GIURISPRUDENZA PENALE

RESPONSABILITÀ DEGLI ENTI: PROBLEMATICHE E PROSPETTIVE DI RIFORMA A VENTI ANNI DAL D. LGS. 231/2001

2021/1-BIS

Dal D.lgs. 231/2001 al GDPR (Regolamento UE 2016/679) attraversando il D.lgs. 81/2008: il modello di organizzazione gestione e controllo integrato, avanguardia di un progetto di attuazione normativa combinata, un'opportunità per le aziende da intuire e cogliere.

di Milena Cirigliano

15 Dal D.lgs. 231/2001 al GDPR (Regolamento UE 2016/679) attraversando il D.lgs. 81/2008: il modello di organizzazione gestione e controllo integrato, avanguardia di un progetto di attuazione normativa combinata, un'opportunità per le aziende da intuire e cogliere.

di Milena Cirigliano

Abstract

La compliance integrata per la governance d'impresa è il futuro.

I sistemi organizzativi a protezione della società, del lavoratore e dei dati, possono essere intesi come complementari, progettati con una visione unitaria; le norme si prestano a letture simmetriche.

Il legislatore comanda da anni alle aziende sforzi seri e misure consapevoli a protezione del rischio in almeno tre grossi ambiti:

- responsabilità amministrativa delle società, ma penale è il giudicante, penale è la sede della ritualità processuale (D.lgs. 231/2001);
- salute e sicurezza del lavoratore, il D.lgs. 81/2008 impone un modello organizzativo a garanzia della sicurezza sul luogo di lavoro, matrice normativa questa che, con il primo decreto, si interseca ed innesta, con simmetrici riverberi penali;
- protezione dei dati personali: GDPR e D.lgs. 101/2018, con mostruose misure sanzionatorie (fino al 4% del fatturato del consolidato) per le aziende che operino in spregio alle norme ed alle raccomandazioni del Garante. La declinazione dei reati informatici spicca in tale ambito ed esige una prevenzione del rischio a doppia valenza (D.lgs.231/2001 e privacy).

Se le leggi hanno natali diversi, "*la ratio*" sembra muovere da un comune sentire giuridico, da un unico moto ispiratore, le richieste organizzative si assomigliano tutte. A leggerle in parallelo le tre normative hanno pretese gemelle, identiche esigenze di compliance e impongono modelli di Organizzazione Gestione e Controllo (MOGC) che possono essere immaginati e progettati con un'ottica innovativa: in forma integrata.

Sia il D.lgs. 231/2001 che il D.lgs. 81/2008 e da ultimo il GDPR implicano mappature dei rischi, procedure, regole etiche, procure chiare, atte a prevenire la consumazione di condotte criminose; organi e organismi di vigilanza (DPO, ODV, Dirigente delegato ex art 16 del D.lgs. 81/2008) a presidio del castello organizzativo. Se si ragiona in maniera integrata, si ottimizza e si colgono le migliori opportunità di un agire sicuro. La partitura degli sforzi aziendali non presenterebbe dissonanze, né duplicazioni e brillerebbe per efficacia.

Un progetto organizzativo pensato invece tradizionalmente, in un'ottica di esecuzione separata delle richieste del legislatore confezionate nei diversi pacchetti normativi (D.lgs. 231/2001, D.lgs. 81/2008, GDPR) se eseguito a compartimenti stagni, implica spesso duplicazioni di sforzi, regole e procedure, perde la convenienza delle sinergie, rinunciando alle opportunità offerte da un ragionamento di attuazione normativa combinata.

La trama integrata dei modelli di organizzazione gestione e controllo è tessuta con mappature dei rischi unificabili, procedure plurivalenti, organismi di vigilanza e controllo (DPO, ODV, Dirigente Delegato) in comunicazione osmotica e sincrona tra loro, riuniti in comitati periodici per la valutazione e gestione dei rischi. Il MOGC integrato è un'opportunità di sintesi innovativa per attuare la legalità d'impresa, che va solo intuita e colta.

Integrated management and control organisation models: From Legislative Decree No. 231/2001 to the GDPR (EU Regulation 2016/679), passing through Legislative Decree No. 81/2008 –
The forerunners of a plan to enact integrated legislation that companies should understand and assimilate
Abstract

Integrated corporate governance compliance is the future.

Organisational systems that protect companies, workers and data are to be envisaged as complementing each other and have been conceived as a whole. The provisions governing them can, therefore, be analysed in conjunction with each other.

Italian lawmakers have, for many years now, been requiring companies to make serious efforts and knowingly take measures that protect them from risk in at least three major areas, namely:

- *companies' administrative liability, even though the courts called upon to judge whether there is any such administrative liability are criminal courts that do so according to the Italian Code of Criminal Procedure (Legislative Decree No. 231/2001 and subsequent amendments);*
- *workers' health and safety; Legislative Decree No. 81/2008 imposes an organisational model that guarantees safety in the workplace: this legislation intersects with and is based on Legislative Decree No. 231/2001, which also has repercussions from a criminal law point of view;*
- *protection of personal data (GDPR and Legislative Decree No. 101/2018), which leads to monstrous fines (i.e. up to 4% of consolidated revenues) being imposed on companies that run their businesses in defiance of the orders issued and recommendations given by the Italian Data Protection Authority; IT-related criminal offences are of great importance in this area and require the adoption of a double-risk prevention strategy (Legislative Decree No. 231/01 and privacy).*

Even though the legislation comes from different sources, the line of reasoning on which it is based seems to be inspired by the same legal philosophy. All of the organisational requirements are also similar. When reading the three laws together, one realises, in fact, that they have two requirements: They have the same compliance requisites and impose Organisation, Management and Control Models (OMCMs) that can be imagined and conceived in an integrated fashion and can be of an innovative nature.

Both Legislative Decree No, 231/2001 and Legislative Decree No. 81/08, as well as the GDPR, envisage clear risk mapping activities, procedures, ethical rules and powers of attorney. This is done with a view to preventing criminal conduct being engaged in; supervisory officers and bodies (DPOs, SBs, Officers appointed in accordance with Article 16 of Legislative Decree No. 81/08) must oversee the company's organisational structure. The best opportunities for acting safely are optimised and seized when companies think in an integrated manner. Ensuring that such efforts are conducted by officers inside the company does not give rise to contradictions or duplications and the effectiveness thereof is evident.

An organisational plan that has, with a view to meeting the requirements imposed by the applicable legislation, been conceived, on the basis of which law such requirements arise from (i.e. Legislative Decree No. 231/2 001, Legislative Decree No. 81/2008, GDPR), in a traditional manner leads, on the other hand, to the company's efforts, rules and procedures being duplicated and also leads to such company missing out on convenient synergies and giving up the opportunities provided by a combined legislative compliance approach.

The organisation, management and control models' integrated structures consist of risk mappings and multi-value procedures, as well as supervisory and control bodies (DPOs, SBs, Appointed Officers) that permeate each other. They are synchronised with each other and meet from time to time in risk assessment and management committees. Integrated OMCMs provide an opportunity to bring together innovations and ensure that lawful practices are implemented inside the company. Such practices must, therefore, be understood and assimilated.

