NOTA INFORMATIVA N. 18/2021

COSA CONTA PER L'IMPRESA: IL MODELLO ORGANIZZATIVO INTEGRATO

1. Introduzione

Il legislatore è compulsivo quando chiede alle aziende di prevenire i rischi di commissione dei reati e di adottare misure a riduzione degli stessi. A volte sente l'esigenza di curare questa patologia che affligge gli ordinamenti e di razionalizzare il disordine normativo: emana per esempio il D.lgs. 626/94, che recependo otto direttive europee sulla sicurezza e l'igiene sul lavoro, attua la mutazione di sistema da normativo risarcitorio a sistema preventivo. È una prima iniezione di norme sulla prevenzione, ma l'innesto vero e proprio viene praticato negli anni duemila con il D.lgs. 231/01, il quale introduce la Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica. Da tale innesto germoglia nell'ordinamento italiano la colpa di organizzazione imputata all'impresa, radicata nella carenza di controllo e di vigilanza, e nell'assenza di misure di prevenzione e di protezione. Compare nella normativa nazionale un canone inverso: *societas delinquere potest*. E se il reato è commesso a vantaggio e nell'interesse dell'impresa, il vuoto organizzativo colpevole, accertato in sede penale, è sanzionato con pene rilevanti:

i. sanzioni pecuniarie commisurate alle condizioni economiche e patrimoniali dell'impresa, da applicare *tout court*,
ii. sanzioni interdittive, che nei casi più gravi comportano l'interdizione dall'esercizio dell'attività; nei casi meno gravi, il divieto di pubblicizzare beni o servizi, di contrattare con la pubblica amministrazione o l'esclusione da agevolazioni, finanziamenti, sussidi, ecc. ecc.,
iii. confisca, anche per equivalente, del prezzo o profitto del reato,
iv. pubblicazione della sentenza, con i conseguenti riverberi reputazionali.

Che si tratti di responsabilità amministrativa o penale è questione sintattica più che discussione giuridica. Certo è che penale è il giudicante, penale la sede di accertamento della responsabilità dell'impresa. La liturgia processuale diventa bifida: se il reato è fra quelli declinati dal D.lgs. 231/2001 ed è commesso a vantaggio e nell'interesse della società, si iscrive nel registro delle notizie *criminis* e si processa l'autore materiale della condotta criminosa, ma anche la società colpevole di non essersi adeguatamente organizzata al fine di prevenire i reati. La filosofia della prevenzione e della responsabilizzazione raggiunge l'apice con il GDPR: una pioggia di regole d'ispirazione europea riecheggianti in quelle autoctone, nazionali, contenute nel codice privacy (D.lgs. 196/03), che richiedono attenzione perché temibile è l'entità della sanzione (fino al 4% del fatturato del consolidato). La pioggia di norme diventa tempesta se alle leggi sopra esplorate si aggiungono altre forze normative:

- le regole previste in materia di crisi di impresa, di antiriciclaggio, di anticorruzione e trasparenza, antitrust,
- le disposizioni in ambito di bilancio contabile e di sostenibilità, di cybersecurity,
- i regolamenti di settore, i codici di autodisciplina.

Le aziende devono proteggersi. Spontaneo l'approccio tradizionale di costruire Modelli organizzativi separati, indotti dalle norme confezionate dal legislatore in pacchetti distinti, concepiti ed efficaci in tempi diversi. Nondimeno, sono barriere a compartimenti stagni, magari pensati da attori differenti, senza connessione osmotica. Dalla pratica tradizionale, nelle aziende di medie e grandi dimensioni, nascono almeno tre Modelli per garantire la sicurezza:

i. delle persone in esecuzione del D.lgs. 81/ 2008,
ii. dell'azienda in esecuzione del D.lgs. 231/2001,
iii. dei dati in esecuzione del GDPR e del D.lgs. 196/2003 come modificato dal D.lgs. 101 20018.

