5. PREVENZIONE, SISTEMI DI CONTROLLO INTERNO E CONTRASTO ALLE FRODI

5.1. STRUMENTI DI PREVENZIONE DELLE FRODI

La frode contabile, in particolare nella sua forma più sofisticata (*fraudulent financial reporting*), può essere considerata come la patologia estrema di un sistema informativo malfunzionante. La prevenzione delle frodi passa quindi attraverso un approccio sistemico alla costruzione degli assetti, che coinvolge:

- *la progettazione dell'organigramma e la separazione delle funzioni;*
- *l'adozione di procedure formalizzate di autorizzazione, contabilizzazione e rendicontazione;*
- *la presenza di un sistema di controllo interno integrato e documentato;*
- *la capacità del sistema informativo di produrre dati coerenti, tempestivi e verificabili.*

Come osserva Savioli[1], l'assetto contabile non si riduce alla tenuta ordinata dei registri, ma coincide con l'intero sistema informativo aziendale, inteso come supporto decisionale e strumento di governo. In questa accezione, la contabilità è solo una parte del sistema, che deve essere completato da *budget*, *forecast*, *report* analitici e analisi degli scostamenti.

Nel panorama economico-aziendale contemporaneo, la prevenzione delle frodi in bilancio rappresenta un obiettivo strategico imprescindibile per garantire l'affidabilità dell'informazione finanziaria e la tutela degli *stakeholders*. Tradizionalmente, la rilevazione delle irregolarità contabili si fondava prevalentemente su un *approccio ispettivo*, *ex post* e spesso episodico, affidato a controlli formali e a verifiche documentali condotte da organi di vigilanza o autorità giudiziarie. Questo modello, tuttavia, mostrava limiti evidenti, soprattutto in contesti ad elevata complessità tecnica e in presenza di condotte fraudolente sofisticate e intenzionalmente dissimulate[2].

Negli ultimi decenni, anche in risposta ai grandi scandali finanziari internazionali, si è progressivamente affermata una nuova logica di intervento, basata non più sulla mera repressione *a posteriori*, bensì sulla costruzione di *sistemi organici di prevenzione ex ante*. In tale prospettiva, la gestione del rischio di frode è divenuta parte integrante dei sistemi di *corporate governance*, con un rinnovato *focus*, concentrandosi sull'ambito nazionale, su assetti organizzativi, amministrativi e contabili adeguati, come previsto dall'art. 2086, comma 2, c.c., nonché sull'adozione di controlli interni strutturati e su modelli organizzativi conformi al D.Lgs. n. 231/2001.

L'evoluzione normativa, unitamente al consolidarsi di framework internazionali come il CoSO – Internal Control Integrated Framework e l'ISA 240 sul ruolo del revisore nella prevenzione delle frodi, ha determinato una transizione culturale significativa: la frode non è più considerata un'eventualità patologica residuale, ma un rischio fisiologico da gestire attivamente attraverso sistemi predittivi, indicatori di anomalia, controlli preventivi multilivello, formazione e diffusione di una cultura etica d'impresa.

In tale scenario, la prevenzione si fonda su una molteplicità di strumenti integrati – tecnologici, organizzativi, normativi – che, se correttamente implementati e monitorati,

[1] Savioli G. (2025), *L'adeguatezza degli assetti contabili alla luce delle indicazioni dell'Economia Aziendale*, Milano.
[2] Così Allegrini, M., D'Onza, G., Mancini, D., & Garzella, S. (2003), *Le frodi aziendali. Frodi amministrative, alterazioni di bilancio e computer crime*. Milano pag. 34.

consentono di intercettare i segnali premonitori di frode, disincentivare condotte illecite e rafforzare la trasparenza e l'affidabilità del bilancio d'esercizio. La logica reattiva lascia dunque il posto a un paradigma proattivo di prevenzione e controllo del rischio fraudolento, coerente con le esigenze di *accountability* e sostenibilità richieste all'impresa moderna.
In ambito internazionale, la questione della prevenzione delle frodi contabili è stata affrontata attraverso l'introduzione di normative specifiche e *framework* metodologici di riferimento. Tra i più significativi si segnalano:
a) Il *Sarbanes-Oxley Act (SOX, 2002) – Stati Uniti*[3].
La sezione 404 del SOX impone alle società quotate l'obbligo di istituire e mantenere un sistema di controllo interno sull'informativa finanziaria. I manager devono certificare personalmente l'efficacia dei controlli, e la violazione di tali obblighi può dar luogo a responsabilità penale. Il SOX ha introdotto una visione integrata della *governance*, in cui la trasparenza contabile è funzione dell'integrità organizzativa.
b) Il *UK Corporate Governance Code (Regno Unito)*
Il codice britannico richiede agli organi societari di garantire l'efficacia dei sistemi di *risk management* e internal control. L'approccio è basato sul principio del *comply or explain*, con un forte *focus* sul ruolo degli amministratori indipendenti e sull'*audit* committee.

