo al datore di lavoro allorché si verifica l'evento infausto (lesioni o decesso) in danno dell'infortunato. Nel caso di specie, l'infortunio sul lavoro è stato determinato dal ribaltamento del serbatoio utilizzato come filtro industriale per la depurazione delle acque, che ha tranciato il piede del lavoratore che si accingeva ad entrare nel medesimo al fine di eliminarne dei difetti di saldatura.

- *Con la sentenza n. 18323 del 03.05.2019, la Cassazione ha affermato che il datore di lavoro è da considerarsi responsabile penalmente in caso di infortunio occorso ad un dipendente, qualora il documento di valutazione rischio (DVR) risulti incompleto e non specifico. L'omessa specificità del DVR comporta la responsabilità penale del datore, essendo impossibile per l'azienda mettere in campo un'adeguata politica antinfortunistica senza la piena consapevolezza dei pericoli insiti nelle lavorazioni. Nella fattispecie, il lavoratore – mentre era intento ad effettuare un taglio con impegno di fiamma ossidrica – omettendo di accertarsi che nelle vicinanze non vi fosse materiale infiammabile, determinava l'innesco di fiamme che si propagavano da un fusto in cui vi erano residui di diluente e si cagionava, così, ustioni in varie parti del corpo con prognosi superiore a 40 giorni. In conseguenza di ciò, l'amministratore unico della società datrice, in qualità anche di rappresentante del servizio di sicurezza e protezione, è'stato condannato – limitatamente al profilo di colpa di cui all'art. 29 D.Lgs. 81/2008 – per non aver effettuato una valutazione del rischio connesso allo svolgimento di attività lavorative con impegno di prodotti infiammabili.*

RESPONSABILITA' DELLA SOCIETA' IN CASO DI REATI (d.lgs. 231/2001)

- *Secondo la Cassazione Penale, Sez. 4, 10 marzo 2023, n. 10143, la responsabilità dell'ente sussiste anche quando*

l'autore del reato non è stato identificato. Rammenta la Corte come in tema di responsabilità da reato degli enti ex d.lgs. n. 231 del 2001 la Suprema Corte abbia stabilito che all'assoluzione della persona fisica imputata del reato presupposto per una causa diversa dalla rilevata insussistenza di quest'ultimo non consegua automaticamente l'esclusione della responsabilità dell'ente per la sua commissione, poiché tale responsabilità, ai sensi del d.lgs. n. 231 del 2001, art. 8, deve essere affermata anche nel caso in cui l'autore del suddetto reato non sia stato identificato (Sez. 5, n. 20060 del 04/04/2013).

- *Con la sentenza* Sez. 4, 20 ottobre 2022, n. 39615 *la Cassazione ha definito la natura della responsabilità degli Enti che, secondo la Corte può essere definita come una vera e propria responsabilità da colpa di organizzazione, caratterizzata dal malfunzionamento della struttura organizzativa dell'ente, la quale dovrebbe essere volta – mediante adeguati modelli – a prevenire la commissione di reati. Le Sezioni Unite hanno infatti al riguardo affermato che, in tema di responsabilità da reato degli enti, la colpa di organizzazione, da intendersi in senso normativo, è fondata sul rimprovero derivante dall'inottemperanza da parte dell'ente dell'obbligo di adottare le cautele, organizzative e gestionali, necessarie a prevenire la commissione dei reati previsti tra quelli idonei a fondare la responsabilità del soggetto collettivo, dovendo tali accorgimenti essere consacrati in un documento che individua i rischi e delinea le misure atte a contrastarli (Sez. Un., n. 38343 del 24 aprile 2014). La Corte ha ritenuta provata la responsabilità della società S,G., condannandola alla sanzione amministrativa pari a 200 quote dell'importo di euro 500 ciascuna per un importo complessivo di euro 100.000,00 oltre le spese. La società era stata tratta a giudizio per rispondere dell'illecito amministrativo di cui agli artt. 5 e 25 septies d.lvo 231/2001 in relazione alle lesioni colpose patite da un dipendente della società a seguito della violazione delle*

norme poste a tutela della sicurezza sul lavoro. Il sinistro era avvenuto in occasione di un'operazione di sostituzione di un nastro trasportatore finalizzato a fare confluire materiale per la fusione all'interno di un silos.

- *La vicenda – relativa alla sentenza della Cassazione Penale, Sez. 3, 20 gennaio 2022, n. 2234 – si riferisce all'inquinamento del suolo e del sottosuolo verificatosi nell'arco temporale di due mesi nel territorio del Comune di (omissis), a causa di reiterate perdite di idrocarburi avvenute all'interno del complesso industriale della A. S.P.A., e, precisamente, nel suolo sottostante il serbatoio (omissis), posto nell'(omissis) del parco citato. La dinamica dell'evento è stata ricondotta alla perdita di "light catalytic naphtha" dal sistema delle tubature del serbatoio (omissis). Agli imputati, nei rispettivi ruoli ricoperti in seno all'azienda, venivano contestati al capo i reati di inquinamento e omessa bonifica ai sensi dell'art. 110 c.p., d.lgs. n. 152 del 2006, art. 257, commi 1 e 2 ed altri reati ambientali. Alla A. S.P.A. venivano contestati gli illeciti amministrativi di cui al d.lgs. n. 231 del 2001, art. 25 undecies, comma 2, lett. d), n. 2 e all'art. 25 undecies, comma 2, lett. c), n. 2. Sul punto la Corte ha stabilito che come noto, il d.lgs. n. 231 del 2001, inserito nell'ordinamento italiano in forza di fonti normative internazionali e comunitarie, disciplina la responsabilità amministrativa degli enti collettivi per i fatti costituenti reato. Questo modello di responsabilità, originariamente previsto con riguardo ad un ristretto novero di reati presupposti, è stato poi progressivamente esteso, con l'inserimento dell'art. 25 undecies, da parte del l.lgs. 7 luglio 2011, n. 121, e con la successiva, L. 22 maggio 2015, n. 68, ad una più ampia serie di reati inclusivi anche delle fattispecie poste a tutela dell'ambiente, tra le quali, tuttavia non si rinviene l'art. 6, lett. a) e d) citato.*

MERCATO E CONCORRENZA SLEALE

- *L'Autorità Garante della Concorrenza e del Mercato ha adottato un provvedimento cautelare nei confronti delle società T. s.r.l. e P. C. s.r.l., che operano, rispettivamente, tramite i domini (…) e (….). L'intervento dell'Antitrust segue gli accertamenti d'ufficio e le numerose segnalazioni di consumatori che lamentavano di aver effettuato acquisti online su questi siti internet senza però ricevere i prodotti acquistati, né il rimborso di quanto pagato, né altra forma di assistenza. Per questo l'Autorità aveva comunicato alle società l'avvio di un procedimento istruttorio e del sub-procedimento cautelare considerando i presupposti di attualità e pericolosità delle condotte ancora in corso. T. s.r.l. e P. C. s.r.l. non hanno inviato alcuna memoria o documento a propria difesa e dunque l'Autorità ha ordinato, in via cautelare, la sospensione delle condotte illecite che consistono perlopiù nella mancata consegna dei prodotti acquistati e nell'assenza di assistenza o di rimborsi ai consumatori. Con lo stesso provvedimento, l'Autorità ha ordinato che sia inibito l'accesso ai siti internet (…) e (…) perché strumentali proprio alle condotte illecite e per questo ha chiesto la collaborazione del Nucleo Antitrust della Guardia di Finanza (nota stampa AGCM 7/3/2023).*

- *L'Autorità Garante della Concorrenza e del Mercato ha sanzionato per complessivi 5.250.000 euro la società Y. S.p.A. L'istruttoria dell'Antitrust ha consentito di accertare la scorrettezza di alcuni comportamenti attuati attraverso il sito di* e-commerce *(omissis) nell'ambito dell'attività di vendita online di capi d'abbigliamento, di calzature e di altri beni di moda, lusso e design, nel periodo 2019-2022. In particolare, la società ha annullato unilateralmente gli ordini online già perfezionati dai consumatori in caso di superamento di determinate soglie di resi, <u>omettendo contestualmente l'informativa sul blocco degli acquisti</u>. Inoltre, ha prospettato in modo ingannevole i prezzi di vendita dei prodotti e gli sconti effettivamente applicati. Per quanto riguarda la prima pratica, secondo l'Autorità è emersa una*

specifica **policy** ***aziendale interna*** *che prevede – senza informare prima o dopo i consumatori – l'inibizione della possibilità di effettuare ulteriori acquisti nel caso di superamento di determinate soglie di resi, limitando così il diritto di recesso. In riferimento alla seconda pratica, invece, l'Autorità ha ritenuto che Y. Abbia indotto i consumatori ad aderire alle proprie offerte online sulla base della prospettazione di prezzi e di sconti ingannevoli. Ad esempio, si è accertato che, prima del 1° febbraio 2022, a seguito dei frequenti* repricing*, il prezzo finale scontato di alcuni prodotti – in occasione di particolari promozioni – risultava sostanzialmente analogo al prezzo effettivamente praticato nel periodo precedente la promozione, in quanto veniva modificato il prezzo di riferimento rispetto al quale veniva poi applicato lo sconto.*

- *Durante una prima visita a domicilio, la società induceva il consumatore con modalità ingannevoli a firmare un modulo che lo vincolava all'acquisto, rassicurandolo che invece non c'era alcun obbligo, senza peraltro informare dell'esistenza del diritto di recesso. L'Autorità Garante della Concorrenza e del Mercato ha chiuso il procedimento nei confronti di I. S.r.l.s. con una sanzione di 50mila euro perché ne ha ritenuto la condotta ingannevole, omissiva e aggressiva. Secondo quanto ricostruito dall'Autorità, la società contattava telefonicamente i consumatori prospettando loro la visita a domicilio di un agente per la consegna di un catalogo di prodotti, di buoni e/o di tessere per ottenere sconti. Nel corso della visita gli agenti inducevano il consumatore – con modalità ingannevoli – a sottoscrivere un modulo, rassicurandolo sull'assenza di obblighi di acquisto, senza fornire informazioni sull'esistenza del diritto di recesso né sulle condizioni per esercitarlo. In realtà la sottoscrizione del modulo vincolava all'acquisto – nell'arco di tre anni – di prodotti presenti nel catalogo della società, di costo compreso fra 3.990 euro e 6.990 euro.*

RICICLAGGIO:

- *Le operazioni finalizzate ad impedire in modo definitivo oppure a rendere difficoltoso l'accertamento in merito alla provenienza di denaro, beni oppure altre utilità, integrano l'illecito di riciclaggio. Il reato si configura anche nelle ipotesi di versamenti di denaro, di provenienza illecita, a favore di società controllate dall'imputato, attraverso l'utilizzo di "conti di sponda". È quanto stabilito dalla Corte di Cassazione nella sentenza n. 48288/15.*
- *Il reato di riciclaggio di cui all'art. 648-bis c.p. è integrato non soltanto dalle condotte tipiche di sostituzione o trasformazione del bene di origine illecita ma, altresì, secondo la testuale dizione contenuta nella norma* "da *ogni altra operazione diretta ad ostacolare l'identificazione dell'origine delittuosa del bene"***.** *Sul punto, la giurisprudenza di legittimità ha avuto modo di precisare che la disposizione di cui all'art. 648-bis, richiede, pur essendo a forma libera, che le attività poste in essere sul denaro, bene o utilità di provenienza delittuosa, siano specificamente dirette alla sua trasformazione parziale o totale, ovvero siano dirette ad ostacolare l'accertamento sull'origine delittuosa della* res*, anche senza incidere direttamente, mediante alterazione dei dati esteriori, sulla cosa in quanto tale. Tali assunti sono stati richiamati dalla Corte di cassazione, nel testo della sentenza n. 9533 del 21 marzo 2022, nel confermare la condanna impartita ad un soggetto, accusato del reato di riciclaggio riferito a un cane di provenienza illecita.*

SISTEMI INFORMATICI:

- *PA e imprese devono prestare la massima attenzione nell'impostazione e gestione dei sistemi di whistleblowing, garantendo la massima riservatezza dei dipendenti e delle altre persone che presentano segnalazioni di condotte illecite. Lo ha ribadito il Garante per la privacy che ha sanzionato un'azienda ospedaliera e la società*

informatica che gestiva il servizio per denunciare presunte attività corruttive o altri comportamenti illeciti all'interno dell'ente. L'accesso all'applicazione web di whistleblowing, basata su un software open source, avveniva attraverso sistemi che, non essendo stati correttamente configurati, registravano e conservano i dati di navigazione degli utenti, tanto da consentire l'identificazione di chi la utilizzava, tra cui i potenziali segnalanti.
(https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9768702).

- *Il Garante privacy ha sanzionato una società di servizi di messaggistica con una multa di 80mila euro per aver conservato illecitamente il contenuto degli sms inviati dai propri clienti (circa 7.250 utenze). Alla società sono state inoltre contestate altre condotte illecite relative in particolare alle misure adottate per garantire la sicurezza del trattamento dei dati di traffico telematico e l'assenza di una base giuridica per effettuare controlli antifrode. L'Autorità, nel corso degli accertamenti ispettivi avviati a seguito di una segnalazione e di un reclamo, ha rilevato che il contenuto integrale dei messaggi inviati dai clienti (in genere persone giuridiche) era conservato senza che questi avessero espressamente acconsentito.*

ANTICORRUZIONE

- *L'omessa adozione del Piano triennale di prevenzione della corruzione ha comportato per i vertici di un importante Comune sardo un procedimento sanzionatorio da parte di Anac. L'Autorità Nazionale Anticorruzione ha irrogato una sanzione pecuniaria complessiva pari a 7000 euro ai responsabili dell'ente, sanzione che dovrà essere saldata personalmente dagli stessi amministratori, per mille euro ciascuno. L'indagine di verifica di Anac ha portato ad accertare una mancata pubblicazione annuale del Piano sul sito istituzionale, violando così l'obbligo di adozione, con relative inadempienze nella sezione Amministrazione Trasparente.*

Quelli che precedono sono solo alcuni esempi estrapolati da decisioni delle varie autorità garanti – tanto per avere un'idea - senza soffermarsi invece sulle responsabilità penali in merito alle quali si è stratificata una giurisprudenza purtroppo molto copiosa.

4. Il principio di accountability: organizzazione, procedure e controlli

Dagli esempi sintetizzati nel paragrafo che precede è facile comprendere che il moderno sistema di responsabilità aziendale e professionale si basa su tre presupposti fondamentali:

a) l' "accountability", vale a dire la necessità di una razionale previsione del rischio legale;
b) la conformità al quadro normativo fatto non solo di norme imperative ma anche, e sempre di più, da determinazioni della pubblica amministrazione, da circolari e prassi che insieme costituiscono il modello legale di riferimento;
c) il modello organizzativo ed il relativo sistema di vigilanza interna.

Questi tre presupposti rappresentano il minimo comune denominatore del rispetto di tutti gli obblighi legali nei vari settori di responsabilità dell'imprenditore ed in parte del professionista e, al tempo stesso, uno "scudo" rispetto all'esito dei controlli della pubblica amministrazione.
Non solo, ma si tratta di elementi interconnessi in una continuità funzionale unitaria. Potremmo immaginarli, insomma, come fasi di un medesimo processo di assestamento dell'azienda rispetto ai propri obblighi legali.

La prima fase è rappresentata da una valutazione del rischio (in tema di tutela dei dati personali, di attenuazione della responsabilità per reati commessi dai dipendenti, di rischi connessi al mercato e alla concorrenza, di riciclaggio e così via), che in altri termini viene appunto indicata come *accountability*. Non solo, ma affrontare rischi ed opportunità costituisce anche la base per accrescere l'efficacia del sistema di gestione per la qualità, ottenendo migliori risultati e

prevedendo e superando gli accadimenti negativi. Una volta valutato il rischio l'imprenditore sarà libero di approcciare ad esso in modo più o meno codificato. Ma la codificazione, cioè la traduzione delle contromisure in un modello organizzativo interno, consentirà non solo di prevenire eventuali responsabilità legali, ma anche di dimostrare, in sede di controllo o di contenzioso, di aver fatto la gestione del "buon padre di famiglia".

Da una corretta accountability deriva la necessità di uniformare la propria organizzazione al quadro normativo, considerato nel senso più esteso e cioè costruito sul rispetto della legge, ma anche delle prassi, delle linee guida, della normativa tecnica e degli orientamenti della pubblica amministrazione. La conformità di cui trattasi richiede una particolare conoscenza delle norme e prassi che definiscono i vari modelli di responsabilità. Per fare qualche esempio concreto, in tema di concorrenza non basta conoscere la norma ma occorre conoscere l'orientamento dell'antitrust nell'interpretarla in concreto; in tema di privacy occorre conoscere le numerose determinazioni del garante; in materia di corruzione è necessario conoscere le linee guida per costruire un modello di prevenzione adeguato; altrettanto dicasi in tema di ambiente e di anticorruzione. Per sintetizzare, possiamo dire che in questa fase, come nella fase di valutazione del rischio che la precede, è fondamentale la conoscenza dell'universo normativo che informa ogni settore di responsabilità.

L'ultima fase riguarda l'adeguamento dell'organizzazione, ovvero, a seconda della profondità dell'intervento, l'adeguamento delle regole aziendali, dei processi decisionali, delle responsabilità interne, dei regolamenti aziendali e di sistemi di reazione rispetto alle criticità. Si pensi, per dare concretezza al discorso, ad una sottrazione di dati dai sistemi gestionali dell'azienda ed alla necessità di una tempestiva identificazione degli stessi per una altrettanto tempestiva – doverosa – segnalazione all'Autorità Garante. Oppure si pensi molto più banalmente alla corretta gestione della posta elettronica aziendale secondo i dettami delle leggi sulla privacy. Ma altri esempi potrebbero essere fatti sulla regolamentazione dei processi decisionali interni per mallevare l'impresa dalle pesanti sanzioni previste dal d.lgs. 231/2001 per i reati commessi dai dipendenti. Messa a punto l'organizzazione interna, i codici di condotta e le

regole interne occorre poi prevedere degli idonei meccanismi di verifica atti a garantire la tenuta del sistema.
Possiamo schematizzare il discorso in merito alle responsabilità e al dovere (sanzionato) di prevenirle dicendo che:

a) gran parte di tali responsabilità si inquadrano nelle previsioni della d.lgs. 231/2001 perché conseguono a reati commessi da soggetti legati all'azienda da un rapporto di dipendenza. Ovviamente la responsabilità penale è personale, ma la condotta illecita si riverbera in una responsabilità amministrativa dell'azienda qualora non siano state adottate misure atte a prevenire. Per essere più chiari, l'azienda si malleva dalla responsabilità se il dipendente abbia commesso il reato forzando le regole di prevenzione interne.

b) Esistono altre fonti di responsabilità non legate all'ambito penale, come per la violazione della disciplina della privacy, o della concorrenza sul mercato, le quali devono essere parimenti attenuate attraverso un modello organizzativo e policy aziendali di prevenzione.

5. La conformità alla normativa sulla responsabilità dell'azienda per reati commessi dagli amministratori e dipendenti (d.lgs. n. 231/2001)

Cos'è*:*

Il d.lgs. 8 giugno 2001, n. 231 prevede la "responsabilità amministrativa delle società e degli enti collettivi" per reati commessi nel loro interesse o vantaggio.

Quali sono i rischi:
Il sistema sanzionatorio previsto dal d.lgs. 231/2001 prevede, in relazione ai reati commessi nell'interesse a vantaggio della persona giuridica diversi tipi di sanzione:

a) sanzione pecuniaria fino ad €. 1,5 milioni

b) sanzione interdittiva della confisca del profitto illecito; della pubblicazione della sentenza di condanna; dell'interdizione dall'esercizio dell'attività; della sospensione o revoca delle

autorizzazioni, licenze o concessioni che sono state funzionali alla commissione dell'illecito; divieto di contrattare con la pubblica amministrazione; esclusione da agevolazioni, finanziamenti, contributi e sussidi o revoca di quelli già ottenuti; divieto di pubblicizzare beni o servizi.

Le misure interdittive incidono pesantemente sul futuro dell'attività imprenditoriale. Per alcune fattispecie legate alle ipotesi di corruzione, qualora il reato sia stato commesso da soggetti in posizione apicale, le misure interdittive possono avere una durata compresa tra i 4 ed i 7 anni, mentre possono durare tra i 2 e i 4 anni se l'illecito è stato commesso da un sottoposto.

Le misure interdittive di cui trattasi, peraltro, che esse possono essere applicate anche a titolo di "misura cautelare" cioè in epoca antecedente alla sentenza di condanna.

I reati che espongono l'ente alle sanzioni per responsabilità amministrativa:

In ordine ai reati previsti va precisato che gli stessi sono fonte di responsabilità della persona giuridica o dell'ente se a commetterli è un soggetto:

a) in posizione apicale;

b) in posizione subordinata sottoposto alla direzione ed alla vigilanza del datore di lavoro.

Il novero di reati che danno luogo alla responsabilità amministrativa ed alle conseguenti sanzioni è tassativamente indicato dal d.lgs. 231/2001.