È naturale da principio, al fine di evitare rischi e costi da mancata conformità, adottare ragionamenti a compartimenti separati, procedere all'esecuzione autonoma delle leggi e costruire Modelli organizzativi indipendenti. Nondimeno, questa visione tradizionale è datata. Le norme si prestano a letture simmetriche, unica la *ratio legis*, unico il moto ispiratore: la sicurezza e la prevenzione sono un comune denominatore. Anche la meccanica dei Modelli è gemellare: i Modelli organizzativi a tutela della società, delle persone e dei dati sono costruiti ad *hoc*, ritagliati sulla realtà operativa aziendale, seguono i mutamenti degli scenari normativi e dell'organizzazione societaria.
In questi tre ambiti: D.lgs. 231/2001, D.lgs. 81/2008, GDPR, interessa al legislatore una riflessione consapevole in termini di prevenzione dei rischi. Vale la pena cogliere questa opportunità, individuare le simmetrie normative nel miglior interesse dell'azienda, progettando un Modello organizzativo integrato, che includa le tre diverse discipline con possibilità di essere implementato, abbracciando anche altri quadri normativi la cui attuazione implica organizzazioni interne per la gestione e il controllo del rischio.

2. La contrazione del Modello organizzativo

Nelle realtà aziendali è presente una tradizionale attuazione dei *dictat* normativi. La separatezza del Modelli a tutela della sicurezza della società, delle persone e dei dati è suggerita dalle leggi che sono diverse e che richiedono diverse specializzazioni aziendali:

i. *HSE, Health, Safety & Environment*, collaborando con il dirigente delegato ex art. 16 del D.lgs. 81/08, si occupa per competenza specialistica dell'attuazione del D.lgs. 81/08 e della legge 152/06,
ii. il legale interno, quando istituito il *compliance officer*, si occupa solitamente di presidiare l'attuazione del D.lgs. 231/01 e sue successive modifiche e integrazioni,
iii. il DPO, *Data Protection Officer*, sorveglia la corretta attuazione del regolamento europeo (GDPR) e quindi contribuisce progettare un Modello organizzativo a tutela della privacy.

Senza una visione d'insieme, un disegno unitario, la tentazione di procedere all'attuazione separata dei diversi settori normativi è forte, ma gli svantaggi sono evidenti:

- duplicazioni inutili,
- antinomie gestorie,
- appesantimento degli apparati organizzativi.

Quando poi si ingaggiano consulenti diversi, perché diversi sono gli aggiudicatari delle gare organizzate dall'azienda, il rischio di pareri confliggenti e soluzioni non raccordate cresce. Adempiere ai dettati normativi secondo il metodo tradizionale dell'esecuzione separata delle leggi non è conveniente: produce una frammentazione ingiustificabile di tutele forse accettabile anni fa, ma oggi più che mai, per la migliore protezione aziendale, è auspicabile una lettura innovativa delle norme, basata su una visione di compliance trasversale. Le norme offrono l'occasione propizia: la contrazione dei modelli o comunque la progettazione di un Modello organizzativo in forma integrata. Sperimentare questo nuovo approccio, frutto di una visione innovativa di compliance, reca almeno i seguenti vantaggi:

- contenzione dei costi,
- uniformità di procedure e di controllo,
- omogeneità e congruenza documentale.