Sommario:

1. Il quadro storico-normativo

Il legislatore è bulimico quando chiede alle aziende di prevenire i rischi di commissione dei reati e di adottare misure serie a riduzione degli stessi.

A volte sente l'esigenza di curare questa patologia che affligge gli ordinamenti e razionalizzare il disordine normativo, emana per esempio il D.lgs. 626/94, che recependo ben otto direttive europee sulla sicurezza e l'igiene sul lavoro, attua la mutazione di sistema da normativo risarcitorio a sistema essenzialmente 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 giuridico italiano la "colpa di organizzazione" imputata all'ente, radicata nella carenza di controllo e di vigilanza, nonché nell'assenza di misure di prevenzione

protezione.
Compare nella partitura normativa nazionale un canone inverso: *societas delinquere potest;* e se il reato è commesso a vantaggio e nell'interesse dell'ente, il vuoto organizzativo colpevole, accertato in sede penale, è sanzionato con pene rilevanti e temibili:

- sanzioni pecuniarie commisurate alle condizioni economiche e patrimoniali dell'Ente, da applicare tout court;
- sanzioni interdittive, che nei casi più gravi comportano l'interdizione dall'esercizio dell'attività, mentre nei casi meno gravi, il divieto di pubblicizzare beni o servizi, di contrattare con la pubblica amministrazione o l'esclusione da agevolazioni, finanziamenti, sussidi, etc.;
- confisca, anche per equivalente, del prezzo o profitto del reato[1];
- pubblicazione della sentenza, qui saltano agli occhi i riverberi reputazionali.

Che si tratti di responsabilità amministrativa o penale è questione sintattica più che affascinante discussione giuridica[2]; certo è che penale è il giudicante, penale la sede di accertamento della responsabilità dell'ente. La liturgia processuale diventa bifida: se il reato è fra quelli declinati dal D.lgs. 231/2001(e ss. mm. ii.) 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 che da declinazione minimalista nel tempo il legislatore ha reso "catalogo".
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)[3] che incutono grande rispetto poiché temibile è l'entità della sanzione (fino al 4% del fatturato del consolidato).
La pioggia di norme diventa tempesta a tratti tsunami 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, nonché in ambito di bilancio contabile e di sostenibilità, di cybersecurity, per non dimenticare i regolamenti di settore[4], i codici di autodisciplina, qui le regole si amplificano per le quotate. Alle aziende tocca proteggersi. Spontaneo l'approccio tradizionale tirare su modelli di organizzazione gestione e controllo separati, indotti dalle norme confezionate dal legislatore in pacchetti distinti, concepiti ed efficaci in tempi diversi; ma 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 di organizzazione e gestione e controllo per garantire la sicurezza:
- delle persone in esecuzione del D.lgs. 81/ 2008;
- dell'azienda in esecuzione del D.lgs. 231/2001;
- 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[5], adottare ragionamenti a compartimenti stagni, procedere all' esecuzione separata delle leggi e costruire modelli organizzativi segregati dagli steccati normativi.
Ma è superata questa visione tradizionale, è datata, ed a ben guardare sconveniente. 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 di organizzazione gestione e controllo a tutela della società, delle persone, dei dati, sono costruiti ad hoc ritagliati sulla realtà operativa aziendale non sono statici ma dinamici, seguono i mutamenti degli scenari normativi e dell'organizzazione della società.
In questi tre ambiti (D.lgs. 231/2001, D.lgs. 81/2008, GDPR) ma il ragionamento è estensibile ad altri perimetri normativi, interessa al legislatore una riflessione consapevole e meditata in termini di prevenzione dei rischi, val la pena cogliere questa opportunità, individuare e sfruttare le simmetrie normative nel miglior interesse dell'azienda progettando un MOGC integrato che includa le tre diverse discipline (D.lgs. 231/2001, D.lgs. 81/08, GDPR) con evidenti possibilità di essere implementato abbracciando anche ulteriori quadri normativi la cui attuazione implica organizzazioni interne in termini di gestione e controllo del rischio.

2. La crasi dei modelli

Nelle grosse realtà aziendali è presente perlopiù una tradizionale attuazione dei *dictat* normativi. La separatezza del modelli di organizzazione gestione e controllo a tutela della sicurezza della società, delle persone, dei dati, è suggerita dai natali delle leggi che sono diversi e dalle attribuzioni organizzative che coltivano esecuzioni normative a progetto, imputandole solitamente a diverse specializzazioni aziendali: l'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; il legale interno (quando istituito il compliance officer) si occupa solitamente di presidiare l'attuazione del D.lgs. 231/01 e sue successive modifiche ed integrazioni; il DPO (Data Protection Officer) sorveglia la corretta attuazione del regolamento europeo (GDPR) e quindi contribuisce progettare un modello di organizzazione gestione e controllo a tutela della privacy. Senza una visione d'insieme, un disegno unitario, la tentazione di procedere all'attuazione separata dei diversi pacchetti normativi è forte ma gli svantaggi saltano agli occhi: brulicano le duplicazioni, le sovrastrutture e si appesantiscono gli apparati organizzativi.
Quando poi si ingaggiano consulenti diversi (per pacchetto) perché diversi sono gli aggiudicatari delle gare organizzate dall'azienda, il rischio di pareri confliggenti e soluzioni non raccordate lievita.
Adempiere ai dettati normativi secondo il metodo tradizionale dell'esecuzione separata delle leggi, non è conveniente: produce schermi frammentati di tutela a pacchetto forse giustificabile anni fa, ma oggi più che mai, per la migliore protezione aziendale, è auspicabile una lettura innovativa e combinata delle norme basata su una visione di compliance integrata. Le norme offrono un'occasione propizia: "la crasi dei modelli" o comunque la progettazione di un modello di organizzazione, gestione e controllo in forma integrata.
Osare, sperimentare questo nuovo approccio, frutto di una visione innovativa di compliance, reca vantaggi che saltano agli occhi:
saving di costi;
evitare duplicazioni procedurali e di controllo;
omogeneità e congruenza documentale.