Li elenchiamo qui di seguito:

- indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o dell'unione europea o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture;
- delitti informatici;
- delitti di criminalità organizzata;
- peculato, concussione, induzione indebita, corruzione e abuso d'ufficio;
- falsità in monete, in carte di pubblico credito, in valori di bollo o in strumenti o segni di riconoscimento;

- delitti contro l'industria in commercio;
- reati societari;
- delitti con finalità di terrorismo o di eversione dell'ordine democratico;
- pratiche di mutilazione degli organi genitali femminili;
- delitti contro la personalità individuale;
- abusi di mercato;
- omicidio colposo lesioni gravi o gravissime commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro;
- ricettazione, riciclaggio, autoriciclaggio e reimpiego;
- delitti in materia di strumenti di pagamento diversi dai contanti;
- delitti in materia di violazione del diritto d'autore;
- induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria;
- reati ambientali;
- impiego di cittadini dei paesi terzi il cui soggiorno è irregolare;
- reati di razzismo e xenofobia;
- frode in competizioni sportive, esercizio abusivo di gioco e scommesse;
- reati tributari;
- contrabbando
- delitti contro il patrimonio culturale;
- riciclaggio di beni culturali e devastazione saccheggio di beni culturali e paesaggistici;

Cosa occorre fare per non risponderne:

Il d.lgs. 231/2001 prevede che la persona giuridica non risponde per responsabilità amministrativa conseguente ad un reato commesso dal proprio rappresentante, soggetto apicale o dipendente, nel caso dimostri di avere adottato e correttamente attuato, prima della commissione del reato stesso, un valido "**modello di organizzazione, gestione e controllo**" idoneo a prevenire simili fatti.

Come deve essere costruito il modello di organizzazione, gestione e controllo:

La legge e le prassi in materia descrivono le caratteristiche essenziali del modello di organizzazione, gestione e controllo.

- **a)** L'individuazione delle aree di rischio, tecnicamente definite "aree sensibili": cioè la selezione le attività più esposte al rischio di condotte penalmente sanzionabili.
- **b)** La predisposizione di specifici protocolli diretti a disciplinare e programmare l'assunzione e l'attuazione delle decisioni in "area sensibile";
- **c)** Produzione di "policy" per informare i dipendenti sulle corrette prassi interne, conformemente a quanto indicato nel Modello Organizzativo;
- **d)** Individuare le modalità di gestione delle risorse finanziarie in modo da prevenire la commissione di reati mediante il loro utilizzo;
- **e)** Prevedere una griglia di obblighi di informazione confronti dell'organismo di vigilanza;
- **f)** Introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure previste nel modello;
- **g)** Prevedere canali di segnalazione a favore dell'Organismo di Vigilanza;
- **h)** Costituire un organismo di vigilanza.

Le piccole imprese

Le piccole imprese o gli enti di minore rilevanza non sono esenti dagli obblighi previsti dal d.lgs. 231/2001. L'unica eccezione risiede ne fatto che tali enti sono esentati dal dover costituire l'Organismo di Vigilanza, poiché i compiti assegnati a detto organismo possono essere svolti direttamente dal vertice della persona giuridica. Ovviamente, la dimensione ridotta dell'ente condiziona le previsioni contenute nel modello organizzativo le quali sono inevitabilmente correlate alla complessità dei sistemi.

Qui di seguito analizziamo alcune delle aree di rischio sulle quali è fondamentale creare adeguati modelli organizzativi

ed integrarli con quelli eventualmente già presenti nell'azienda.

---

6. La conformità alla normativa sul trattamento dei dati personali (privacy)

Cos'è:

La responsabilità amministrativa delle persone giuridiche non si limita solo alle ipotesi di reati commessi da personaggi di vertice o dipendente, ma per talune materie si configura per la violazione di specifiche discipline. A sanzionare dette violazioni provvedono le varie autorità di garanzia istituite *ratione materie*.
E' il caso della violazione delle regole sul trattamento dei dati personali (semplificando sulla privacy) sanzionato ad opera di una specifica Autorità Garante.
I Compiti del Garante sono definiti dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101, oltre che da vari altri atti normativi italiani e internazionali.
Secondo il citato Regolamento Europeo, la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Definizioni:

Per «dato personale» si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati

relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Si dice «trattamento» qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
E' «titolare del trattamento» la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali, mentre è «responsabile del trattamento» la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Le misure di "accountability" e le responsabilità del titolare e dei suoi dipendenti:

Le rilevanti sanzioni pecuniarie irrogate dall'Autorità Garante non riguardano solo le condotte illecite, ma trovano fondamento soprattutto sulla valutazione negativa circa le misure preventive che il titolare è obbligato a prevedere per mallevarsi dalla responsabilità.
Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.
Il primo fra tali criteri è sintetizzato dall'espressione inglese *"data protection by default and by design"*, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei

titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**
Il principio di base su cui si fonda la disciplina è quello della autorizzazione al trattamento, cui corrisponde un dovere di legittima custodia e di corretto trattamento.
Pertanto il processo di accountability, preceduto dalla valutazione del rischio, impone in primis un sistema di protezione delle banche dati, e poi che, tanto il titolare, quanto suoi dipendenti, rispettino delle precise regole comportamentali.
Tutto questo si risolve in una preventiva verifica dei sistemi e in una precisa produzione di policy e deleghe interne da parte del titolare.

Le sanzioni:

L'Autorità garante si avvale di organismi di controllo, e prevalentemente della Guardia di Finanza.
A fronte di una infrazione chi la commette, cioè il titolare del trattamento (imprenditore o soggetto privato o anche pubblico) è soggetto a sanzioni amministrative pecuniarie fino a 20 milioni di €. o, per le imprese, fino al 4 % del fatturato totale annuo dell'esercizio precedente, se superiore.
Le violazioni riguardano:

- **a)** i principi di base del trattamento, comprese le condizioni relative al consenso;
- **b)** i diritti degli interessati;
- **c)** i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale;
- **d)** qualsiasi obbligo ai sensi delle legislazioni degli Stati membri;
- **e)** l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.

7. Conformità antiriciclaggio

Cos'è:

Il riciclaggio di denaro è il reinvestimento di capitali illeciti in attività lecite. In altri termini il denaro sporco, tramite una serie di passaggi che possono involgere anche i professionisti, viene lavato e impiegato nei settori immobiliare, imprenditoriale e finanziario.
Il rischio relativo ai casi di riciclaggio si configura con maggiore intensità per alcune categorie professionali (Notai, Commercialisti) o nell'ambito creditizio (Istituti Bancari), ma non ne vanno esenti anche le imprese nel rapporto con la propria clientela e nell'ambito della formazione del bilancio.

Quali sono i rischi:

L'impianto punitivo riguardante gli obblighi di adeguata verifica antiriciclaggio è sancito negli artt. 55 e ss. del **d.lgs. 231/2007** con sanzioni sia a carattere penale che amministrativo.
L'art. 55, c. 1, punisce con la reclusione da 6 mesi a 3 anni e la multa da 10.000 a 30.000 euro la falsificazione di dati, informazioni e ogni altro elemento relativo al cliente, al titolare effettivo e all'esecutore dell'adeguata verifica, nonché delle informazioni relative allo scopo ed all'an della prestazione professionale ed alla natura dell'operazione stessa. Ad essere sanzionato non è solo il falsificatore ma anche chi ne fruisce.
Alla stessa pena soggiace chi acquisisce o conserva dati falsi ovvero informazioni non veritiere sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto professionale e sulla prestazione. E' altresì rilevante – e sanzionata nei citati termini – la condotta di chi utilizza mezzi fraudolenti al fine di pregiudicare una corretta conservazione dei dati e delle informazioni. In questo caso il soggetto attivo individuabile è la persona fisica che è tenuta agli obblighi di conservazione.
Quanto detto vale in generale ma, come accennato, il d.lgs. 231/2007 prevede specifici obblighi di verifica da parte di professionisti appartenenti a determinate categorie, come i notai, i commercialisti, gli avvocati e da parte degli istituti finanziari.
A tale obbligo di verifica corrisponde un correlato obbligo di segnalazione delle operazioni sospette alle autorità preposte. Il comma 4, dell'art. 55 citato al fine di tutelare le comunicazioni, sanziona la violazione del divieto di comunicazione dell'effettuata

segnalazione di operazione sospetta e di comunicazione sul flusso di ritorno delle informazioni richiamando gli artt. 39, c. 1, e 41, c. 3 del D. Lgs. 231/2007.
Con riferimento alle sanzioni amministrative il decreto se ne occupa negli artt. 56-59 punendo con la sanzione pecuniaria di 2.000 euro – salvo il caso di violazioni gravi, reiterate, plurime ovvero sistematiche per cui la sanzione si colloca tra un minimo di 2.500 ed un massimo di 50.000 euro – l'inosservanza degli obblighi di adeguata verifica e astensione e l'inosservanza degli obblighi di conservazione. Viene punita invece con la sanzione amministrativa pecuniaria da 5.000 a 30.000 euro calcolata a persona, la violazione degli obblighi di comunicazione degli organi di controllo.
L'omessa segnalazione di operazioni sospette viene invece sanzionata in via residuale, ossia salvo il fatto non costituisca reato, con la pecuniaria ammontante a 3.000 euro che, in caso di violazioni gravi, reiterate, plurime o sistematiche, è determinata tra un minimo di 30.000 ed un massimo di 300.000 euro. La sanzione grava sull'azienda ma anche sulle persone che hanno commesso l'omessa segnalazione. Nel caso in cui l'omissione porti un vantaggio economico determinato o determinabile in un valore inferiore o pari a 450.000 euro la sanzione si aumenta sino al doppio, mentre nel caso in cui il vantaggio non sia determinato o determinabile la sanzione può raggiungere fino il milione di euro.

Le linee della Guardia di Finanza:

La Guardia di Finanza è l'autorità di vigilanza in materia di antiriciclaggio sulle libere professioni. In ragione di detta funzione il predetto Ente ha emanato diverse circolari esplicative e applicative. Tra queste riveste una particolare rilevanza la Circolare n. 83607/2012 in seguito integrata dalla Circolare n. 0210557/2017. In applicazione di tali direttive si è formata una prassi che costituisce il livello minimo di cautele da osservare per evitare l'irrogazione di sanzioni. La Guardia di Finanza riferisce le proprie linee a seconda che il professionista abbia optato per un differente tipo di verifica (semplificata, indiretta, rafforzata ed ordinaria).
Nel caso in cui il professionista abbia optato per una verifica rafforzata gli operatori della Guardia di Finanza accertano che siano state attuate tutte le prescrizioni di cui all'art. 24, D. Lgs. 231/2007.