3. La costruzione di un Modello organizzativo integrato

La tutela dell'azienda, della sicurezza delle persone e dei dati, sottendono tutte una consapevole e meditata mappatura dei rischi. In primo luogo, occorre individuare i comuni denominatori: le *best practices* ISO 31000. Con tale strumento è possibile procedere a una mappatura unificata che abbracci tutti i rischi aziendali, evitando ragionamenti a compartimenti viziati da stratificazioni. Se si adotta un approccio valutativo d'insieme, è possibile individuare il rischio sulla base del principio di accountability, ossia di responsabilizzazione dell'impresa. Seguendo questo metodo, la società abbandona l'approccio tradizionale consistente nel semplice rispetto della normativa vigente, evolvendo a un approccio sostanziale (*risk based approach*) unificato. Del resto, le norme tracciano questa linea: la valutazione dei rischi è richiesta certamente dal Modello 231, così come dalla valutazione di impatto prevista dall'art. 35 del Regolamento (UE) 2016/679 e più in generale dall'adozione di un Modello di organizzazione *privacy*. L'obbligo di valutare i rischi è poi esplicito nel D.lgs. 81/08 in materia di Salute e sicurezza sui luoghi di lavoro che agli artt. 17, 28 e 29 introduce il Documento di Valutazione dei Rischi (DVR). La gamma dei rischi si apprende solitamente con interviste ai principali attori espressi dallo scenario dell'organizzazione aziendale, spesso il complemento è un sistema informatico che elabora i risultati delle interviste e produce la mappa e la pesatura degli stessi: i sistemi più evoluti indicano le misure per colmare i gap correlati a rischi non accettabili.
Se questo è il metodo, basta allargare l'ottica di valutazione ai principali rischi aziendali tenendo a mente il perimetro delle attività, non i confini normativi. Tale epilogo metodologico si presta a essere più conveniente, viene naturale agli addetti ai lavori (giuristi e manager) che si confrontano con le norme. L'utilizzo di tecniche RSA (*Risk Self Assessment*) può essere comune a tutti e tre gli ambiti in esame, giungendo poi a una valutazione più completa, che include:

i. l'andamento storico delle perdite operative per casi di non conformità,
ii. la componente reputazionale (con verifica di possibili effetti della reputazione su deterioramento o perdita di relazione con il cliente),
iii. le possibili conseguenze sul fatturato, di rilevanza per i fattori che generano il rischio.

Gli esperti della materia lo chiamano *Enterprise Risk Management*: un sistema omogeneo e sinergico che ingloba i rischi sotto vari profili e che si presta a essere utilizzato in sede di predisposizione di Modelli organizzativi integrati. Una mappatura unica dei rischi aziendali è conveniente perché meglio monitorabile in termini di manutenzione. Che si usi il metodo del *Tool* informatico per raccogliere ed elaborare le informazioni e/o il metodo delle sole interviste, adottare una visione allargata consente:

- risparmio di tempo e di costi,
- maggior controllo degli aggiornamenti normativi, organizzativi e di business.

Se immaginiamo di dover mappare il rischio di commissione di reati informatici, la metodologia integrata consente di individuare:

i. i profili di rischio rilevanti per prevenire ipotesi di responsabilità 231,
ii. i profili di rischio inerenti alla privacy (GDPR),
iii. i riverberi collaterali sul business e quelli reputazionali.

Gli standard internazionali in materia di governance per la sicurezza delle informazioni (ISO 27001:2013) e per il *business continuity* (ISO 22301:2019) sono preziosi strumenti per la costruzione del Modello organizzativo che prevenga condotte criminose informatiche e che, al contempo, garantisca la sicurezza dei dati, abbassando il rischio di *data breach*.
Esplorando l'ambito della sicurezza sul luogo di lavoro, il nucleo dei reati rilevanti richiama:

- l'art. 589 c.p.: omicidio colposo (commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro),
- l'art. 590 c.p.: lesioni personali colpose (commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro).

Per evitare doppie mappature contenenti rischi sovrapposti o descrizioni configgenti di uno stesso rischio, la soluzione va solo intuita e colta: ragionare in termini di Modelli organizzativi integrati. Anche la gestione del rischio fiscale di non conformità si presta a essere inglobata in un Modello organizzativo integrato. I delitti di frode fiscale sono collegabili a reati rilevanti ai fini della responsabilità amministrativa delle imprese:

- ai delitti tributari di cui all'art. 25-quinquiesdecies del D.Lgs. n. 231/2001,
- alla fattispecie dell'autoriciclaggio, di cui all'art. 648-ter.1 c.p. e inserito nell'art. 25-ocites del Decreto n. 231 del 2001.