3. Come costruire un modello integrato

In primo luogo, occorre individuare i comuni denominatori. La tutela dell'azienda, della sicurezza delle persone e dei dati, sottendono tutte una consapevole e meditata mappatura dei rischi, a guardare le best practices, ISO 31000 che guida gli esperti nel risk assessment si presta ad essere un arnese multiuso; metodica comune a tutte le diverse discipline. Con tale strumento è possibile ed auspicabile procedere ad una mappatura unificata che abbracci tutti i rischi aziendali, evitando ragionamenti a compartimenti stagni spesso viziati da duplicazione, sovrapposizioni e stratificazioni.
Se si adotta un approccio valutativo d'insieme le tessere di individuazione del rischio singolarmente intese, come frammenti di un prezioso mosaico si compongono in un quadro unico montato sul principio di *accountability*, ossia di responsabilizzazione dell'ente stesso trasversale a ben guardare in tutti e tre i pacchetti.
La società chiamata dal legislatore a valutare i propri rischi a documentarli per una consapevole pesatura degli stessi, seguendo il metodo proposto, abbandona l'approccio tradizionale consistente nel semplice rispetto della normativa vigente, evolvendo ad un approccio sostanziale (risk based approach) unificato. Le norme tracciano questa linea: La valutazione dei rischi è richiesta certamente dal Modello di Organizzazione, Gestione e Controllo ex art. 6, comma 2, del D.lgs. 231/01, così come dalla valutazione di impatto prevista dall'art. 35 del Regolamento (UE) 2016/679 (finalizzata a misurare le ripercussioni sui diritti e le libertà delle persone dovute ad un'eventuale violazione dei dati personali) e più in generale dall'adozione di un modello di organizzazione gestione e controllo 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 attraverso 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 ad essere più conveniente, viene naturale agli addetti ai lavori (giuristi e manager) che, scevri da visioni atomistiche[6], maneggiano l'arnese delle norme. L'utilizzo di tecniche RSA (Risk Self Assessment) per la valutazione del rischio potenziale collegato ad eventi di non conformità, può essere comune a tutti tre gli ambiti normativi in esame, in tale ottica integrata si possono sfruttare le sinergie possibili al fine di rappresentare in una valutazione più completa: l'andamento storico delle perdite operative per eventi di non conformità, la componente reputazionale, valutando possibili effetti della stessa su deterioramento o perdita di relazione con il cliente, possibili conseguenze su volumi fatturato, rilevanza mediatica dei fattori generatori di rischio. Gli esperti della materia lo battezzano Enterprise Risk Management[7]; un sistema omogeneo e sinergico che ingloba i rischi sotto vari profili e che ben si presta ad essere utilizzato alla luce di diverse normative. Una

mappatura unica dei rischi aziendali è conveniente perché meglio monitorabile e implementabile anche in termini di manutenzione. Che si usi il metodo del Tool informatico per raccogliere ed elaborare le informazioni essenziali ad una completa individuazione dei rischi e/o il metodo delle sole interviste in voga da anni, adottare una visione allargata consente senza dubbio un saving di tempo e costi e di monitorare più agevolmente gli aggiornamenti derivanti dai mutamenti esogeni (degli scenari normativi) o endogeni (organizzativi e di business).

Se immaginiamo di dover mappare il rischio di perfezionamento dei reati informatici, la metodologia integrata consente di individuare e pesare sia i profili di rischio rilevanti al fine di prevenire ipotesi di responsabilità amministrativa dell'ente alla luce del D.lgs. 231/2001 e s.s.m.i., sia i profili di rischio inerenti la privacy (GDPR) ma anche i riverberi collaterali sul business e quelli reputazionali. I principali standard internazionali in materia di governance in riferimento alla sicurezza delle informazioni (ISO 27001:2013) e in riferimento alla business continuity (ISO 22301:2019) sono preziosi strumenti di lavoro per un modello organizzativo a tenuta che prevenga al meglio le condotte criminose appartenenti all'alveo dei reati informatici ed al contempo sia idoneo a garantire la sicurezza dei dati riducendo il rischio di data breach.

Si respirano conferme di questi ragionamenti a leggere gli standard internazionali, la Direttiva NIS1148/2016 ed il DL 105/2019 sul perimetro di sicurezza nazionale cibernetico; letture che a ficcarci il naso, avvallano l'adozione di una visione multi disciplinare e integrata delle organizzazioni aziendali.[8]

Esplorando l'ambito della sicurezza sul luogo di lavoro il nucleo dei reati rilevanti in ambito 231, richiama l'art. 589 c.p. – Omicidio colposo (commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro); e l'art. 590 c.p. – Lesioni personali colpose (commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro) e presuppone rischi certamente e per definizioni già mappati in un DVR che si rispetti. Per evitare doppie mappature contenenti rischi sovrapposti o magari descrizioni configgenti di uno stesso rischio, misure di contenimento dei rischi duplicate, la soluzione va solo intuita e colta: ragionare in termini di modelli integrati.

Anche la gestione del rischio fiscale di non conformità si presta bene ad essere inglobata in un modello di organizzazione gestione e controllo integrato. I delitti di frode fiscale sono collegabili a reati rilevanti ai fini della responsabilità amministrativa degli enti (in primo luogo ai delitti tributari di cui all'art. 25-quinquiesdecies, D.Lgs. n. 231/2001 e alla fattispecie criminosa dell'autoriciclaggio, di cui all'art. 648-ter.1 del Codice penale, introdotto dalla Legge n. 186/2014 e inserito nell'art. 25-ocites del ripetuto Decreto n. 231 del 2001). Sono "omozigoti" i modelli di organizzazione gestione e controllo descritti dagli articoli 6 del Dlgs 231/2001 e 4 ("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 e sintattiche operate dal legislatore che nel comma 1 dell'art. 4 Dlgs 128/2015 scrive: "*Il contribuente che aderisce al regime (ndr: "regime di adempimento collaborativo") deve essere dotato, nel rispetto della sua autonomia di scelta delle soluzioni organizzative più adeguate per il 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) una 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.* 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*>>. E' il "Tax Control Framework[9]" (TCF) lo strumento di cui diverse aziende si dotano al fine di gestire i rischi fiscali e realizzare la "cooperazione rafforzata" fisco-contribuente, con i benefici che ne derivano,[10] ad un analisi istologica delle componenti, questo sistema di controllo mostra struttura e contenuto analoghi a quelli del Modello di Organizzazione, Gestione e Controllo previsto dall'art. 6 del D.Lgs. n. 231/2001, anche su questo fronte si potrebbero sfruttare le sinergie che le norme consentono, praticando ragionamenti di compliance integrata e progettando un modello di Organizzazione Gestione e Controllo dall'efficacia amplificata.

Si supera in tal modo il metodo tradizionale di valutazione frammentata dei rischi che deriva

da una pluralità di progetti simmetrica ad una pluralità di mappature. Tale metodologia genera documenti diversi e stratificati che mostrano ad un'analisi comparata alee sovrapponibili, informazioni incoerenti e/o duplicate, controlli ridondanti, alti costi di gestione, coinvolgimento di un eccessivo numero di risorse.
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 e riflessione meditata in un'ottica e con una visione multidisciplinare della legalità d'impresa; dove l'approccio risk- based accomuna tutte le normative esaminate.
La gestione integrata della compliance, basata sulla correlazione fra framework legislativi, si impone come brillante soluzione; sprigiona vantaggi competitivi, mira a focalizzare l'impegno sulle aree di rischio garantendo il coordinamento tra tutte le componenti normative e trasformando la compliance da fattore di costo a fattore generatore 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 stratificate, sovrapposte, tanto da costituire una "selva oscura" piuttosto che una guida per l'utente che rischia di smarrirsi fra le fronde delle regole costruite dalla preoccupazione aziendale di doversi schermare il più possibile.
Eppure, 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, ed a voler estendere lo sforzo progettuale 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.
Affinché il modello di organizzazione gestione e controllo 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 privacy i riferimenti ed i richiami, fra obblighi antiriciclaggio e disposizioni in materia di protezione di dati personali, sono continui spesso espliciti:
L'art. 16 del D.lgs. 231/07, nel trattare le procedure di mitigazione del rischio, stabilisce:

- 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…".*
- 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 dovesse adottare per arginare il rischio di prevenzione di questo reato non potrà che essere 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. Cambiano i quadri normativi internazionali al mutare dell'autore delle norme, il legislatore statunitense rende i dati patrimonio dell'azienda che li tratta, ma quello europeo vira, prende le distanze da questa impostazione e rende i dati personali proprietà del singolo individuo pari ai diritti umani elevandone rango e tutela. Gli adempimenti antiriciclaggio comportano obblighi di identificazione, conservazione dei dati personali e segnalazione di operazioni sospette, salta agli occhi la bivalenza dello strumento procedurale: tali attività costituiscono a tutti gli effetti trattamento dei dati protetti regolamentati dal GDPR ergo un MOGC che ambisca una valutazione di idoneità *banco iudicis*, dovrà bandire procedure duplicate, ipertrofiche e vessatorie nei dettagli e privilegiare protocolli comportamentali lineari, chiari, concepiti in un' ottica di compliance integrata. Ecco allora che una procedura aziendale concepita al fine di scongiurare e prevenire condotte criminose di riciclaggio (ed il ragionamento si presta ad essere esteso alla prevenzione della corruzione) prevederà anche:

- un'idonea informativa ai clienti nella quale si specifichi che il trattamento dei dati avverrà anche per le finalità previste dalla normativa antiriciclaggio;
- individuazione dei soggetti incaricati al trattamento debitamente istruiti e formati sulle

operazioni da compiere previa individuazione puntuale dell'ambito del trattamento consentito;
- il ricorso a credenziali di autenticazione per l'accesso ai dati conservati elettronicamente;
- identificazione di misure tecniche atte a prevenire la perdita delle informazioni, prevenzione dei rischi di distruzione o perdita dei dati, anche accidentale, garanzia che non venga effettuato un accesso alle informazioni da parte di soggetti non autorizzati;
- tempi di conservazione dei dati giustificati dalla finalità del trattamento e predefiniti.

Le procedure nate dall'attuazione normativa separata sono arnesi obsoleti si stratificano nella realtà organizzativa aziendale producendo un magma di regole interne frammentate in diversi processi guida. 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 costituendo una magnifica occasione di sintesi attuativa per la migliore tutela aziendale.

Altro esempio eclatante di processo a valenza multipla suggerito dai framework normativi integrati, riguarda la disciplina del whistleblowing.

Fa il suo ingresso nel nostro ordinamento alla fine del 2017, prevede una specifica tutela dei soggetti che segnalino reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro.

La tutela richiamata dalla norma implica:
- divieto di ritorsioni;
- riservatezza dell'identità del segnalante;
- sanzioni disciplinari per chi viola le misure di tutela del segnalante o presenta con dolo o colpa grave segnalazioni che si rivelano infondate.[11]

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, ma si infittisce la trama normativa per le banche, le assicurazioni, e l'attività di intermediazione finanziaria, settori particolari nei quali pullulano regole specifiche. Anche il settore pubblico è normato ad hoc (art. 54 del D.lgs 165/2001).[12]

Qualunque sia il comparto o il settore, la novità normativa viene tradotta in moltissimi codici etici aziendali ed 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 il segnalante, il segnalato ed eventuali terzi cui si fa riferimento (direttamente o indirettamente) nella segnalazione.

Saltano agli occhi le possibili e rilevanti implicazioni relative alla tutela dei dati personali, il Garante Privacy è sensibile al tema lo segna in agenda facendone uno dei settori oggetto di attività ispettiva nel primo semestre del 2020.

Qualunque sia la procedura costruita dall'azienda, affinché 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 identificazione del segnalante, dei segnalati e delle altre persone coinvolte (identità, funzioni e recapiti), i fatti segnalati, gli elementi raccolti nella verifica, 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 del Regolamento Generale sulla Protezione dei Dati – RGPD o GDPR).

Proteggere i dati significa per un titolare accorto: fornire moduli di segnalazione che guidino il solerte "soffiatore" e gli impediscano il rigurgito di informazioni eccedenti rispetto al fatto narrato, nel caso in cui si utilizzi una piattaforma informatica, verificare la sicurezza della piattaforma, limitare i dati protetti da cifratura, dotarsi di preziosi strumenti tecnici *ad adiuvandum*[13]: quello di trasporto dei dati meglio noto come protocollo HTTPS (acronimo di *Hyper Text Transfer Protocol Secure* [14]) tecnicamente affascinante per la verità, sfruttando avanzati sistemi di crittografia, cifra la comunicazione tra server e utente finale proteggendo il contenuto del messaggio e poi la rete TOR (acronimo di "The Onion Router"), che avvolge i dati con una cifratura a strati multipli assicurando l'anonimato del segnalante, rendendo impossibile per il destinatario e per tutti gli intermediari nella trasmissione avere traccia dell'indirizzo internet del mittente.

Impera in questa materia il principio di minimizzazione, i dati raccolti nella procedura di segnalazione sono solo quelli necessari e pertinenti per il raggiungimento della finalità perseguita. I dati ulteriori non potranno essere oggetto di trattamento. Il titolare deve fare in modo che il segnalante inserisca solo i dati necessari (tornano utili a tal fine i sistemi informatici che indirizzano il segnalante nell'inserimento delle informazioni); ma che sia una piattaforma informatica con indicazione dei dati da inserire o la più tradizionale modulistica cartacea, il titolare deve conservare e

trattare solo le informazioni necessarie nella fase istruttoria e d'indagine preziose anche al fine di definire la strategia processuale che l'azienda si trovasse a dover scegliere.

Il processo penale è spettacolo dialettico, tensione agonistica[15], duello tra accusa e difesa, domina la parte che ottiene il controllo delle informazioni; quelle utili alla ricostruzione della vicenda potrebbero essere determinati per accedere ai benefici premiali, (in questo ambito anche l'azzardo dell'autodenuncia può convenire) ma le regole interne da seguire nel corso delle investigazioni difensive condotte dall'azienda per l'accertamento di notizie in spregio al modello o su comportamenti che espongano la stessa, devono esser informate al più rigoroso rispetto della normativa privacy in difetto si trasformerebbero da opportunità a fattore di rischio. E qui si fa strategica la collaborazione fra ODV e DPO, si aprono frontiere di vigilanza integrata.

L'ODV, soggetto preposto al controllo sul funzionamento e il rispetto del Modello di Organizzazione, Gestione e Controllo (art. 6 del Decreto Legislativo 231/2001) è senza dubbio coinvolto in concorso con il DPO:

- nella valutazione di adeguatezza della procedura di whistleblowing,[16]
- nel vigilare sul corretto corso delle indagini difensive interne.

Il DPO (artt. 37-39 GDPR), coprotagonista nell'attività di controllo, avrà senz'altro un ruolo nella procedura, essendo la figura di riferimento in materia di protezione di dati personali 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 ad 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 e quindi curando che lo stesso sia conforme alla normativa di legge in materia e a quella privacy, 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 verificherà anche il rispetto dei principi previsti dall'art. 5 del GDPR[6] si assicurerà i che la tutela delle identità degli interessati sia piena mai a rischio, che all'interno della organizzazione i soggetti che attuano la procedura di segnalazione ricevano specifiche istruzioni ed una adeguata formazione sulla attività da svolgere; dichiarerà le finalità del trattamento[17], la durata del periodo di conservazione: breve (qualche mese) nell'ipotesi in cui, dopo la segnalazione, il caso sia archiviato, ma l'asse temporale si allunga ed è legato all'uso anche processuale del dato, quando si tratti dell' accertamento, l'esercizio o la difesa di un diritto della società in sede giudiziaria .