In specie rileva se, non essendo comparso fisicamente il cliente all'atto dell'identificazione, ne sia stata verificata correttamente l'identità attraverso il ricorso a documenti, dati o informazioni supplementari, se siano state adottate ulteriori misure per la verificazione dei documenti forniti e, infine, se il primo pagamento della prestazione professionale ovvero dell'operazione sia stato effettuato per mezzo di un conto corrente del cliente tenuto presso un istituto di credito. Nel caso invece la verifica sia stata rafforzata in ragione del cliente persona politicamente esposta l'accertamento mira a controllare se l'avvio del rapporto professionale sia stato autorizzato e siano state adottate tutte le misure idonee per stabilirne la fonte sia del patrimonio che dei fondi che sono stati utilizzati. Si verifica poi che durante l'intero rapporto professionale sia stato effettuato un controllo continuo.
In tutti gli altri casi non contemplati da quanto specificato sopra il professionista attua una verifica di tipo ordinario. Nel controllo l'Authority procede ad esaminare l'allineamento della procedura di verifica seguita dall'obbligato con i precetti normativi dell'art. 19 D. Lgs. 231/2007, in primo luogo indagherà in ordine agli adempimenti relativi all'identificazione e verifica del cliente e del titolare effettivo in punto a tempistica ed esecuzione e, successivamente, alle modalità di esecuzione.

La verifica della clientela

Il nuovo assetto valutativo, attuato con il D. Lgs. 90/2017, segue l'approccio *know your customer (KYC)* che delinea una *due diligence finanziaria* complessa basata sulla valutazione del rischio di profilo soggettivo e di profilo oggettivo. Il primo riguarda il cliente e ne esamina la natura giuridica, l'attività prevalentemente svolta, l'area geografica di residenza o sede, nonché il comportamento tenuto al momento dell'operazione. Il secondo si riferisce all'operazione, individuandone il tipo, la modalità di svolgimento, l'ammontare, l'area geografica di destinazione del prodotto e, valutati in rapporto all'attività svolta dal cliente, la frequenza, il volume e la ragionevolezza dell'operazione.

8. **Conformità anticorruzione**

Il 16 gennaio 2019, sulla gazzetta ufficiale è stata pubblicata la c.d. **legge anticorruzione** intitolata "*misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*".
La citata normativa riguarda la corruzione nell'ambito della pubblica amministrazione e cioè si inserisce nell'articolata disciplina dei reati contro la pubblica amministrazione.
L'**art. 2635 c.c.** prevede, invece, il delitto di **corruzione tra privati** il cui rischio è aumentato nell'attuale contesto economico, il quale favorisce l'esternalizzazione delle funzioni ed il decentramento delle fasi produttive, con la conseguente frammentazione delle attività nel suo complesso.
Sebbene inizialmente la condotta di cui all'art. 2635 citato non fosse contemplata tra i reati presupposto della responsabilità dell'impresa, il nuovo l'art. 25 ter, d.lgs. 231/2001 ha introdotto la corruzione tra privati tra i reati fonte della responsabilità amministrativa per l'impresa. L'impianto sanzionatorio è poi stato inasprito ad opera del d.lgs. n. 38/2017 in esecuzione della *decisione quadro* 2003/568/GAI del consiglio UE anche per gli enti.
In tema di corruzione tra privati, occorre tuttavia – ai fini della responsabilità dell'impresa, tracciare la distinzione tra "corruzione attiva" e "corruzione passiva".
La corruzione privata nella sua **forma attiva** viene ora punita con la sanzione pecuniaria pari a un minimo di 400 quote fino a un massimo di 600.
Si parla di forma attiva quando il corruttore, appartenente alla società, operi nell'interesse della stessa. In questo caso sorge anche la responsabilità amministrativa dell'impresa quando il caso sia commesso da un soggetto che svolga genericamente funzioni di leadership sempre che la persona giuridica non dimostri di avere adottato un efficace un modello di organizzazione e di gestione in epoca precedente al fatto. Tale modello malleva dalla responsabilità l'azienda per l'azione del corrotto disciplinata dal comma 1 dell'art. 2653 c.c. ovvero delle condotte degli amministratori, direttori generali, direttori preposti alla redazione dei documenti contabili e societari, sindaci e liquidatori di società o enti privati che, anche per interposta persona, sollecitano o ricevono per sé o per altri denaro o altre utilità non dovuti o ne accettano la promessa, per compiere o

mettere un atto in violazione degli obblighi inerenti al loro ufficio o gli obblighi di fedeltà. La scelta del legislatore di escludere la responsabilità della persona giuridica nel caso del proprio dipendente corrotto si radica nella considerazione che il vantaggio, in tale caso, è personale e non avvantaggia l'azienda.

Le linee guida della Confindustria

Nell'ambito delle misure preventive in materia di corruzione sia pubblica che privata la Confindustria si è attivata dettando delle linee guida utili per le aziende nella costruzione dei propri modelli di prevenzione e di esenzione da responsabilità per fatti di questo tipo. In difetto di un modello di organizzazione preventiva scatta la responsabilità dell'azienda. Il d.lgs. n. 61/2000 ha inserito nel d.lgs 231/2001 l'articolo 25-ter[3] che reca sanzioni specifiche carico delle società in relazione a reati in materia societaria previsti dal codice civile - se commessi nell'interesse della società da amministratori, direttori generali, liquidatori o da persone che sono sottoposte alla loro vigilanza - nel caso in cui il fatto non si sarebbe realizzato se essi avessero vigilato in conformità degli obblighi inerenti alla loro carica. Questo preambolo significa in pratica che l'azienda risponde se non abbia approntato strumenti di prevenzione adeguati.
Come possiamo vedere, il legislatore è intervenuto più volte per specificare meglio la norma o per estenderne la portata. In questo senso va osservato che la legge 262/2005 (sulla riforma del risparmio) ha inasprito il regime delle pene pecuniarie applicabili agli enti per la commissione di reati societari, raddoppiandone gli importi
Possiamo quindi affermare che anche la Confindustria, in questa materia, ma non solo, ha preso atto della necessità di costruire modelli di prevenzione affinché le aziende possano mallevarsi da responsabilità di tipo riflesso.
Le linee guida della Confindustria individuano alcune aree di rischio:

- La predisposizione di bandi di gara o la partecipazione a procedure competitive finalizzate alla negoziazione o stipula di contratti attivi, cioè in grado di generare un ricavo per la società;
- La negoziazione, stipula, gestione di contratti attivi con società, consorzi, fondazioni, associazioni e altri enti

privati, anche privi di personalità giuridica, che svolgono attività professionale e di impresa
- la gestione delle attività di trading su commodities, finanziario o fisico: selezione delle controparti e dei prodotti, gestione del deals, stipula dei contratti;
- la gestione dei rapporti con società consorzi, fondazione, associazioni o altri enti privati, anche privi di personalità, che svolgono attività professionale ed impresa, dal cui mancato svolgimento possa derivare un vantaggio per la società o per le quali la stessa possa avere un interesse (esempio analisti finanziari, mass media, agenzie di rating, organismi di certificazione ecc);
- negoziazione stipula e gestione dei contratti attivi con intermediari come gli agenti procuratori, i procacciatori di affari, i consulenti commerciali, ecc;
- la selezione dei fornitori di beni e servizi, la negoziazione e stipula dei relativi contratti
- gestione di contratti per l'acquisto di beni e servizi.

9. La conformità in materia di salute e lavoro

Tra le preoccupazioni principali dell'imprenditore rientra sicuramente quella della sicurezza del lavoro disciplinata dal d.lgs. n. 81/2008, il quale, individua i soggetti responsabili della sicurezza degli ambienti di lavoro e dei lavoratori, descrive le misure gestionali e degli adeguamenti tecnici necessari per ridurre i rischi per i lavoratori, specificando le sanzioni in caso di inadempienza.
L'art. 25*septies* del d.lgs. 231 include, tra le cause di responsabilità amministrativa dell'azienda le ipotesi di lesioni gravi e gravissime e di omicidio colposo commessi con violazione delle norme sulla tutela della salute e della sicurezza del lavoro. Alla condanna per tali reati, consegue anche una sanzione irrogata alla società, a titolo di responsabilità amministrativa per non avere organizzato adeguati sistemi di malleva.
La recente giurisprudenza, fra l'altro, include tra i rischi che formano oggetto di valutazione da parte del datore di lavoro e di sorveglianza sanitaria, quelli collegati allo stress da lavoro correlato. Quindi, il d.lgs. 81/2008 prevede la necessità di adottare misure di

prevenzione in relazione a tutti i rischi compreso quello dello stress dal lavoro correlato. Per quest'ultima ipotesi l'attività di prevenzione postula prima di tutto la condivisione di principi etico comportamentali a garanzia della persona lavoratore.
I maggiori rischi per l'imprenditore derivano: dall'ipotesi di omicidio colposo aggravato di cui all'art. 589 CP, reato che si verifica tutte le volte che il decesso del lavoratore avvenga in conseguenze dell'infortunio sul lavoro; nonché delle ipotesi di malattia professionale cioè di una patologia alla quale non consegue l'evento della morte, secondo quanto previsto dall'art. 590 cp. In entrambe queste ipotesi affinché sussista la responsabilità del datore di lavoro è necessario che l'evento dannoso per il lavoratore sia collegato da un rapporto di causalità - cioè causa effetto - con l'azione o l'omissione del datore di lavoro.
Si può anche trattare di una condotta omissiva cioè conseguente all'omessa adozione di misure ritenute indispensabili per la tutela dell'integrità della salute dei lavoratori.
In particolare, per quanto riguarda le lesioni colpose, si tratta di un delitto configurabile nella forma aggravata ogni qualvolta l'infortunio sul lavoro, o la malattia professionale, comporti l'insorgere di una patologia per il soggetto.
La responsabilità dell'ente ipotizzabile nelle sole ipotesi in cui le lesioni siano procedibili d'ufficio ovvero quando le stesse siano gravi o gravissime ed il reato sia stato commesso in violazione delle norme per la prevenzione degli infortuni sul lavoro.
Rispetto agli obblighi derivanti dal d.lgs 81/2008 ed alle conseguenze riflesse previste dal d.lgs 23/2001 è buona prassi che il datore di lavoro definisca - informandone tutto il personale - la propria politica aziendale per la salute e la sicurezza. Inoltre, sussiste l'obbligo di individuare: il datore di lavoro; il responsabile del servizio di prevenzione e protezione; il medico competente; il rappresentante dei lavoratori per la sicurezza; gli addetti alla squadra di pronto soccorso ed emergenza e il preposto o dirigente.
La delega di funzioni da parte del datore di lavoro in questa materia ove, non espressamente esclusa, è ammessa con alcuni limiti e condizioni. Occorre che: che essa risulti da un atto scritto recante una data certa; che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura della funzione delegata; che essa attribuisca al delegato tutti i poteri di

organizzazione gestione e controllo richiesti dalla specifica natura della funzione delegata; che si attribuisca al delegato l'autonomia di spesa necessaria per lo svolgimento delle funzioni delegate; che la delega sia accettata dal delegato per iscritto. Alla delega deve essere data adeguata e tempestiva pubblicità.