Sono omozigoti i Modelli 231 e i Requisiti del D.lgs. del 5 agosto 2015, n. 128. La gemellarità degli strumenti di controllo si coglie nella genetica metodologica, ed emerge dalle scelte lessicali operate dal legislatore, che nel comma 1 dell'art. 4 Dlgs 128/2015 scrive:

«*Il contribuente che aderisce al regime* [di adempimento collaborativo] *deve essere dotato, nel rispetto della sua autonomia di scelta, delle soluzioni organizzative più adeguate al perseguimento dei relativi obiettivi, di un efficace sistema di rilevazione, misurazione, gestione e controllo del rischio fiscale, inserito nel contesto del sistema di governo aziendale e di controllo interno. Fermo il fedele e tempestivo adempimento degli obblighi tributari, il sistema deve assicurare:*

(a) *chiara attribuzione di ruoli e responsabilità ai diversi settori dell'organizzazione dei contribuenti in relazione ai rischi fiscali,*
(b) *efficaci procedure di rilevazione, misurazione, gestione e controllo dei rischi fiscali il cui rispetto sia garantito a tutti i livelli aziendali,*
(c) *efficaci procedure per rimediare ad eventuali carenze riscontrate nel suo funzionamento e attivare e necessarie azioni correttive*».

Al comma 2: «*il sistema di rilevazione, misurazione, gestione e controllo del rischio fiscale prevede, con cadenza almeno annuale, l'invio di una relazione agli organi di gestione per l'esame e le valutazioni conseguenti. La relazione illustra, per gli adempimenti tributari, le verifiche effettuate e i risultati emersi, le misure adottate per rimediare a eventuali carenze rilevate, nonché le attività pianificate*».
È il *Tax Control Framework* (TCF) lo strumento di cui diverse aziende si dotano al fine di gestire i rischi fiscali e realizzare la cooperazione rafforzata fisco-contribuente. Anche su questo fronte si potrebbero sfruttare le sinergie che le norme consentono, praticando ragionamenti di *compliance* integrata e progettando un Modello organizzativo dall'efficacia amplificata. Così facendo, si supera il metodo tradizionale di valutazione frammentata dei rischi, che deriva dalla pluralità di mappature.
La sfida è trasformare il disagio di una sequenza di interviste necessarie a mappare i rischi in una opportunità per sfruttare questi snodi di conoscenza con una visione multidisciplinare della legalità d'impresa: l'approccio *risk-based* accomuna tutte le normative esaminate. La gestione integrata della *compliance* si impone come brillante soluzione: sprigiona vantaggi competitivi, mira a focalizzare l'impegno sulle aree di rischio, garantisce il coordinamento tra tutte le componenti normative e trasforma la *compliance* da fattore di costo a fattore di valore aggiunto.

4. Procedure plurivalenti

Se unica è la mappatura, più facile è progettare e costruire procedure plurivalenti. A ragionare prigionieri degli steccati normativi si rischiano processi e regole ridondanti, tanto da costituire una selva oscura piuttosto che una guida per l'utente che rischia di smarrirsi fra le disposizioni costruite dalla preoccupazione aziendale di doversi schermare il più possibile. Nondimeno, in più di un ambito, è possibile costruire un unico processo plurivalente a prevenzione e protezione del rischio che conduca l'agire aziendale in conformità con la legge sulla privacy, con il Dlgs 231/2001 e con il Dlgs. 81/08.
In alcuni casi è il legislatore che suggerisce esplicitamente procedure bivalenti. Un esempio pratico si coglie a leggere la disciplina sull'antiriciclaggio. Perché il Modello organizzativo sia idoneo, urgono procedure interne all'azienda per prevenire condotte ricollegabili ai fenomeni di *money laundering*. Ma a guardare bene le norme, è chiaro il punto di contatto fra disciplina 231 e disciplina sulla privacy. L'art. 16 del D.lgs. 231/07, nel trattare le procedure di mitigazione del rischio, stabilisce:

a) al comma 3 che *«i soggetti obbligati adottano misure proporzionate ai propri rischi, alla propria natura e alle proprie dimensioni, idonee a rendere note al proprio personale gli obblighi cui sono tenuti ai sensi del presente decreto, ivi compresi quelli in materia di protezione dei dati personali»,*
b) al comma 4 che *«i sistemi e le procedure adottati ai sensi del presente articolo rispettano le prescrizioni e garanzie stabilite dal presente decreto e dalla normativa vigente in materia di protezione dei dati personali»*.

Le norme fissano un principio irrinunciabile: la procedura che l'azienda adottasse per arginare il rischio di prevenzione di questo reato sarà informata anche al rispetto della normativa privacy contenuta nel GDPR. Poiché tutta la normativa antiriciclaggio si erge per sua intrinseca natura sui dati personali dei clienti e sul trattamento di tali dati per finalità di contrasto al riciclaggio, il rispetto del GDPR si impone. I destinatari delle norme, per adempiere ai propri obblighi di adeguata verifica del cliente, di controllo costante, di segnalazione delle operazioni sospette e conservazione delle informazioni, devono necessariamente gestire, analizzare e conservare dati personali nel rispetto della normativa di settore e dei principi di *accountability* e proporzionalità. Gli adempimenti antiriciclaggio comportano obblighi di identificazione, conservazione dei dati personali e segnalazione di operazioni sospette: è evidente la bivalenza dello strumento procedurale. Tali attività costituiscono a tutti gli effetti trattamento dei dati protetti regolamentati dal GDPR. Di conseguenza, un Modello organizzativo che ambisca a una valutazione di idoneità *banco iudicis*, dovrà bandire procedure ipertrofiche e privilegiare protocolli comportamentali lineari, concepiti in un'ottica di *compliance* integrata. Ne deriva una procedura aziendale strutturata che comprende:

i. l'informativa ai clienti nella quale si specifichi che il trattamento dei dati avverrà per le finalità previste dalla normativa antiriciclaggio,
ii. l'individuazione dei soggetti incaricati al trattamento debitamente istruiti e formati sulle operazioni da compiere,
iii. il ricorso a credenziali di autenticazione per l'accesso ai dati conservati elettronicamente
iv. l'identificazione di misure tecniche atte a prevenire la perdita delle informazioni, prevenzione dei rischi di distruzione o perdita dei dati,
v. la determinazione dei tempi di conservazione dei dati giustificati dalla finalità del trattamento.

Le procedure nate dall'attuazione normativa separata si stratificano nella realtà organizzativa aziendale, producendo regole interne frammentate. Per numero e mole, questi strumenti invece di rendersi utili, si mutano in percorsi labirintici che mal si combinano con un solido Modello di prevenzione. Un protocollo nato da una visione di *compliance* integrata, ispirato da uno sforzo di riflessione multidisciplinare, snellisce gli apparati e costituisce l'occasione di sintesi attuativa per la migliore tutela societaria. Altro esempio di processo a valenza multipla riguarda la disciplina del *whistleblowing*. La tutela richiamata dalla norma implica:

i. divieto di ritorsioni,
ii. riservatezza dell'identità del segnalante,
iii. sanzioni disciplinari per chi viola le misure di tutela del segnalante o presenta con dolo o colpa grave segnalazioni che si rivelano infondate.