L'alchimia generata dall'attuazione normativa combinata della legge sulla privacy e di quella sul whistleblowing, è difficile ma necessaria, l'equilibrismo delle aziende nel contemperare le esigenze normative richiede prove di destrezza attuativa; a volte interviene il legislatore *ad adiuvandum*, non transige sulla protezione dell'identità del segnalante (e dei dati che possano comunque se pur indirettamente riportare a tale identità), e limita in tale ambito, i diritti degli interessati, con il D.lgs. 101/2018 introduce l'art. 2 *undecies* del Codice Privacy con riferimento (anche) alle procedure di whistleblowing (comma 1, lett. f). Tale norma sancisce che i diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo all'Autorità Garante qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del dipendente che segnala l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.

Sono geneticamente polivalenti queste procedure si impongono utili come un vaccino evoluto per la governance d'impresa.

Anche i protocolli di ultima generazione nati per arginare il rischio COVID 19, ad esempio la rilevazione della temperatura all'ingresso della sede di lavoro con valore determinante ai fini del MOGC ex D.lgs. 231/2001, avranno certamente valenza alla luce del DVR in esecuzione del D.lgs.81/ 08 ma saranno ampiamente informate al rispetto della normativa privacy tantopiù che il dato principalmente trattato, perché enormemente rilevante, è in questo caso relativo alla salute, ergo "particolare" a voler usare il lessico del legislatore europeo. Nulla può essere lasciato all'improvvisazione se tutto deve essere a tenuta: i soggetti che subiscono il processo vanno debitamente informati, chi rileva il dato deve essere incaricato ed istruito con apposita nomina; il terreno è scivoloso se il modello organizzativo non viene adeguato nel rispetto delle copiose disposizioni governative emergenziali di recente emanazione, ma in ogni caso anche nel rispetto di antichi paletti: l'art. 5 dello Statuto dei Lavoratori (Legge 300/1970) vieta accertamenti da parte del datore di lavoro sulla idoneità e sulla infermità per malattia o infortunio, ammettendo che il controllo delle assenze per "infermità" possa essere

effettuato soltanto attraverso i servizi ispettivi degli istituti previdenziali competenti. ma tale norma va contemperata - qui l'azienda deve dare prova di equilibrismo nell'esecuzione normativa- con l'art. 2087 del Codice Civile, secondo la quale il datore di lavoro deve "adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro" va da se che un tale sforzo organizzativo torni utile anche al fine di prevenire le condotte criminose di cui agli articoli (589 c.p. 590 c.p.) e quindi evitare il coinvolgimento dell'ente nel processo penale. Tanti gli input normativi che motivano il datore di lavoro a dotarsi di procedure di controllo finalizzate alla protezione della sicurezza dei lavoratori. La misurazione della temperatura corporea, pare misura ovvia e utilissima al fine di consentire l'accesso sicuro ai locali aziendali, è autorizzata direttamente dal DPCM dell' 11 marzo 2020 anche mediante apparecchi automatici, ovvio che sia preziosa una indicazione del medico competente che prescriva una tale misura come idonea a prevenire il rischio, tanto quanto la valutazione del DPO sulla conformità del trattamento di tali dati particolari perché inerenti la salute e la vigilanza dell'ODV ai fini della tenuta del modello.

Questo protocollo (misurazione della temperatura) atto a tutelare la salute del lavoratore e la sicurezza del luogo di lavoro, necessario ai fini della compliance al D.lgs. 231/2001 e al Dlgs 81/08 trasuda necessità di conformità privacy.

Costruire una procedura a norma impone alla società titolare del trattamento di individuare:

- la base giuridica del trattamento -motivi di interesse pubblico: implementazione dei protocolli di sicurezza anti-contagio ai sensi dell'art. art. 1, n. 7, lett. d) del DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni -obbligo di legge: art. 32 Costituzione; art. 2087 c.c.; d.lgs. 81/2008 (in particolare art. 20);
- la finalità del trattamento - prevenzione dal contagio da COVID-19 - tutela della salute delle persone in azienda - collaborazione con le autorità pubbliche e, in particolare le autorità sanitarie;
- tipologia dei dati raccolti e modalità di conservazione degli stessi;
- modalità e tempi di conservazione dei dati posto che nessuna registrazione e/o conservazione è effettuata nel caso di mancato superamento della soglia di temperatura.

I dati identificativi e il superamento della soglia di temperatura, andranno registrati solo qualora sia necessario a documentare le ragioni che hanno impedito l'accesso ai locali aziendali e potranno essere conservati fino al termine dello stato d'emergenza previsto dalle autorità pubbliche competenti; è fatta salva la conservazione dei dati personali, anche particolari, per un periodo superiore, nei limiti del termine di prescrizione dei diritti, in relazione ad esigenze connesse all'esercizio del diritto di difesa in caso di controversie.

Tutte le procedure sopradescritte nate in attuazione del Dlgs 231/2001 complementari ad un modello di Organizzazione gestione e controllo idoneo richiamano la compliance alla legge sulla privacy un fil rouge che se non presente le rende automaticamente non conformi. In tutti e tre i processi esaminati ma il ragionamento vuol essere esemplificativo non certo esaustivo emergono metodologie comuni di costruzione del protocollo:

1. Il titolare del trattamento ha una grande libertà e discrezionalità nell'organizzazione della propria attività di *compliance*, modello *privacy by design* e *privacy by default* (art. 25 GDPR), ma nel definire il *modus operandi* occorre mantenga sempre dritta la barra della protezione dei dati fin dalla progettazione del trattamento.
2. Il titolare ha il potere di tarare gli adempimenti alla propria realtà organizzativa ed economica le norme lo consentono ma nello scegliere il *modus adimplendi* sulla base del principio di *accountability* sarà comunque sempre responsabile delle scelte attuate e dovrà essere in grado di dimostrare di aver adottato le misure (organizzative tecniche e fisiche) idonee a protezione dei dati.
3. Riguardo alle operazioni di trattamento sarà necessario dimostrare di aver impartito specifiche istruzioni ai soggetti coinvolti nei trattamenti che pure dovranno essere adeguatamente formati attraverso contenuti profilati ad hoc in ragione dei trattamenti svolti.

In un'ottica di modello integrato, tutte queste procedure dovrebbero essere concepite partendo dal sistema di prevenzione dei rischi non settoriale ma frutto di un approccio olistico che dovrebbe avere quale naturale approdo la creazione di un sistema di organizzazione, gestione e controllo integrato.[18]

5. Deleghe *multitasking*

L'insieme magmatico delle norme che impongono alle aziende uno sforzo di conformità, generano un vortice documentale di deleghe e procure, il

legislatore le esige ordinate, chiare, ben strutturate, non configgenti. 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, meglio se con l'aiuto di un tool informatico. Sono svegli i player di mercato, oligopolisti della consulenza best, ne propongono di accattivanti: sistemi di gestione della compliance integrata automatizzata, testata d'angolo dei modelli di organizzazione e gestione e controllo progettati anche questi secondo la metodologia che qui stiamo teorizzando ed auspicando. In ogni caso e 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.