5.2. ADEGUATI ASSETTI ORGANIZZATIVI, AMMINISTRATIVI E CONTABILI

Il tema dell'adeguatezza degli assetti organizzativi, amministrativi e contabili ha assunto una posizione centrale nel diritto societario e nella scienza aziendalistica contemporanea che oggi si pone, non solo, come presidio di *governance* e continuità aziendale, ma anche come strumento primario di prevenzione e contrasto delle frodi contabili, in particolare delle frodi in bilancio. A partire dalla riforma dell'art. 2086, comma 2, c.c., introdotta con il D.Lgs. n. 14/2019, la funzione degli assetti è divenuta ancora più centrale nella sistematica del diritto societario e della crisi d'impresa, ponendo l'accento su un'organizzazione imprenditoriale che sia al contempo efficiente, trasparente e idonea alla rilevazione anticipata delle disfunzioni gestionali, contabili e patrimoniali. Il valore dell'assetto si misura, in quest'ottica, non sulla sola conformità formale, ma sulla capacità concreta di prevenire comportamenti devianti e distorsivi dell'informazione economico-finanziaria[4].
Le frodi contabili, per definizione, rappresentano una devianza intenzionale dalla rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria dell'impresa. Esse si alimentano in contesti in cui gli assetti sono inadeguati, le funzioni non sono segregate, i flussi informativi sono opachi e le responsabilità gestionali risultano non tracciabili. In questa prospettiva, la prevenzione della frode non è affidata

[3] Sul punto si veda quanto diffusamente argomentato nel paragrafo 2.1.3. ("*Il Sarbanes-Oxley Act ed il rafforzamento della trasparenza e della responsabilità nelle pratiche contabili*").
[4] Rordorf R., "Doveri e responsabilità degli organi della società alla luce del codice della crisi d'impresa e dell'insolvenza", in *Riv. Soc.*, 2019.

unicamente alla funzione di controllo, ma all'intero disegno dell'organizzazione aziendale, la cui efficacia è misurabile in termini di *compliance, trasparenza e accountability.*
In questa prospettiva, l'adeguatezza diviene concetto "*polidimensionale*"[5], articolato su tre direttrici interconnesse: (i) *organizzativa*, in quanto attiene alla formalizzazione e responsabilizzazione delle funzioni; (ii) *amministrativa*, in quanto concerne i processi decisionali e autorizzativi; (iii) *contabile*, in quanto include i meccanismi di rilevazione, controllo e rappresentazione dei dati aziendali. La frode in bilancio – nella sua forma più insidiosa, quella "manageriale" (*fraudulent financial reporting*) – trova terreno fertile in assetti deboli, informali o concentrici, in cui le funzioni di controllo non sono segregate da quelle esecutive e in cui la cultura del risultato sopravanza la cultura della legalità[6].
La frode in bilancio si manifesta tipicamente in operazioni simulate, registrazioni fittizie o omissioni dolose di dati rilevanti, volte ad alterare la rappresentazione della realtà economica dell'impresa, spesso per occultare situazioni di crisi, attrarre finanziamenti, eludere obblighi fiscali o distribuire utili fittizi. Tali condotte si alimentano di *vuoti organizzativi* e *controlli inefficaci*, che rendono l'impresa *permeabile a logiche opportunistiche*. Di qui l'esigenza, normativamente codificata, di adottare assetti proporzionati alle caratteristiche dimensionali e settoriali dell'impresa, ma dotati di presidi robusti per l'integrità del dato contabile e la tracciabilità delle operazioni. L'adeguatezza è, pertanto, una categoria funzionale, da valutarsi in relazione alla capacità del sistema aziendale di prevenire, rilevare e reagire agli scostamenti patologici dai principi di corretta amministrazione.
In chiave aziendalistica, gli assetti contabili adeguati vanno ricondotti all'ambito del *sistema informativo aziendale* nella sua interezza. Secondo l'elaborazione della dottrina aziendalistica[7], la funzione contabile va integrata con i sottosistemi di *rilevazione preventiva* (es. *budget*, piani industriali, *forecast*), *concomitante* (es. contabilità generale, analitica, centri di costo) e *consuntiva* (bilanci, reporting, analisi degli scostamenti). Nondimeno, occorre dare rilievo al piano strategico che rappresenta, nell'ambito della governance aziendale, uno degli strumenti principali mediante cui l'organo amministrativo esercita le proprie funzioni di direzione, programmazione e controllo. Esso costituisce non soltanto una proiezione dell'agire d'impresa nel futuro, ma anche una matrice