La regolamentazione del *whistleblowing* nel settore privato è attualmente contenuta nei commi 2-*bis*, 2-*ter* e 2-*quater* dell'art. 6 della L. 231/2001, introdotti dalla L. n. 179 del 2017: nondimeno, il quadro normativo si complica per le banche, le assicurazioni, e l'attività di intermediazione finanziaria (settori particolari nei quali vigono regole specifiche). Anche il settore pubblico è normato *ad hoc* (art. 54 del D.lgs 165/2001). Qualunque sia il comparto o il settore, la novità normativa viene tradotta in molti codici etici aziendali e impone procedure fitte di regole per guidare i dipendenti alla segnalazione di comportamenti in spregio al Modello o che costituiscano reato.
Gli interessati, ossia i soggetti i cui dati sono trattati da parte del titolare nella procedura di *whistleblowing* sono:

i. il segnalante,
ii. il segnalato,
iii. eventuali terzi cui si fa riferimento (direttamente o indirettamente) nella segnalazione.

Qualunque sia la procedura costruita dall'azienda, perché sia idonea, il canale dedicato alla segnalazione deve essere sicuro e certamente conforme alla disciplina relativa al trattamento di dati. Quelli maneggiati in tale ambito riguardano:

i. l'identificazione del segnalante, dei segnalati e delle altre persone coinvolte (identità, funzioni e recapiti),
ii. i fatti segnalati,
iii. gli elementi raccolti nella verifica,
iv. il rendiconto delle operazioni di verifica e l'epilogo della segnalazione.

L'impresa che appronta un protocollo di *whistleblowing* è titolare del trattamento ovvero il soggetto che *determina le finalità e i mezzi del trattamento di dati personali* (art. 4, n. 7 GDPR).
Per il titolare accorto, proteggere i dati significa:

- fornire moduli di segnalazione che guidino il solerte denunciante e gli impediscano il rigurgito di informazioni eccedenti rispetto al fatto narrato (se si seguono i metodi tradizionali),
- verificare la sicurezza della piattaforma, limitare i dati protetti da cifratura, dotarsi di preziosi strumenti tecnici *ad adiuvandum* (se si utilizza una piattaforma informatica).

Impera in questa materia il principio di minimizzazione: i dati raccolti nella procedura di segnalazione sono solo quelli necessari per il raggiungimento della finalità perseguita. I dati ulteriori non potranno essere oggetto di trattamento. Nondimeno, che sia una piattaforma informatica, o la più tradizionale modulistica cartacea, il titolare deve conservare solo le informazioni indispensabili per definire la strategia processuale che l'azienda si trovasse a scegliere. E qui si fa strategica la collaborazione fra OdV e DPO, e si aprono frontiere di vigilanza integrata. L'OdV, soggetto preposto al controllo sul funzionamento e il rispetto del Modello 231 è senza dubbio coinvolto in concorso con il DPO:

- nella valutazione di adeguatezza della procedura di *whistleblowing,*
- nel vigilare sul corretto corso delle indagini difensive interne.

Il DPO, coprotagonista nell'attività di controllo, avrà senz'altro un ruolo nella procedura: essendo la figura di riferimento in materia di protezione di dati personali egli si pone come supervisore dell'attività del

titolare, e in tale veste deve vigilare sulla attribuzione delle responsabilità, sulla sensibilizzazione e sulla formazione del personale, oltre a effettuare assieme all'OdV le relative attività di controllo sul corretto svolgimento delle investigazioni difensive condotte dall'azienda. Nell'improntare un protocollo di *whistleblowing* attuando ragionamenti di *compliance* integrata, la società si troverà a costruire protocolli a valenza multipla con utilità amplificata. Nell'indicare le modalità di effettuazione della segnalazione, qualificandosi titolare del trattamento, la società:

- **i.** verificherà il rispetto dei principi previsti dall'art. 5 del GDPR,
- **ii.** si assicurerà che la tutela delle identità degli interessati sia effettiva,
- **iii.** vigilerà perché all'interno della organizzazione i soggetti che attuano la procedura di segnalazione ricevano specifiche istruzioni e una adeguata formazione sulla attività da svolgere,
- **iv.** dichiarerà le finalità del trattamento, la durata del periodo di conservazione.