Ad esempio, l'ODV, che sia interno oppure esterno, è il CDA che lo individua e nomina attribuendo compiti e spesso novando la declinazione delle responsabilità, già sancita dal legislatore, nell'atto di nomina.

Ma non troppo tempo fa è il Garante a precisare in un parere del 12 /05/2020 richiesto dall' associazione dei componenti dell'organismo di vigilanza che i componenti di tali organismi (la best practice li pretende collegiali) vengano debitamente autorizzati al trattamento dei dati dalla società (titolare del trattamento).

"*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 - che si esplica nell'esercizio dei compiti che gli sono attribuiti dalla legge, attraverso il riconoscimento di "autonomi poteri di iniziativa e controllo" - 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 (ad esempio, l'accesso alle informazioni acquisite attraverso flussi informativi), designerà - nell'ambito delle misure tecniche e organizzative da porre in essere in linea con il principio di accountability (art. 24 del Regolamento) - i singoli membri dell'OdV quali soggetti autorizzati (artt. 4, n. 10, 29, 32 par. 4 Regolamento; v. anche art. 2- quaterdecies del Codice)".*

A voler progettare gli atti di nomina in ottica multitasking, si presta bene quella atta all'individuazione e nomina dei i membri dell'ODV ad accogliere anche in forma di allegato le istruzioni cui il Garante fa riferimento.

Stesso metodo ben può essere seguito per costruire la delega/procura ad individuare il dirigente delegato ex art. 16 D.lgs. 81/08, quale miglior supporto per inserirvi tutte le istruzioni del titolare sul corretto trattamento dei dati tantopiù che quelli maneggiati da tale figura aziendale, sono dati riguardanti lo stato di salute o i rischi specifici legati alla mansione e alla idoneità del singolo lavoratore rispetto alla mansione. Anche la delega al dirigente preposto alla corretta tenuta dei documenti contabili[19] può avere a doppia valenza e ricomprendendo le istruzioni impartite dal titolare per un corretto trattamento dei dati personali.

A guardar bene le organizzazioni aziendali si ergono su procure e deleghe che si prestano ad essere implementate alla luce della normativa privacy divenendo strumenti poliedrici, multiuso e purificaci.

6. Norme etiche a geometria ellittica

Il codice etico complemento essenziale di un MOGC che ambisca ad essere considerato idoneo *banco iudicis,* è un meraviglioso strumento per attuare in forma integrata le norme contenute nei tre pacchetti e si presta per duttilità ed efficacia ad essere estensibile ed accogliere le politiche etiche ben oltre i perimetri normativi fin qui esaminati.

Il legislatore lo rende componente essenziale ed integrante di un modello di organizzazione gestione e controllo idoneo, è in sostanza un compendio di policy e regole che diventa prezioso in caso d'uso e se ben strutturato e capillarmente diffuso prova l'impegno delle aziende a prevenire la commissione dei reati rilevanti alla luce del Dlgs 231/2001 e a ridurre i rischi aziendali attraverso la forza del monito etico. La duttilità dello strumento lo rende per definizione materia ideale da plasmare in un'ottica multidisciplinare.

Attraverso le norme etiche si promuove la parità sul luogo di lavoro, la salute e sicurezza dei lavoratori, la tutela dell'ambiente, si gestiscono in modo responsabile i rapporti con i fornitori e con la Pubblica Amministrazione (corruzione pubblica e privata), si sponsorizza la tutela del diritto alla privacy di tutti gli stakeholder, si detta il modus operandi sui mercati con lealtà e trasparenza e nel rispetto delle regole, si forniscono valori guida per evitare condotte che possano integrare reati contro

l'industria e il commercio, in materia di diritto d'autore; si bandiscono condotte volte a foraggiare il terrorismo, il lavoro irregolare, attraverso le regole etiche si punta alla prevenzione dell'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).
Il codice etico ha la finalità precipua di guidare le decisioni dei destinatari (risorse interne ed esterne alle aziende) al fine di compiere azioni coerenti con la cultura della responsabilità e della legalità, è uno strumento poliedrico e versatile; spesso in esecuzione del D.lgs. 231/2001 (art. 6, comma 2, lett. e), ingloba il sistema disciplinare[20] acquisendo efficacia deterrente e sanzionatoria a scapito dei trasgressori di protocolli e norme etiche e di ogni altra misura preventiva indicata dal modello.
Si presta bene geneticamente questo strumento ad essere progettato con una visione integrata, l'efficacia delle norme concepite in ottica multidisciplinare, si amplifica, diventa una bussola di orientamento per evitare smarrimenti di condotta nell'ambito di una geografia normativa attuata in forma integrata.

7. Formazione multidisciplinare

Quale meravigliosa 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:

1. D.lgs. n. 81/08: l'art. 18, co. 1 lett. l) e l'art. 37 del Decreto 81/2008 prevedono l'obbligo di assicurare ad ogni lavoratore una formazione sufficiente ed adeguata in materia di salute e sicurezza sul lavoro. La formazione deve avvenire 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.
2. Privacy: il Regolamento Europeo 2016/679 (G.D.P.R.), agli artt. 29 e 32, stabilisce che il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali, debba essere istruito in tal senso dal titolare del trattamento.
3. Dlgs 231/2001: il modello organizzativo è facoltativo, ma operata la scelta, per poter essere "efficacemente attuato" - condizione necessaria affinché si sprigioni l'efficacia esimente prevista dall'art. 6 del Decreto - è necessario che la popolazione aziendale sia adeguatamente formata sulla disciplina di legge, e sui contenuti del Modello Organizzativo adottato dalla Società.

I formatori affetti da visione tradizionali lanciano periodicamente l'anatema dei moduli separati per pacchetto normativo che colpisce gli apparati aziendali sfinendo le risorse obbligate ex lege e dai MOGC a non sottrarsi.
Questi moduli, che le aziende progettano sempre più spesso in modalità e-learning per raggiungere capillarmente i destinatari, vengono solitamente vissuti con fastidio dalla popolazione aziendale che si sente distolta dall'operatività quotidiana e obbligata a subire spesso in sequenza la somministrazione della formazione a tema, terminata quella della D.lgs. 231/2001 dopo qualche tempo subentra la necessità di quella sulla sicurezza (D.lgs. 81/08) e come tentare di chiudere l'anno senza la formazione privacy. La serietà dei moduli è spesso legata alla durata degli stessi ed all'impossibilità tecnica di far scorrere i contenuti senza l'adeguata attenzione del discente chiamato puntualmente ad eseguire il test di fine corso.
Spesso concepita ed accettata come una terapia dolorosa ma necessaria cui non ci si può sottrarre, le aziende somministrano a dosi gli inesorabili, obbligatori, moduli formativi in materia di salute e sicurezza sul lavoro privacy, di D.lgs. 231/2001/ ed in materia D. lgs.81/08. La posologia della formazione li vuole almeno annuali, tutti i pacchetti formativi prevedono, per essere compliance, un test di fine corso per comprovare il passaggio dei contenuti dal docente (spesso virtuale) al succube discente.
I modelli integrati ispirano una formazione plurivalente evidentemente conveniente in termini di costi e certamente meglio accolta dalla popolazione aziendale che invece di galleggiare nuoterebbe agevolmente fra i flutti dei contenuti formativi, acquisendo una visione d'insieme, senza rischiare di essere sopraffatta dalle diverse ondate di formazione a pacchetto.