La valutazione del rischio e la sua inferenza con le previsioni del d.lgs 231/2001

La normativa in materia di sicurezza del lavoro obbliga il datore di lavoro ad effettuare una valutazione del rischio che deve essere aggiornata periodicamente, o comunque in caso di mutamenti significativi o di infortuni occorsi o malattie professionali accertate, tenendo traccia delle revisioni.
In caso di nuove attività aziendali la valutazione del rischio andrebbe fatta preventivamente e poi ufficializzata all'avvio della nuova lavorazione stessa.
In un'ottica più ampia il documento di valutazione del rischio relativo alla sicurezza del lavoro dovrebbe integrarsi con il modello organizzativo e con le attività di vigilanza di cui al d.lgs. 231/2001.

10. La conformità in materia di ambiente

Come è noto la sempre maggiore attenzione sulle questioni ambientali ha indotto il legislatore, non solo italiano ma anche europeo, ad intervenire sulla materia con l'intento di approntare strumenti di tutela dell'ambiente medesimo.
Il d.lgs. n. 121/2011 di attuazione della direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché la direttiva 2009/123/CE hanno esteso la responsabilità amministrativa alle società ed agli enti per una serie di reati di natura ambientale, integrando il testo del d.lgs. 231/2001.
Pertanto, anche per alcuni reati ambientali, il giudice penale può attribuire - una volta accertate le responsabilità penali a carico di soggetti condannati che ricoprono posizioni apicali (legale rappresentante, amministratore, dirigenti) oppure in posizione intermedia (quadri ed impiegati) - anche una **responsabilità amministrativa** a carico degli enti e delle società per le quali essi operano, combinando sanzioni da 25.800 a 774.500 €. Alle sanzioni

pecuniarie possono anche aggiungersi quelle interdittive, come ad esempio il divieto di contrarre con la pubblica amministrazione, il divieto di fare pubblicità, o in estrema ratio il commissariamento.
La filosofia che regna alla base di un simile trattamento sanzionatori riservato alla società o all'impresa risiede nell'idea che l'azienda non possa trarre profitto dal parziale o mancato rispetto delle legislazioni in materia ambientale.

Le procedure organizzative.

Gli amministratori, quindi, devono approntare le apposite procedure organizzative, cioè, in sintesi, devono predisporre il **modello di organizzazione e gestione**. Tale modello, richiesto a malleva delle responsabilità previste dal d.lgs. 231/2001 non deve essere confuso con i **sistemi di gestione ambientale certificabili ISO 14.001,** le quali sono "sistemi di gestione volontari" che vengono adottati per garantire la massima tutela dell'ambiente ed hanno come destinatari tanto i legali rappresentanti e amministratori delegati ambientali quanto in genere tutto l'organigramma dell'azienda. Il modello di **organizzazione e gestione**, invece, ha un altro scopo: quello di prevenire la commissione dei reati da parte di soggetti apicali, dei loro sottoposti. Questo non toglie che i sistemi di gestione certificati ed il modello di organizzazione e gestione, non possano in parte sovrapporsi in parte. Di qui, ancora una volta l'esigenza di costruire un modello di organizzazione – secondo il d.lgs. 231/2001 – integrato con riguardo a tutti i rischi (compreso quello ambientale, visto che ne parliamo).
Il modello di organizzazione gestione deve prevedere anche un **organismo di vigilanza** dotato di sufficiente competenza professionale, di autorevolezza, di una propria autonomia ed indipendenza anche sul piano delle risorse economiche assegnate. E' buona prassi che nell'organismo sia inclusa anche una persona esterna rispetto all'impresa.
L'organismo di vigilanza deve controllare che l'amministratore delegato ambientale col suo staff di dirigenti e preposti, attui la normativa ambientale senza esitazioni, cioè per meglio dire senza rincorrere ipotetici risparmi sui costi ambientali che possano poi tradursi in un percolo di inquinamento ambientale oltre i limiti imposti dalla legge.

Non tutti i reati ambientali sono stati inclusi nel campo di applicazione del d.lgs. 231/2001: Rientrano nelle ipotesi previste dalla norma:

- la gestione non autorizzata di rifiuti comprendente le attività di raccolta, trasporto e recupero, lo smaltimento, il commercio, l'intermediazione di rifiuti e i fatturati conseguiti in mancanza di autorizzazione o iscrizione e comunicazione prevista dagli artt. 208- 216 del dlgs 152/2006
- realizzazione e gestione non autorizzata di una discarica
- miscelazione di rifiuti pericolosi
- deposito temporaneo di rifiuti sanitari pericolosi
- falsità nella predisposizione di certificati di analisi dei rifiuti e uso di certificati falsi durante il trasporto traffico illecito di rifiuti
- attività organizzata per il traffico illecito di rifiuti
- scarico illecito di acque reflue industriali contenenti sostanze pericolose
- violazione del divieto di scarico sul suolo o nelle acque sotterranee
- scarico illecito nelle acque del mare da parte di navi o aeromobili di sostanze materiali per i quali imposti il divieto assoluto di sversamento
- inquinamento doloso o colposo provocato da navi
- violazione dei valori limite di emissione del cammino qualora ciò comporti anche uno sforamento in conseguenza del superamento dei valori legali dei limiti generali di qualità dell'aria ambiente
- violazione delle prescrizioni stabilite dalle disposizioni normative emanate dalle autorità
- violazione delle disposizioni relative alla produzione e al consumo all'importazione all'esportazione alla detenzione e commercializzazione di sostanze lesive
- distruzione o deterioramento di habitat all'interno di un sito protetto
- uccisione distruzione cattura prelievo o detenzione di esemplari di specie animali o vegetali selvatiche protette
- reati relativi al commercio internazionale di specie di animali e vegetali in via d'estinzione

- violazione di norme per la commercializzazione e la detenzione degli esemplari vivi di mammiferi e rettili che possono costituire pericolo per salute e incolumità

Anche per quanto riguarda la materia ambientale è buona prassi che il rappresentante legale definisca una **politica ambientale aziendale** la quale veda fissati i suoi principi in un codice etico comunque su valori condivisi.
Anche in questo caso va definito l'organigramma che va dal legale rappresentante, all'amministratore delegato, al procuratore ambientale se necessario, ai dirigenti ambientali, al responsabile tecnico degli impianti.
Tra gli obblighi generali c'è quello della **formazione** specifica del personale che cura le pratiche ambientali o la gestione diretta degli impianti di recupero e smaltimento e deposito temporaneo di rifiuti, di scarichi idrici, delle emissioni di un'atmosfera, degli impianti di abbattimento e depurazione. Ma la formazione deve essere estesa anche a coloro che all'interno dell'azienda si occupano di acquisti, del laboratorio, della fabbricazione, produzione, manutenzione degli impianti.
Deve essere previsto un aggiornamento informativo anche da attuale in occasione dell'emanazione di nuovi provvedimenti legislativi.
Inoltre, l'azienda si deve anche dotarsi di un sistema aziendale che preveda le eventuali sanzioni disciplinari per il mancato rispetto delle procedure ambientali, contemplando le conseguenti previsioni sanzionatorie in linea col contratto di lavoro.
Le autorizzazioni in materia ambientale conseguite dall'azienda devono essere periodicamente rinnovate
Dovrà essere anche prevista la gestione delle emergenze per evitare danni ambientali. Quindi, le emergenze anche di lieve entità e di ridotto impatto ambientale possono avere significative conseguenze in termini di costo per l'azienda anche se sottostimate in termini di probabilità di accadimento.
Dovrebbero pertanto essere approntate per procedure di emergenza ambientali, con l’indicazione dei mezzi e dispositivi per gestire le emergenze, esercitazioni di emergenza e simulazioni,
Deve essere prevista una procedura di affiancamento degli enti di controllo in occasione delle ispezioni.

———————

Tra le numerose aree di illecito contemplate dal d.lgs. 231/2001 – per brevità - ne abbiamo esplicate solo alcune. Pertanto, l'avvertenza è che il campo d'azione della responsabilità dell'impresa è molto più esteso come si evince dall'elenco di cui al precedente paragrafo 5.

———————

11. Il modello organizzativo

Il modello organizzativo rappresenta il documento che dimostra la buona fede dell'azienda e traccia la distanza tra l'azienda e la condotta illecita tenuta dal proprio amministratore, dirigente o impiegato.
In sostanza – in applicazione dei doveri di *accoutability* (autovalutazione) – il modello organizzativo rappresenta lo strumento di prevenzione atto a limitare le occasioni di illecito da parte dei dipendenti.
Le caratteristiche di tale modello, della gestione e del controllo, sono codificate nell'art. 6, comma 2, del d.lgs. 231/2001.
Lo stesso art. 6 prevede i modi in cui l'azienda si malleva dalla responsabilità.
L'ente non risponde **se prova** che:

a) l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) le persone hanno commesso il reato eludendo fraudolentemente i modelli di organizzazione e di gestione;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b).