---

[5] Irrera M., *Assetti adeguati e modelli organizzativi*, Torino, 2020.

[6] Cools, M., & Van Caneghem, T. (2015). *Management Control in the Public Sector: A Matter of Results or Legality?* Public Money & *Management*, 35(3), pagg. 161-168. Nell'articolo, gli autori distinguono tra due approcci culturali predominanti nelle organizzazioni pubbliche:
- *Cultura del risultato*: orientata al raggiungimento di obiettivi specifici e alla *performance*, spesso misurata attraverso indicatori quantitativi.
- *Cultura della legalità:* incentrata sul rispetto rigoroso delle leggi, regolamenti e procedure formali, con un'enfasi sulla conformità normativa.
Cools e Van Caneghem discutono come l'equilibrio tra queste due culture influenzi le decisioni manageriali e le pratiche di controllo interno, sottolineando l'importanza di una *governance* che bilanci efficacemente l'efficienza operativa con l'aderenza alle normative.

[7] Savioli G., *L'adeguatezza degli assetti contabili alla luce delle indicazioni dell'Economia Aziendale*, cit.; anche Bastia P., *Gli adeguati assetti nelle imprese: criteri di progettazione*, in Ristrutturazioni aziendali, 2021.

operativa di riferimento per valutare l'adeguatezza delle decisioni gestionali, soprattutto sotto il profilo della loro conformità a criteri di diligenza e prudenza. Insomma, la dottrina[8] lo definisce come:

– uno strumento previsionale, in quanto consente di rappresentare scenari futuri attesi e di predisporre le risorse necessarie per affrontarli;
– uno strumento precauzionale, in quanto mira a contenere i rischi connessi all'incertezza che inevitabilmente caratterizza gli obiettivi strategici;
– una sintesi di decisione e organizzazione, poiché integra la funzione deliberativa dell'organo gestorio con l'individuazione operativa dei mezzi, delle risorse e delle modalità attuative.

Con i suddetti presupposti il piano strategico funge anche da strumento di benchmarking interno nel senso che:

– agisce *ex ante* come elemento di guida nella gestione;
– opera *ex post* come parametro valutativo della condotta degli amministratori;
– rappresenta un presidio documentale utile ai fini della responsabilità gestoria, in quanto consente di verificare la coerenza e la ragionevolezza delle scelte compiute.

Il livello di dettaglio del piano è direttamente proporzionale alla sua efficacia vincolante: quanto più esso è analitico, tanto più si riduce il margine di discrezionalità degli amministratori. In assenza di tale struttura articolata, l'amministrazione aziendale risulta "*cieca*" e facilmente manipolabile. Un sistema informativo siffatto consente non solo la rappresentazione dei dati, ma la formulazione di giudizi anticipatori, elemento essenziale per l'emersione di anomalie sintomatiche della frode (es. *overstatement* di ricavi, riclassificazioni improprie, utilizzo improprio delle poste transitorie o discrezionali).

Proprio per questo, il legislatore ha inteso il termine "*contabile*" in senso lato, quale sistema di rappresentazione razionale e anticipatoria delle dinamiche economico-finanziarie aziendali. Tale impostazione è confermata dall'art. 3, comma 3, del Codice della Crisi d'Impresa, che impone agli assetti l'obiettivo di rilevare squilibri, valutare la sostenibilità dei debiti, e fornire informazioni adeguate al test di risanabilità.