5. Deleghe multiuso

L'insieme delle norme che impongono alle aziende uno sforzo di conformità genera un vortice documentale di deleghe e procure: il legislatore le esige ordinate. La chiave è un Modello integrato che consenta la centralizzazione, gestione e l'aggiornamento delle deleghe, di monitorarne le scadenze o gli adeguamenti ai cambi organizzativi o normativi. In ogni caso, a prescindere dal monitoraggio centralizzato delle deleghe, anche sui contenuti sarebbe possibile teorizzare una implementazione che tenga conto delle diverse necessità imposte dalle diverse normative. Per esempio, l'OdV è individuato e nominato dal CDA, con conseguente attribuzione di compiti, spesso novando la declinazione delle responsabilità nell'atto di nomina.
Recentemente il Garante per la privacy ha precisato:

«*Sulla base delle valutazioni sopra riportate, si ritiene che l'OdV, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongano siano interni o esterni, debba essere considerato "parte dell'ente". Il suo ruolo si svolge nell'ambito dell'organizzazione dell'ente, titolare del trattamento, che, attraverso la predisposizione dei modelli di organizzazione e di gestione, definisce il perimetro e le modalità di esercizio di tali compiti. Tale posizione si intende ricoperta dall'OdV nella sua collegialità, tuttavia, non può prescindersi dalla necessità di definire anche il ruolo che, in base alla disciplina in materia di protezione dei dati personali, deve essere previsto per i singoli membri che lo compongono. Lo stesso ente, in ragione del trattamento dei dati personali che l'esercizio dei compiti e delle funzioni affidate all'OdV comporta, designerà i singoli membri dell'OdV quali soggetti autorizzati (artt. 4, n. 10, 29, 32 par. 4 Regolamento)».*

Stesso metodo può essere seguito per costruire la delega/procura a individuare il dirigente delegato *ex* art. 16 D.lgs. 81/08, quale supporto per inserirvi tutte le istruzioni del titolare sul corretto trattamento dei dati, tanto più che quelli gestiti dai dirigenti sono dati riguardanti lo stato di salute o i rischi specifici legati alla mansione e alla idoneità del singolo lavoratore rispetto alla mansione.
A ben vedere, le organizzazioni aziendali si ergono su procure e deleghe che si prestano a essere implementate alla luce della normativa privacy, divenendo strumenti multiuso.

6. Le norme etiche
Con le norme etiche si promuove:

- **i.** la parità sul luogo di lavoro,
- **ii.** la salute e sicurezza dei lavoratori,
- **iii.** la tutela dell'ambiente.

e si gestiscono in modo responsabile:

iv. i rapporti con i fornitori e con la pubblica amministrazione (corruzione pubblica e privata),
v. la tutela del diritto alla privacy di tutti gli stakeholder,
vi. il *modus operandi* sui mercati con lealtà e trasparenza,
vii. i valori guida per evitare condotte che possano integrare reati contro l'industria e il commercio,
viii. le condotte volte a foraggiare il terrorismo, il lavoro irregolare e l'ampio catalogo di reati rilevanti in ambito Dlgs 231/2001: reati tributari, informatici, reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, autoriciclaggio.

Queste le caratteristiche del codice etico:

i. complemento del Modello organizzativo che ambisca a essere considerato idoneo *banco iudicis,*
ii. strumento per attuare in forma integrata le norme contenute nei tre pacchetti,
iii. compendio di policy e regole, che accoglie le politiche etiche e i perimetri normativi fin qui esaminati,
iv. dimostrazione dell'impegno delle aziende a prevenire la commissione dei reati rilevanti alla luce del Dlgs 231/2001 e a ridurre i rischi aziendali, se ben strutturato e diffuso.