2. In relazione all'estensione dei poteri delegati e al rischio di commissione dei reati, i modelli di cui alla lettera a), del comma 1, devono rispondere alle seguenti esigenze:

a) individuare le attività nel cui ambito possono essere commessi reati;

b) prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;

c) individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati;

d) prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;

e) introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Gli elementi del modello organizzativo:

Per costruire il modello organizzativo occorre sviluppare le seguenti fasi:

L'identificazione dei rischi potenziali

La costruzione di un modello organizzativo (di prevenzione della responsabilità) richiede una preventiva analisi e valutazione del rischio. Ovviamente quando parliamo di rischio ci riferiamo alla lista di fattispecie la cui violazione, secondo il d.lgs. 231/2001, possono riflettersi sulla responsabilità dell'azienda o ente.
La valutazione del rischio richiede logicamente una ricognizione, o meglio ancora, l'identificazione del rischio.
Innanzitutto, occorre definire il concetto stesso di rischio. Per rischio si intende "qualsiasi variabile o fattore che nell'ambito dell'azienda autonomamente o in correlazione ad altre variabili possono incidere negativamente sul raggiungimento degli obiettivi indicati dal decreto 231".
In altre parole, il rischio deve essere valutato in relazione agli **ambiti di attività** che sono specificatamente richiamati dal d.lgs. 231 Nei quali il fatto del dipendente si riverbera sulla responsabilità dell'imprenditore.
La lista è molto lunga e riguarda le attività commesse alla percezione di erogazioni, o al conseguimento di erogazioni pubbliche o pubbliche forniture; alle cautele necessarie nell'approntamento ed utilizzo di strutture informatiche, alla sicurezza del lavoro, il

trattamento dei dati personali, il rischio di riciclaggio e corruzione, la gestione degli appalti e molto altro (per completezza si fa rimando alla lista riportata nel paragrafo 5).
Rientrano poi nella valutazione dei possibili rischi anche le questioni inerenti alla concorrenza sul mercato ed i possibili reati societari.
Ovviamente per dar luogo all'analisi di cui trattasi è necessaria una mappatura delle aree aziendali a rischio in relazione all'eventualità che possano essere commessi reati rilevanti ai fini della responsabilità dell'azienda. La mappatura comporta il compimento di una revisione periodica, esaustiva, della realtà aziendale con l'obiettivo di individuare le aree che in ragione della natura e delle caratteristiche delle attività effettivamente svolte risultano interessate dal potenziale compimento di taluno dei reati contemplati nella norma. Si può procedere con diverse modalità, cioè mappando per "attività", per "funzioni" o per "processi".
In particolare, è importante individuare le fattispecie di reato rilevanti per l'ente e parallelamente le aree che, in ragione della natura delle caratteristiche delle attività effettivamente svolte, possono essere interessate da eventuali casistiche di reato o di illecito.
Tra l'altro, visto che nella valutazione del rischio devono essere incluse tutte le variabili che direttamente o indirettamente possono incidere in negativo sugli obiettivi fissati dalla legge, nel processo di valutazione occorre considerare anche la interrelazione o l'interdipendenza sistemica fra i vari effetti rischiosi: occorre cioè considerare la possibilità di un cosiddetto effetto domino.
Naturalmente devono essere identificati anche i soggetti sottoposti all'attività di monitoraggio e tra questi non vanno inclusi solo i dipendenti dell'azienda ma anche coloro che siano legati all'impresa da semplici rapporti di parasubordinazione o da altri rapporti di collaborazione come i partner commerciali e i dipendenti di questi ultimi. Ad esempio, per quanto concerne il rischio connesso alla sicurezza del lavoro i soggetti sottoposti al monitoraggio saranno tutti lavoratori che sono destinatari delle protezioni previste dalla normativa.
Nel valutare il rischio poi va considerata anche l'ipotesi di possibili casi di concorso nel reato. In generale, e a titolo esemplificativo, possiamo citare alcune misure di prevenzione da prendere in considerazione come compiere un'analisi preventiva dei soggetti da

invitare alla gara; evitare appalti al massimo ribasso soprattutto in determinati settori (movimento terra e trasporto conto terzi, gestione rifiuti, ecc.), prevedere il divieto di subappalto o comunque rigorose forme di disciplina dell'accesso allo stesso.
Per l'analisi ed il monitoraggio, naturalmente possono essere utilizzati anche strumenti informativi: si pensi per esempio alla consultazione presso le prefetture dell'elenco dei fornitori, prestatori di servizio, esecutori di lavori, non soggetti a tentativo di infiltrazione mafiosa operanti nei settori maggiormente a rischio individuati dalla legge 190 del 2012.
In definitiva possiamo dire che ogni settore presenta propri specifici ambiti di rischio che possono essere individuati solo tramite una puntuale analisi interna.
In questo senso si parla di compliance sulla organizzazione.

L'analisi dei rischi potenziali

Una volta una volta definita la mappatura del rischio occorre valutare il grado di conformità dell'organizzazione rispetto a tale rilevazione.
In ogni caso, in base alla valutazione fatta, bisogna costruire un **modello di prevenzione** nonché quelli che il decreto 231 definisce **specifici protocolli** diretti a programmare la formazione e l'attuazione di decisioni dell'ente in relazione ai reati da prevenire. Si tratta perciò di creare dei **protocolli di comportamento** che tengano conto dei possibili rischi di commissione di quegli specifici reati previsti dal decreto 231 attenuandone la possibilità. In termini più tecnici a questo punto possiamo parlare di **risk assessment**.
L'attività di risk assessment può essere applicata ai più svariati campi come per esempio nel campo informatico, nel settore della privacy, in quello alimentare, in quello ambientale, in quello della sicurezza del lavoro.
Dobbiamo altresì osservare che le aziende sono sempre più poste sotto pressione non solo per il rischio legale che si riverbererebbe sulla propria reputazione e sul proprio patrimonio, ma anche riguardo all'etica sociale e finanziaria, quella operativa e reputazionale che si ricollega al proprio brand.
Per darne una definizione sintetica possiamo dire che il **risk assessment** e un processo col quale i rischi di sistema ed i relativi

impatti sono identificati, analizzati e qualificati. Occorre pertanto svolgere un'operazione di **risk management** cioè un processo posto in essere dal management e altri operatori della struttura aziendale, utilizzato per la formulazione delle strategie in tutta l'organizzazione, tesa ad un progetto per: a) individuare eventi potenziali che possano influire sull'attività aziendale, b) per gestire il rischio entro i limiti accettabili e per fornire una ragionevole sicurezza sul conseguimento degli obiettivi aziende

Detto questo è evidente che non basta una mappatura dei rischi connessi alla commissione dei reati previsti dal decreto 231, ma occorre anche definire la gestione di tati rischi.

L'art. 6 del più volte citato decreto 231 prevede perciò espressamente un'analisi delle attività svolte nell'ambito della società, proprio al fine di individuare quelle che in aderenza al decreto possono considerarsi a rischio di illeciti. Ogni società oente, infatti, presenta margini di rischio la cui individuazione implica una particolareggiata analisi della struttura aziendale e delle singole attività svolte.

E' quindi necessario svolgere uno specifico studio (compliance) dello statuto e dell'atto costitutivo, del sistema di governance, della composizione degli organi amministrativi e di controllo e il loro funzionamento, il sistema di deleghe e procure, i poteri autorizzativi e di firma, l'organigramma e il funzionigramma, i mansionari, l'analisi dei regolamenti approvati e vigenti (per esempio quello di contabilità o per servizi e fornitur), l'analisi del sistema procedurale in uso anche compresi quelli di certificazione dei processi aziendali. Dovrà individuare le attività svolte da ciascuna funzione aziendale attraverso lo studio delle disposizioni organizzative e delle procedure applicate, dovrà valutare la se nel pregresso dell'azienda siano già intervenuti a procedimenti amministrativi di cui al decreto 231, procedimenti penali a carico dei componenti degli organi societari o i dipendenti, effettuare approfonditi interviste ai soggetti individuati in posizione di rilievo al fine di una più coerente mappatura dei rischi, accertare le singole attività a rischio nell'ambito delle diverse funzioni dell'azienda.

In quanto la rischio, semplificando e per concludere, possiamo dire che esso interessa sotto i seguenti aspetti:

- una potenziale minaccia che l'evento negativo possa manifestarsi
- la probabilità che l'evento tenutosi si verifichi

- le conseguenze della verificazione dell'evento temuto sull'azienda
- il danno che può derivare dalla verificazione dell'evento temuto

Per dirla in una parola si tratta di una valutazione dei **parametri probabilità** e di **impatto.**

I protocolli comportamentali nel rapporto con i partners, in particolare:

Un'area di potenziale esposizione al pericolo è certamente quella dei rapporti con i partners, siano essi commerciali o contrattuali. Per attenuare il rischio in tale settore il modello organizzativo deve necessariamente contenere un protocollo comportamentale che prenda in considerazione almeno i seguenti elementi:

- il processo di selezione e valutazione del partner dovrà essere condiviso tra tutte le unità organizzative dell'ente;
- possibilmente dovrà essere garantito un processo comparativo degli offerenti sulla base di almeno due o tre offerte concorrenti;
- dove è possibile deve essere richiesta idonea documentazione per poter verificare i requisiti di cosiddetta moralità del partner;
- dove non sia possibile una raccolta di documenti tale da poter verificare i cosiddetti requisiti di moralità si dovranno assumere tutte le informazioni lecite al fine di valutare l'affidabilità del partner, assicurando la tracciabilità e verificabilità delle informazioni medesime tramite apposita relazione scritta;
- la documentazione sull'esito dei controlli e delle valutazioni del partner dovranno essere archiviate in modo da garantirne sempre la tracciabilità.

Il protocollo dovrà prevedere anche doveri di segnalazione:

- quando sussistono dubbi sulla qualifica o sulla permanenza dei requisiti in capo ai partner occorre dare informazione all'amministratore delegato e all'organo di vigilanza;
- deve essere reso noto al partner che l'eventuale violazione del modello dei principi adesso collegati costituiscono

impedimento al rapporto contrattuale;
- l'eventuale insorgenza di criticità con il partner deve essere comunicata all'amministratore delegato e all'organismo di vigilanza

Dovrà essere disciplinato anche la modalità per gli esborsi:

- ogni esborso deve sempre recare una causale espressa ed essere registrato;
- il pagamento deve essere:

a) effettuato esclusivamente sul conto corrente indicato nel contratto,
b) corrispondere esattamente a quanto indicato nel contratto;
c) non può in nessun caso essere effettuato su conti correnti cifrati;
d) non può essere effettuato a favore di un soggetto diverso dalla controparte contrattuale;
e) non può essere effettuato in un paese terzo rispetto a quello delle parti contraenti o a quello di esecuzione del contratto
f) se effettuato sui conti correnti di banche appartenenti operanti in paesi elencati nei cosiddetti paradisi fiscali o in favore di società offshore deve avvenire nel rispetto delle leggi di settore;
g) ne deve essere garantita la tracciabilità con l'indicazione dell'importo il nome e la denominazione e l'indirizzo e il numero di conto corrente.

Dovranno essere particolarmente disciplinati i processi di acquisto e vendita di beni e servizi secondo i seguenti accorgimenti:

- gli acquisti devono avvenire nel rispetto del budget assegnato;
- se possibile dovrà essere predisposto un albo dei fornitori e collaboratori;
- occorre archiviare la documentazione rilevante relativa alla transazione cioè: ordini, contratti, scambi, di comunicazione coi fornitori, così da consentire la ricostruzione tracciabilità delle diverse fasi del processo decisionale;
- la sottoscrizione dei contratti dovrà essere eseguita esclusivamente da chi è titolare del potere di firma;

- se è possibile occorre adottare una politica di rotazione dei fornitori.