L'interconnessione tra assetti e sistemi di controllo interno è altrettanto essenziale: le frodi in bilancio trovano il loro terreno fertile in assenza di separazione delle funzioni, di responsabilità formalizzate, di controlli incrociati, e di supervisione effettiva dell'organo amministrativo e del collegio sindacale[9]. Il D.Lgs. n. 231/2001 rafforza ulteriormente questo presidio, inserendo i reati societari, tra cui il falso in bilancio, tra quelli presidiabili attraverso l'adozione di un Modello Organizzativo e di Gestione (MOG), che deve prevedere specifiche misure di controllo contabile, *audit*, e canali di segnalazione. Una simile integrazione tra assetti *ex* art. 2086 e MOG *ex* art. 6 D.Lgs. n. 231/2001 configura un sistema di *compliance* integrato, nel quale la prevenzione della frode contabile diviene obiettivo strategico.

---

[8] Così Galletti D., *Le politiche di gestione del rischio*, 2021, Napoli, p. 38.

[9] Fortunato S., "Codice della crisi e Codice civile: impresa, assetti organizzativi e responsabilità", in *Rivista delle società*, 2019.

La prevenzione delle frodi in bilancio non può prescindere da un'effettiva integrazione tra gli assetti *ex* art. 2086 c.c. e il modello organizzativo previsto dal D.Lgs. n. 231/2001. Il reato di falso in bilancio rientra tra i reati-presupposto e richiede specifiche misure di prevenzione, tra cui:

- controlli incrociati tra contabilità generale e analitica;
- definizione di ruoli e responsabilità nelle registrazioni contabili;
- procedure di approvazione e verifica dei dati di bilancio;
- *audit* periodici e funzione di *whistleblowing*.

Solo in presenza di assetti coerenti, implementati e monitorati è possibile attivare un sistema efficace di *compliance*, in grado di presidiare il rischio contabile in modo organico.

A supporto di questa impostazione, un contributo rilevante è stato fornito dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili (CNDCEC) attraverso l'elaborazione delle *check-list* operative del 25 luglio 2023, predisposte come completamento del documento teorico del 7 luglio 2023. Le *check-list*, costruite in forma matriciale e articolate per sezioni (modello di *business*, modello gestionale, assetti organizzativi, amministrativi e contabili), consentono una valutazione puntuale dell'adeguatezza degli assetti in chiave tipologica e dimensionale. Esse rappresentano uno strumento operativo di autocontrollo e autodiagnosi, utile non solo per imprenditori e revisori, ma anche per il collegio sindacale nell'espletamento dei doveri di vigilanza (art. 2403 c.c.). L'utilità delle *check-list* risiede nella capacità di tradurre il principio di proporzionalità in una prassi concreta e documentabile: per ogni area indagata, viene richiesto di indicare il livello di implementazione, la rilevanza del presidio in relazione all'impresa, e le eventuali misure correttive. Tale approccio consente di mappare il rischio di frode su base oggettiva e sistematica.

È interessante osservare come la metodologia sottesa alle *check-list* integri perfettamente le esigenze di controllo preventivo (*ex ante*) e reattivo (*ex post*), ponendosi come ponte tra la dottrina aziendalistica e l'operatività della *governance* societaria. Come rilevato in dottrina[10], si tratta di un "*approccio evidence-based al governo dell'impresa*", fondato su indicatori strutturali e processuali in grado di disinnescare i fattori abilitanti della frode, quali l'asimmetria informativa, l'accentramento del potere decisionale e la mancanza di responsabilità diffusa.

L'utilità delle *check-list* è duplice: da un lato, esse consentono *l'emersione di vulnerabilità strutturali* che potrebbero fungere da varco per condotte fraudolente; dall'altro, esse introducono una logica di *autodiagnosi e rendicontazione interna* che rafforza il principio di *accountability*. Come osservato[11], esse rappresentano uno strumento di "*controllo meta-organizzativo*", in grado di riflettere sul funzionamento stesso del sistema di controllo. In ambito di frode in bilancio, la possibilità di mappare e documentare l'adeguatezza degli assetti *ex ante* potrebbe rivelarsi decisiva non solo in ottica preventiva, ma

[10] Bastia P., "Gli adeguati assetti organizzativi, amministrativi e contabili nelle imprese a struttura complessa e nei gruppi societari", in *La Magistratura*, 2022.