Il codice etico ha la finalità di guidare le decisioni delle risorse interne ed esterne alle aziende, di compiere azioni coerenti con la cultura della responsabilità e della legalità. Spesso detto codice include il sistema disciplinare, acquisisce efficacia deterrente e sanzionatoria a scapito dei trasgressori di protocolli e norme etiche: si presta molto bene a essere progettato con una visione integrata e in ottica multidisciplinare.

7. La formazione multidisciplinare

La formazione multidisciplinare è l'occasione per diffondere i principi di un Modello integrato che garantisca la *compliance* alle norme sulla sicurezza delle persone dei dati e della società: unico il contenitore, unica la diffusione, unica la formazione, pur mantenendo un dettaglio profilato.
Il legislatore la rende obbligatoria:

A) in materia di salute e sicurezza sul lavoro, in occasione della costituzione del rapporto di lavoro, del mutamento di mansioni o della introduzione di nuove attrezzature o tecnologie e deve essere periodicamente ripetuta,
B) in tema di privacy, per il responsabile del trattamento dei dati o chiunque agisca sotto la sua autorità o che abbia accesso a dati personali ,
C) sul Modello 231 adottato dalla società, nei confronti della popolazione aziendale.

La formazione si articola in moduli ed è suddiviso per pacchetto normativo di volta in volta di interesse per i differenti apparati aziendali. A fine corso è previsto un test, per comprovare la trasmissione dei contenuti dal docente al discente.

8. I flussi informativi e i comitati di controllo

Il D.lgs. 231/2001 esige un'organizzazione che preveda flussi informativi verso l'OdV e dall'OdV verso il Cda. Simmetricamente, in tema di privacy, la norma impone che i dipartimenti aziendali riferiscano periodicamente al DPO i profili di criticità del Modello. Anche il Dirigente delegato *ex* art. 16 D.lgs. 81/08 raccoglie e genera flussi (ISO 45000 enfatizza il dialogo strutturato sui temi della sicurezza dei lavoratori). Se si abbattono le barriere dei perimetri normativi e si segue la logica dei Modelli integrati, sarebbe possibile

organizzare altresì flussi informativi sincroni, con la creazione di comitati di controllo per il miglior monitoraggio dei rischi: DPO, OdV, Dirigente delegato *ex* art. 16 del D.lgs. 81/08.
Ci sono ambiti dal confine labile fra D.lgs. 231/2001 e privacy, basti pensare ai reati informatici la cui prevenzione interessa tanto all'OdV quanto al DPO, o alla sicurezza delle persone che riguarda sia l'OdV sia Dirigente delegato *ex* art. 16 del D.lgs.81/08 e DPO.
Un Modello integrato si basa su flussi informativi coordinati, sul dialogo strutturato fra soggetti incaricati di effettuare controlli periodici. La chiave per ottenere il massimo risultato è la sinergia: intuire che leggi frammentate possano creare un'opportunità di lavoro integrato nell'ambito del quale i controller (OdV, DPO, dirigente delegato e dirigente preposto alla corretta tenuta dei documenti contabili) si riuniscono regolarmente in un comitato per il controllo interno, e si confrontano sulla gestione dei rischi, organizzandolo con protocolli di prevenzione di sicura efficacia, perché ispirati da una visione d'insieme.
La *compliance* integrata è la svolta, i Modelli di organizzazione progettati con una visione integrata sono avanguardia della migliore tutela aziendale: un concetto sfidante per le aziende che hanno:

i. la necessità di stare al passo con la normativa e la sua evoluzione,
ii. l'esigenza di contenere i costi,
iii. l'obiettivo di mantenere un corretto bilanciamento tra le attività di business e le richieste di adeguamento alla normativa.

Se raccolta come un'opportunità di organizzare al meglio i propri presidi di controllo, la *compliance* integrata può fornire valore aggiunto nella gestione dei rischi. Il Modello integrato è un'idea progressista, che si presta per genesi a essere strumento in grado di abbracciare le diverse esigenze dettate dalla legge.

19 aprile 2021

A cura di Avv. Bruna Capparelli