12. Il sistema “integrato” della gestione del rischio

Abbiamo già detto in premessa che il rischio di compliance, ossia di non conformità alle norme, comporta per le imprese il pericolo di incorrere in sanzioni giudiziarie o amministrative, nonché di perdite finanziarie o danni reputazionali in conseguenza della violazione di norme imperative o di norme di autoregolamentazione, molte delle quali sono indicate nel decreto 231.
Tuttavia, esistono altri aspetti di responsabilità, parimenti puniti con pesanti sanzioni pecuniarie, che fanno capo a diverse legislazioni.
Una fra tutte, per esempio, la normativa sulla privacy che ha assunto una rilevanza notevole dopo l'emanazione del regolamento europeo e l'attivazione dei controlli da parte di un nucleo specializzato della Guardia di finanza.
In breve, possiamo dire che l'impresa o l'ente si trovano a dover gestire numerosi obblighi di compliance, cioè una pluralità di processi interni afferenti ai diversi obblighi legali, che potrebbero apparire scoordinati o incoerenti tra loro. Questo vale anche per i controlli connessi alle diverse procedure che, per la varietà dei protocolli, possono apparire ridondanti. I modelli di prevenzione, in sostanza, potrebbero stratificarsi al pari di una legislazione stratificata nel tempo.
Di qui nasce la necessità di un **sistema integrato di gestione dei rischi** cioè, in pratica, di un unico **modello organizzativo che comprenda tutte le procedure di abbattimento del rischio legale** connesso alle diverse materie.
In questo senso si parla di compliance integrata, capace di evitare sovrapposizioni e ridondanze.
In pratica l’integrazione di cui trattasi riguarda:

- la razionalizzazione delle attività (quindi: delle risorse, delle persone, dei protocolli);
- il miglioramento dell'efficacia e dell'efficienza dell'organizzazione (l’efficacia è l’idoneità di raggiungere il

risultato; l'efficienza è la capacità di raggiungere i migliori risultati in rapporto alle risorse spese);
- un più facile flusso di informazioni attraverso una visione integrata delle diverse esigenze di compliance

Conviene, quindi, all'azienda procedere ad un **risk assessment** che prenda in considerazione in un'unica soluzione tutti gli aspetti di responsabilità e che si occupi di una manutenzione costante dei modelli organizzativi e dei relativi protocolli.
Si tratta, quindi, in pratica, di prevedere procedure comuni o per meglio dire orizzontali rispetto ai diversi ambiti, che garantiscano l'efficienza e la snellezza operativa dell'azienda, evitando sovrapposizioni di ruoli, oppure duplicazioni nelle verifiche o nelle azioni correttive.
Sintetizzando ciò che abbiamo detto, le società in quanto oberate di possibili responsabilità derivanti da diverse normative nei diversi settori, dovrebbero evitare la frammentazione mantenendo in vita distinti modelli organizzativi e distinte attività di controllo. Anche per conseguire maggiori livelli di efficienza e di risparmio (tanto di risorse umane che finanziarie) dovrebbero giungere a predisporre un **unico modello** capace di integrare tutte le procedure di garanzia, tenendo conto delle peculiarità di ciascun settore di responsabilità (privacy, 231/2001, corruzione, concorrenza sleale, riciclaggio, ecc.), attraverso una sintesi degli adempimenti e ad un unico esercizio della funzione di vigilanza.
Il predetto modello, naturalmente, deve contenere specifici meccanismi di coordinamento e collaborazione tra i principali settori aziendali ed in particolarmente tra i dirigenti. Inoltre, per favorire l'attività di vigilanza, il modello dovrà contenere degli indicatori idonei a garantire all'organismo di vigilanza una più rapida verifica del rispetto delle procedure.
Il **criterio generale**, e paradigma di efficacia (accauntability) da considerare nella costruzione di un **modello integrato**, è che **le misure siano tali** per cui l'agente che ha commesso quel reato o illecito che coinvolge l'azienda, **debba averlo voluto al punto che per metterlo in atto ha deciso di aggirare o forzare i protocolli aziendali**.
L'insieme delle misure che l'agente, volendo trasgredire, sarà costretto a forzare per mettere in atto la sua condotta illecita, dovrnno comprendere le specifiche attività dell'ente ed in

considerazione del rischio di possibili reati o illeciti ipoteticamente collegabili alle stesse.
La necessità di un modello integrato nasce dalla realtà delle imprese (e degli enti), nelle quali la gestione del rischio tramite il modello voluto dal decreto 231, spesso incrocia altri sistemi di prevenzione e gestione dei rischi già oggetto di altre previsioni legislative operanti all'interno dell'organizzazione aziendale: per questo motivo e opportuno che un modello integrato, appunto, inglobi tutti i protocolli di prevenzione nuovi con quelli già esistenti ed afferenti altre aree di rischio legale.
Un esempio significativo può riguardare il tema della sicurezza del lavoro, area di rischio per la quale la legislazione di settore (d.lgs. 81/2008) prevede già un processo di valutazione del rischio e un apposito documento di prevenzione. I reati connessi ha l'obbligo di garantire la sicurezza del lavoro, però, sono annoverati anche nel decreto 231 come fonte di responsabilità amministrativa aziendale. Pertanto, il modello organizzativo previsto dall'art. 6 del decreto 231 deve necessariamente inglobare anche quello, magari già esistente, di sicurezza del lavoro. Altrettanto dicasi per il trattamento di dati personali, per la protezione dei sistemi informatici, per la gestione delle comunicazioni aziendali e per tutto quello che ne deriva in termini di responsabilità dell'impresa, dell'ente o del professionista.

13. **L'organismo di vigilanza**

L'art. 6 del decreto 231 prevede il compito di **vigilare sul funzionamento e l'osservanza dei modelli** e di curare il loro aggiornamento affidato a un **organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo**.
Tradotto: la mancanza di un organismo di controllo è fonte di responsabilità per l'ente in caso di illecito del dipendente.
Su come concepire un "Organismo di Vigilanza e Controllo" può essere utile la lettura delle linee guida di Confindustria pubblicate nel 2008 ed aggiornate nel 2014 e nel 2021. Tale riferimento è utile in quanto le linee guida hanno precisato alcuni aspetti specifici dell'organismo di vigilanza, definendone i poteri e i requisiti, l'autonomia ed indipendenza, la professionalità e la continuità dell'azione

E’ un principio di base, infatti, che per poter svolgere in modo efficace i propri compiti l'organismo di controllo deve essere dotato delle caratteristiche essenziali di autonomia indipendenza professionalità e continuità d'azione in difetto dei quali il modello di cui al decreto 231, nei fatti, verrebbe vanificato. Detto principio peraltro è richiamato anche dalla giurisprudenza.[4]
Per meglio illustrare brevemente i requisiti predetti, cioè quelli indicati dall’art. 6 del d.lgs. 231 come necessari per il valido funzionamento dell'organismo di vigilanza, sintetizziamo:

- **autonomia dell’organismo di controllo**: si tratta della necessaria autonomia rispetto ai soggetti sottoposti al controllo. Tale requisito si consegue attraverso lo svincolo per quanto possibile dei componenti dell’organismo dalla gerarchia interna. Pertanto, i soggetti facenti parte dell’organismo devono essere collocati in rapporto diretto con il vertice aziendale (in una posizione cioè di staff). Secondo una certa giurisprudenza i componenti non dovrebbero essere adibiti a compiti operativi in azienda. Per quanto espresso nelle lenee guida della Confindustria, inoltre, si deve escludere la possibilità di conferire un ruolo di organismo di controllo, per il modello 231, al responsabile del servizio di prevenzione e protezione di cui al d.lgs 81/2008. Infatti, tale figura, sia essa interna o esterna all’azienda, è dotata di autonomi poteri di iniziativa e controllo che esplica con continuità d'azione, nel modo di volta in volta da lui ritenuto più opportuno, attraverso ispezioni, richieste di chiarimenti, controlli effettuati in loco, verifiche delle procedure di sicurezza e aggiornamento delle stesse avvalendosi di strumenti e tecniche specialistiche. Ma di regola questo soggetto svolge in azienda un ruolo operativo ed è quasi sempre inserito all'interno di precise gerarchie aziendali dalle quali dipende o, se trattasi di soggetto esterno all'azienda, egli è vincolato da rapporti contrattuali con le gerarchie medesime. Possiamo dire in definitiva che il modello organizzativo, per poter esplicare la propria efficacia esimente, deve prevedere e strutturare il compito di vigilare sul funzionamento e l'osservanza dei modelli o protocolli e curare il loro aggiornamento. Questo compito è

appunto affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo. In ogni caso il requisito dell'autonomia va inteso nel senso che la posizione dell'organismo di vigilanza nell'ambito dell'ente deve garantirne l'autonomia dell'iniziativa di controllo da ogni forma di interferenza o condizionamento da parte di qualsiasi componente dell'ente medesimo. La giurisprudenza ha poi affiancato al requisito dell'autonomia quello dell'indipendenza. Infatti, secondo il ragionamento dei giudici l'autonomia risulterebbe svuotata di significato allorquando i membri dell'organismo di vigilanza risultassero condizionati a livello economico o personale, oppure venissero collocati in situazioni di conflitto di interesse anche potenziale. Ecco perché le stesse linee guida della Confindustria consigliano che l'organismo di cui trattasi venga collocato nell'organizzazione aziendale come unità di staff, collegata al massimo vertice dell'azienda: quindi, nelle società, al consiglio di amministrazione. È corretto in ogni caso osservare che quando l'Organismo è a composizione collegiale, giocoforza ne faranno parte anche soggetti legati da un certo grado di subordinazione gerarchica interna, cosicché, in relazione a detti soggetti l'indipendenza richiesta potrà essere solo relativa. Anche per questo è consigliabile che l'Organismo collegiale abbia al suo interno soggetti esterni all'azienda. Quando l'organismo si avvale di componenti esterni all'azienda il modello organizzativo dovrà indicarne i casi di incompatibilità.

- **professionalità:** si tratta di un requisito proprio dei soggetti facenti parte dell'organismo di controllo, che devono essere dotati delle competenze tecniche e professionali necessarie per lo svolgimento del proprio ruolo. La scelta dei componenti, infatti, deve tenere conto del bagaglio di strumenti e tecniche che la persona deve possedere per poter efficacemente svolgere la propria attività all'interno dell'organismo di valutazione. Sulla definizione di tale requisito è intervenuta anche la giurisprudenza di merito stabilendo che ciò che è essenziale è che la scelta dei membri avvenga previa

verifica del possesso di specifiche competenze professionali. Pertanto, sempre secondo questa giurisprudenza non è sufficiente un generico rinvio al *curriculum* del soggetto, ma il modello deve esigere che i membri abbiano competenze in attività ispettiva, consulenziale, ovvero la conoscenza di tecniche idonee a garantire l'efficacia dei poteri di controllo e del potere propositivo demandato all'organismo di vigilanza. La giurisprudenza si è espressa anche in merito all'attività ispettiva la quale richiede la capacità di analisi e di valutazione del rischio, capacità di elaborare e valutare questionari e di conoscere le metodologie per l'individuazione delle frodi. È utile, tra l'altro, che almeno taluno dei componenti abbia competenze in tema di analisi dei sistemi di controllo e conoscenze di tipo giuridico, in particolare in campo penalistico e civilistico, come e auspicabile che taluno dei componenti abbia competenze nel campo della salute, della sicurezza e dell'ambiente, oltre che nelle tecniche di *audit* al fine di garantire che l'organismo di valutazione possa effettivamente muoversi in una effettiva sfera di autonomia. Naturalmente, da ultimo, è importante che i membri abbiano gli strumenti per conoscere e valutare la struttura aziendale.