8. Vigilanza osmotica

e Sistema dei controlli rafforzato e capillare Un modello integrato elimina per definizione i controlli ridondanti e crea efficienza e valore essendo basato su un approccio multidisciplinare delle verifiche svolte dai controller interni[21].
Le mappature dei rischi generate da visioni integrate sfruttano la versatilità dei controlli. Il piano di audit aziendale può essere concepito in modo da approcciare più ambiti senza sovrapposizioni.

Si evitano così le maree dei controlli che sfiniscono gli apparati organizzativi.
Se i controlli sono a compartimenti stagni perimetrati e qualificati dai singoli pacchetti di norme la longa manus dei controller interni esplorerà gli *interna corporis* aziendali e verificherà lo stato dell'arte e della compliance senza sfruttare l'opportunità di un controllo combinato. I limiti saltano agli occhi: se l'approccio non è integrato si rischiano duplicazioni e controlli ridondanti e un più alto impiego di risorse. Sia i controllori che i controllati in momenti diversi saranno chiamati a gestire l'attività di controllo per materia normativa, la pecca di questa metodologia è la ripetizione delle verifiche su una stessa funzione e spesso su una stessa "batteria di documenti". Ad esempio, svolto l'audit richiesto dal D.lgs. 231/01 non è escluso, dopo qualche mese, che la stessa funzione aziendale venga raggiunta da una seconda verifica che ha come driver il GDPR magari i controller intervisteranno le stesse risorse ed analizzeranno gli stessi documenti con un'altra ottica.
Queste le pieghe disfunzionali di un sistema di controllo separato lontano dall'integrazione.

9. La teoria dei flussi sincroni e i comitati di controllo.

Il D.lgs. 231/2001 esige un'organizzazione che preveda flussi informativi verso l'"ODV" e da questo, di solito annualmente, verso il "Cda" (Consiglio di amministrazione). Simmetricamente un'organizzazione privacy che si rispetti esige che i dipartimenti aziendali emergano periodicamente dall'apnea dell'operatività quotidiana e facciano una riflessione consapevole e meditata su eventuali profili di criticità rispetto al modello di organizzazione e gestione della privacy riferendo al "DPO" lo stato dell'arte; 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.
Molte organizzazioni aziendali tollerano un incedere disorganizzato dei flussi e che gli organismi posti a presidio dei singoli modelli organizzativi lavorino separatamente ognuno nel proprio ambito senza comunicare. Sono datati e superati questi modus operandi.
Se si abbattono le barriere dei perimetri normativi e si segue la logica dei modelli integrati potrebbero essere organizzati flussi informativi sincroni e nascerebbero spontanei comitati di controllo per il miglior monitoraggio dei rischi basati sul dialogo e sul confronto strutturato fra i controller che le diverse leggi "designano": DPO, ODV, Dirigente delegato ex art. 16 del D.lgs. 81/08 quando presente dirigente preposto alla corretta tenuta dei documenti contabili.
Ci sono ambiti dal confine labile fra D.lgs. 231/2001 e privacy (regolamento 2016/679/ Ue), basti pensare al perimetro dei reati informatici la cui prevenzione deve premere all' "ODV" quanto al "DPO", e ancora ci sono perimetri comuni sulla sicurezza delle persone che devono premere tanto al ODV quanto al dirigente delegato ex art. 16 del D.lgs.81/08 e al DPO poiché particolare è la genesi dei dati trattati in tale ambito. Ed ancora ci sono perimetri d'interesse comune fra ODV dirigente preposto alla corretta tenuta dei documenti contabili e DPO che sui flussi a meno che non siano scevri di dati personali, non cessa mai di concorrere al design privacy.
Un modello integrato si basa su flussi informativi sincroni, sul dialogo strutturato e periodico fra soggetti incaricati di effettuare controlli periodici, sono molte e frammentate, le norme che disciplinano istituzione e funzionamento di tali organi di controllo; producono l'effetto talvolta di delineare responsabilità simili e spesso sovrapposte.[22] La chiave per ottenere il massimo risultato in efficacia con riduzione di tempi e di sforzi è la sinergia: intuire e credere che leggi frammentate possano creare un'opportunità di lavoro integrato nell'ambito del quale i controller per genesi normativa "ODV" (articolo 6 D.lgs. 231/2001), "DPO" (articolo 37, regolamento 2016/679/Ue — "GDPR"), dirigente delegato (articolo 16 del D.lgs. 81/2008), dirigente preposto alla corretta tenuta dei documenti contabili, si riuniscono periodicamente in un comitato per il controllo interno che dialoga e si confronta sulla gestione dei rischi mostrandosi in grado per visione allargata, di monitorare, intuire i rischi dell'agire aziendale organizzandolo con protocolli di prevenzione (norme etiche, deleghe e procedure) di sicura efficacia perché ispirati da una visione d'insieme e per ciò stesso illuminata.
La compliance integrata è la chiave, i modelli di organizzazione gestione e controllo progettati con una visione integrata sono avanguardia della migliore tutela aziendale, un concetto sfidante per le aziende che hanno, da un lato, la necessità di stare al passo con la normativa e la sua evoluzione e, dall'altro, di contenere i costi e 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 e il coordinamento tra le diverse professionalità coinvolte, la compliance integrata può fornire valore aggiunto nella gestione dei rischi. Il MOGC integrato è un'idea progressista che si presta per

genesi e sin dalla sua progettazione ad essere strumento in grado di abbracciare le diverse esigenze dettate dalla normativa. Un tale disegno muove da una visione d'insieme e sottintende un'opportunità quella dei ragionamenti integrati consentita a tratti suggerita dalle norme e che va solo intuita e colta.

---

1 . La Cassazione in una recente sentenza del 16 gennaio 2020, n. 1676, ha legittimato il sequestro dei beni dell'amministratore dell'azienda sanzionata ai sensi del D.lgs. 231/2001, essendo il patrimonio dell'ente insufficiente, fissando il seguente principio: nel caso in cui il profitto o il prezzo del reato sia rappresentato da una somma di denaro, questa si fonde con le altre disponibilità economiche dell'autore del fatto: "*la confisca per equivalente del profitto di cui al D.lgs. n. 231 del 2001, art. 19, ha natura di sanzione principale e autonoma", senza che ricorra "rapporto di sussidiarietà o di concorso apparente tra la detta disposizione e le norme del codice penale che prevedono la stessa misura ablativa a carico delle persone fisiche responsabili del reato, fermo restando logicamente che l'espropriazione non potrà, in ogni caso, eccedere nel quantum l'entità complessiva del profitto*".

2 L'intervento a sezioni unite della Corte di cassazione sentenza del 24 aprile 2014, n. 38343 risolve il dibattito insorto sulla natura delle responsabilità dell'ente facendone un "*tertium genus*" ovvero "*un corpo normativo di peculiare impronta"* che assomma i tratti essenziali del sistema penale e di quello amministrativo.