- **Continuità dell'azione:** significa che l'organismo di controllo deve svolgere un'azione costante di verifica delle eventuali carenze del sistema e di riscontro della effettiva osservanza dei protocolli inseriti nel modello. Per garantire una efficace e costante attuazione del modello si rende necessaria la presenza di una struttura dedicata che, nelle grandi aziende, dovrebbe svolgere la propria attività di vigilanza a tempo pieno. Ciò non è possibile invece nelle aziende di ridotte dimensioni. Per dare continuità all'azione, l'organismo di vigilanza può fornire anche pareri sulla costruzione del modello per renderlo più solido e completo sin dalla fase di elaborazione. Nel caso in cui si opti per la nomina di soli **membri esterni** sarebbe auspicabile la costituzione di una apposita segreteria in grado di coordinare l'attività dell'organismo di vigilanza e assicurarne la costante funzionalità all'interno

dell’azienda. In altre parole, una **interfaccia aziendale**. La continuità dell'azione richiede in ogni caso un riconoscimento della competenza dell'organismo di vigilanza, una sua legittimazione: pertanto, dopo la costituzione dell'organismo di vigilanza il vertice aziendale è tenuto a renderne pubblici all'interno dell'azienda i poteri, prevedendo al limite sanzioni in caso di mancata collaborazione. Lo stesso modello organizzativo deve specificare che le attività poste in essere dall'organismo di vigilanza **non possono essere sindacate** da nessun altro organismo o da nessun'altra struttura aziendale, ma solo il vertice dell'azienda è competente a vigilare sull'adeguatezza del suo intervento e della sua funzionalità. L'organismo di vigilanza, naturalmente, deve avere libero accesso presso tutte le funzioni dell’azienda senza nessun consenso preventivo, onde ottenere ogni informazione o dato utile per lo svolgimento dei compiti di vigilanza. Inoltre, può avvalersi dell'ausilio di tutte le strutture della società o anche di consulenti esterni. Questo significa che nella formazione del *budget* aziendale il vertice dovrà prevedere una adeguata dotazione di risorse finanziarie messe a disposizione dell'organismo di vigilanza per il necessario svolgimento dei compiti assegnati tanto dalla legge, quanto dall'azienda. Sul piano pratico, per quanto attiene la continuità dell'azione dell'organismo di vigilanza, è necessaria una **standardizzazione e calendarizzazione** delle attività di vigilanza, una verbalizzazione a futura memoria delle riunioni, una definizione dei flussi informativi tra le strutture aziendali e l'organismo di vigilanza medesimo. La standardizzazione comporta la necessità di emanare un apposito regolamento che può disciplinare anche in modo specifico la calendarizzazione dei controlli e delle procedure di analisi: meglio se detto regolamento sia formulato su proposta dello stesso organismo di vigilanza, evitando così che si possa sostenere un difetto di indipendenza dell'organismo stesso del disciplinare il proprio funzionamento.

Come già detto, in relazione alla complessità dell’azienda o dell’ente, l’organismo di controllo può essere costituito in forma “monocratica”

oppure in forma “collegiale”.
La legge (art. 6, comma 4, d.lgs. 231) **consente di assegnare i compiti di vigilanza e controllo anche direttamente alla dirigenza aziendale,** la quale data la molteplicità dei propri impegni **può avvalersi di soggetti esterni** cui affidare l’incarico di svolgere verifiche sul rispetto dei protocolli, sulla manutenzione del modello organizzativo e sull’efficacia dello stesso.
E’ buona norma, nel caso di mantenimento delle funzioni di controllo da parte del vertice aziendale (organismo di vigilanza monocratico), che quantomeno per gli *audit* il compito venga affidato ad un professionista esterno, meglio se qualificato in quanto a conoscenze giuridiche sulla tipologia di reati o illeciti fonti di responsabilità dell’azienda.
La scelta di un organismo monocratico (supportato da consulenti esterni) è diffusa soprattutto negli enti e nelle aziende di piccole dimensioni. Data però la relatività della locuzione “piccole dimensioni” è necessario ricercarne una definizione giuridica. In questo senso si può fare riferimento alla raccomandazione della Commissione europea 2003/361/CE del 6 maggio 2003 che indica i seguenti elementi identificativi:

- un numero di dipendenti non superiore a 49 unità (compresi quelli a tempo determinato);
- un fatturato annuo non superiore ai 10 milioni di euro;

La composizione dell’organismo di vigilanza in particolare:

Rammentiamo ancora una volta che l'art. 6 del decreto 231 prevede che l'ente possa essere **esonerato dalla responsabilità** conseguente alla commissione di reati presupposto **se l'organo dirigente ha adottato modelli di organizzazione, di gestione e di controllo idonei a prevenire reati considerati, nonché, affidato ad un organismo dell'ente, dotato di autonomi poteri di iniziativa e controllo, il compito di vigilare sul funzionamento dell'osservanza del modello e curarne l'aggiornamento.**
La legge però non fornisce indicazioni circa la composizione dell'organismo di vigilanza e ciò consente di optare per una composizione sia monocratica (il vertice stesso dell’azienda) che plurisoggettiva (cioè un collegio). Nell'ultimo caso possono essere

chiamati a comporre l'organismo di vigilanza anche **soggetti esterni all'ente** purché dotati dei requisiti previsti.
Come per ogni altro aspetto del modello, anche la composizione dell'organismo di vigilanza deve essere modulato sulla base delle dimensioni, del tipo di attività e della complessità organizzativa dell'azienda.
Ricordiamo di nuovo che l'art. 6 comma 4 del decreto consente alle imprese di piccole dimensioni di affidare i compiti di organismo di vigilanza all'organo dirigente (meglio se coadiuvato da consulenti esterni).
Le attività dell'organismo di vigilanza possono essere così sintetizzate:

- effettuare una vigilanza sulla effettività del modello, controllandone la coerenza tra i comportamenti concreti e il documento di organizzazione;
- compiere un esame della adeguatezza del modello rispetto alle concrete esigenze che si manifestano all'interno della azienda;
- analizzare il mantenimento, nel tempo, dei requisiti di solidità e funzionalità del modello stesso;
- promuovere e curare eventuali correzioni necessarie;
- suggerire proposte di adeguamento o miglioramento del modello agli organi in grado di dare loro concreta attuazione in azienda;
- verificare l'attuazione e la effettiva funzionalità delle soluzioni proposte.

La consulenza:

La complessità del quadro normativo, i diversi campi di intervento e soprattutto la capacità di strutturare un'organizzazione che ne risulti conforme, richiedono specifiche conoscenze ed esperienze raramente presenti all'interno del contesto aziendale o professionale.
Per questo motivo è nato un nuovo ambito della consulenza legale detta appunto "compliance consulting".
Non si tratta solo di conoscere le norme e nemmeno di avere acquisito linee di indirizzo o prassi ministeriali: si tratta di saper verificare la conformità dei modelli organizzativi interni rispetto ad

un paradigma legale sempre più articolato se non addirittura complicato.
In altri termini – restando fedeli al lessico specialistico - si tratta di supportare l'imprenditore o il professionista nel proprio dovere di "accountability" così come spiegato nei paragrafi che precedono.
I livelli di intervento del consulente di "compliance" sono sostanzialmente tre:

a) **la conoscenza degli obblighi**: - Si tratta di fornire al mandante un quadro chiaro dei suoi obblighi di legge, delle situazioni di maggior rischio legale, ma anche degli strumenti che può adottare per attenuare o eliminare il rischio mettendosi al riparo da sanzioni e richieste di risarcimento. Questo livello di consulenza si esaurisce dunque nella capacità di far sì che l'imprenditore (o professionista) prendano coscienza della necessità di conformarsi a modelli legali e organizzativi indicati dal consulente.
b) **la costruzione dei modelli**: E' una fase incrementale rispetto alla precedente: oltre alla conoscenza di obblighi, quadro legale, prassi e necessità di adeguamento, in questo ambito il consulente svolge una analisi del rischio e propone adeguati modelli di conformità.
c) **La consulenza continuativa**: Si tratta di un'ulteriore fase incrementale che presuppone un rapporto stabile di consulenza diretta non solo ad illustrare i regimi giuridici e sanzionatori, non solo a verificare ed adeguare i modelli aziendali rispetto agli obblighi vigenti, ma anche a curarne la periodica manutenzione e l'efficienza attraverso strumenti di vigilanza ad hoc. In sostanza il consulente potrà entrare a far parte dell'Organismo di Vigilanza aziendale, oppure essere nominato come diretto collaboratore del vertice aziendale nel caso in cui questi decida di costituirsi come organismo monocratico secondo quanto previsto dall'art. 6, comma, 4 del d.lgs. 231/2001.

Agosto 2023

Avv. Augusto Baldassari

Notes

[←1]

Alessandro Foti, “Guida operativa per la costruzione e gestione del modello 231”, sistema integrato di gestione dei rischi, pag. Q ho 111

[←2]

Per approfondimenti: Falcone, “Compliance”, in Digesto comm, agg. VI, Torino, 2012

[←3]

La legge n. 69/2015 ha. Ulteriormente modificato l'art. 25ter del d.lgs. 231/2001 estendendone l'applicazione a tutti gli enti citati nella normativa.

[←4]

Un esempio in tal senso è rappresentato dalla notissima sentenza ThyssenKrupp. Con sentenza del 15 aprile 2011, la Corte d'Assise di Torino condannò l'amministratore delegato della società ThyssenKrupp Terni S.p.a. alla pena di sedici anni e sei mesi di reclusione per i reati di omicidio volontario plurimo, incendio doloso e omissione dolosa di cautele contro gli infortuni sul lavoro aggravata dall'evento, uniti dal vincolo della continuazione. Gli altri cinque imputati, quali amministratori e dirigenti della suddetta società, erano stati invece condannati a pene comprese tra tredici anni e sei mesi di reclusione e dieci anni e dieci mesi di reclusione, per i meno gravi delitti di omicidio colposo plurimo e incendio colposo, entrambi aggravati dalla previsione dell'evento. Con la sentenza 12/12/2016 n° 52511 la quarta sezione penale della Corte di Cassazione, pose fine alla vicenda pertinente l'incendio divampato nella notte tra il 5 e 6 dicembre 2007 presso gli stabilimenti dell'acciaieria ThyssenKrupp, nella quale persero la vita sette operai.