3 Il D.lgs. 101/2008 ha adeguato il codice privacy nazionale (D.lgs. 196/2003) alle novità introdotte nel GDPR. Il testo del codice novellato presenta le maggiori innovazioni negli articoli amputati più che per quelli rimasti nel corpo normativo.

4 Nel corso degli ultimi 20 anni è stata emessa una vasta gamma di provvedimenti legislativi di normativa primaria, secondaria e di autoregolamentazione. A titolo esemplificativo le quotate sono soggette al TUF emesso con D.lgs. 58/98; poi il D.lgs. 262/05 che ha introdotto la figura del dirigente preposto alla cura dei documenti contabili. Tra le fonti secondarie emergono i regolamenti emessi dalle autorità regolatorie: il Regolamento Emittenti emesso dalla commissione nazionale per la società e la Borsa, i regolamenti congiunti emessi da Banca d'Italia e CONSOB, le disposizioni di vigilanza per e banche; i regolamenti emessi dall' istituto di vigilanza sulle assicurazioni IVASS, i Regolamenti Ministeriali; fra le fonti di autoregolamentazione val la pena citare il Codice di autodisciplina delle quotate. Una tale pressione normativa ha comportato in diverse società l'istituzione della figura del compliance officer definito nelle disposizioni di Vigilanza di Banca D'Italia quale attore del controllo in materia di conformità a leggi e regolamenti.

5 Sul tema: I costi della Non compliance a cura di Accardi F. Rosato R., rivista Internal Audit- Corporate Governance, risk management e controllo interno n. 82, 2014.

6 Sarebbe piaciuta l'idea di compliance integrata a F. P. Ramsey. Oggi, nessuna teoria giuridica o economica può dirsi unisona, ma tutto è interdisciplinare, flessibile. Le nozioni si prestano ad essere utilizzate in più ambiti secondo l'approccio multi-comprensivo che il geniale matematico, filosofo, economista, allievo di Keynes, ha ideato e diffuso.

7 Il modello di ERM proposto dal committee of Sponsoring Organizationof the treadway commission (CoSO release 2017) si scompone in cinque elementi fortemente interconnessi fra loro: Governance and Culture; Strategy & Objective Setting; Performance; Review & Revision; Information &Communication Reporting.

8 Francesco Capparelli - Alessandro Fratini, *l'importanza di una compliance integrata legal-cibersecurity*, Privacy News ottobre-dicembre 2020, p.9

9 Per un approfondimento su un efficace sistema di controllo del rischio fiscale inserito nel contesto del sistema di governo aziendale e di controllo interno (Tax Control Framework) si veda il documento OCSE 2013 - Cooperative Compliance - A Framework . Sui requisiti che un tale sistema deve possedere, OCSE 2016 – Building Better Tax Control Framework che descrive il sistema efficace se è in grado di garantire all'impresa un presidio costante sui rischi fiscali, per far questo il sistema deve presentare i seguenti requisiti essenziali: strategia fiscale; ruoli e responsabilità, procedure, monitoraggio, adattabilità al contesto interno ed esterno, relazione agli organi di gestione.

10 Le aziende dotate di TCF sono considerate contribuenti virtuosi e in quanto tali, possono beneficiare di sistemi premiali: minori adempimenti, riduzioni di sanzioni, forme di interpello preventivo in tempi abbreviati.

11 art. 6 prevede che sia sanzionato – oltre al soggetto che abbia posto in essere atti di ritorsione o discriminatori nei confronti del *whistleblower* – anche colui che "*effettua con dolo o colpa grave segnalazioni che si rivelano infondate.* Occorre un impianto sanzionatorio ad hoc per queste ipotesi da integrare nel sistema disciplinare *ex* art. 6, comma 2, lett. e, del Decreto 231/01. Nell'espletamento dell' attività di vigilanza, particolare attenzione dovrà essere posta dall'ODV su licenziamenti o altre misure (*e.g.* demansionamenti e trasferimenti) che possano avere natura ritorsiva o discriminatoria nei confronti dei segnalanti.

12 La direttiva 2019/1937 del 23 ottobre 2019 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione,

dovrà essere recepita dagli stati membri entro il 17 dicembre 2021.

13 Si segnalano al riguardo i provvedimenti del Garante n. 215 del 04 12 2019 e n. 17 del 23 gennaio 2020

14 Nota eliminata.

15 Franco Cordero, *Procedura Penale*, Giuffrè p.96

16 L'ODV agisce affinché i segnalanti siano tutelati nel processo di gestione della segnalazione, pur rimanendo protagonista della vigilanza sul rispetto del divieto di "*atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione*" (art. 6, comma 2-*bis*, lett. c, del Decreto 231).

17 Con riferimento ai dati personali la base giuridica su cui si fonda la procedura dovrà essere il legittimo interesse del titolare (ex art. 6 lett. f) GDPR). Con riferimento ai dati "particolari" di cui all'art. 9 del GDPR deve ritenersi che la base giuridica sia quella prevista dall'art. 9, par. 2 lett. f) ossia l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria si precisa che per alcuni aspetti legati al rapporto lavorativo, la base giuridica può essere rinvenuta nella lett. b) della medesima disposizione.

18 Per un approfondimento sull'approccio integrato alla gestione dei rischi: Fabio Accardi, *La gestione della compliance,* Luiss, 2020, a cura di Alessandro Adotti e Saverio Bozzolan, cap.2

19 La legge 262/05 ha normato la struttura dei controlli interni alla società identificando per quelli amministrativi -contabili un centro di responsabilità rappresentato dal dirigente preposto.

20 In alcuni casi il sistema disciplinare è inserito nel documento descrittivo del MOGC ex D.lgs. 231/2001
In altri è contenuto in un codice disciplinare ad hoc che si affianca al codice etico ma sono scelte queste compilative e di estetica documentale che il legislatore lascia alle aziende.

21 Solitamente le aziende medio grandi si muniscono di un sistema declinato su tre livelli di controllo: controlli di primo livello o controlli di linea, diretti ad assicurare il corretto svolgimento delle operazioni. Questi controlli sono effettuati nel corso dell'operatività e sono rappresentati ad esempio da presidi di tipo gerarchico svolti da vari responsabili delle unità organizzative possono essere sistematici o a campione diretti ad identificare, valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività.
Controlli di secondo livello o controlli sui rischi e sulla conformità che hanno l'obiettivo di assicurare la corretta attuazione del processo di gestione dei rischi; il rispetto dei limiti operativi assegnati alle varie funzioni; la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione. Le funzioni preposte a tali controlli sono: Compliance, Controllo costi o controllo di gestione, Servizio pianificazione e controllo, Responsabile Sistemi di gestione, HSE, ecc.,
Controlli di terzo livello fisiologicamente affidati all'Internal Audit. Sono volti ad individuare violazioni delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni.

22 Saverio Bozzolan e Sara Costanzo, *Corporate governance, sistemi di risk management rischi di compliance,* Luiss, 2020, a cura di Alessandro Adotti e Saverio Bozzolan, cap.1.

GIURISPRUDENZA PENALE