[11] Bastia P., *Gli adeguati assetti organizzativi, amministrativi e contabili nelle imprese a struttura complessa e nei gruppi societari*, cit.

anche nei procedimenti penali o civilistici per dimostrare la diligenza organizzativa dell'organo amministrativo.
Infine, la giurisprudenza ha iniziato a cogliere il nesso tra l'inadeguatezza degli assetti e l'insorgenza o l'occultamento di illeciti contabili. Il Tribunale di Catanzaro[12] ha espressamente collegato la dispersione patrimoniale, la manipolazione delle risorse sociali e la commistione tra interessi familiari e aziendali a una situazione di disorganizzazione sistemica, quindi sintomo di rottura dell'assetto aziendale, tale da legittimare l'intervento *ex* art. 2409 c.c. L'assenza di assetti adeguati ha, in tal caso, favorito, se non agevolato, una condotta fraudolenta continuativa, sottraendo la società a un controllo interno efficace.
In definitiva, l'adeguatezza degli assetti nel contesto delle frodi in bilancio deve essere intesa come capacità sistemica di resistere alla manipolazione, intercettare i segnali di allarme e attivare i correttivi prima che il danno si manifesti in forma irreversibile. Essa si colloca all'intersezione tra diritto sostanziale e pratica manageriale, tra cultura organizzativa e responsabilità legale, e impone un cambio di paradigma: non più controllo *ex post* su eventi patologici, ma organizzazione preventiva del rischio, in linea con i principi dell'impresa sostenibile e trasparente.

5.3. LA CORPORATE GOVERNANCE QUALE PRESIDIO NELLA PREVENZIONE DELLE FRODI

La nozione di *corporate governance*, pur avendo assunto rilevanza scientifica e professionale soprattutto nel corso degli ultimi decenni, affonda le proprie radici in un contesto concettuale ben più remoto. Il termine, la cui etimologia riconduce ai concetti di direzione e controllo (dal latino *gubernare*, ma anche dal greco *kybernao*, "dirigere la nave"), è stato progressivamente assimilato nell'ambito aziendalistico per indicare l'insieme dei meccanismi mediante i quali viene esercitata la guida e il controllo strategico dell'impresa. In tale prospettiva, la *corporate governance* si configura come quell'architettura istituzionale finalizzata ad assicurare l'equilibrio tra i diversi interessi in gioco – *in primis* quelli degli azionisti, dei manager e degli *stakeholder* – garantendo trasparenza, *accountability* e tutela dell'integrità dell'azione imprenditoriale.
Nel contesto italiano, lo sviluppo teorico della *corporate governance* è stato significativamente influenzato dagli scandali finanziari emersi alla fine del XX secolo – si pensi ai casi Cirio e Parmalat – che hanno imposto una riflessione profonda sulla necessità di rafforzare i presìdi di legalità e controllo nell'ambito dell'impresa.
Se nella dottrina anglosassone la *corporate governance* è da tempo oggetto di sistematizzazione[13], nel nostro ordinamento l'approfondimento del tema si è imposto con maggior ritardo, stimolando tuttavia un crescente interesse sia in ambito accademico che professionale.

[12] Tribunale di Catanzaro, Decreto *ex* art. 2409 c.c., 6 febbraio 2024.
[13] Cadbury Committee, *Report on the Financial Aspects of Corporate Governance*, London, 1992; cfr. Zattoni A. (2006), *La corporate governance*, Milano.

La *governance aziendale*, in questa ottica, assume un valore che va ben oltre la mera conformità normativa, rappresentando un *sistema di protezione contro i comportamenti opportunistici e le derive fraudolente* che possono compromettere la continuità dell'impresa e la fiducia del mercato. In tal senso, essa è oggi unanimemente riconosciuta come una componente imprescindibile del sistema di prevenzione delle frodi.

5.3.1. Il ruolo del Consiglio d'Amministrazione

Il Consiglio di Amministrazione (CdA) costituisce l'organo centrale nella struttura della *corporate governance*, in quanto incaricato di definire le linee strategiche, controllare la gestione e monitorare il corretto funzionamento dei meccanismi di controllo interno. La sua *composizione*, le *caratteristiche individuali* dei suoi membri, la *struttura interna* e le *dinamiche operative* rappresentano fattori critici di successo nella prevenzione e nella tempestiva rilevazione di comportamenti fraudolenti.
La prima dimensione da considerare è la *composizione del Consiglio*, in termini di numero, ruolo e indipendenza dei suoi membri. Una composizione equilibrata tra amministratori esecutivi e non esecutivi – con una significativa presenza di consiglieri indipendenti – rappresenta un elemento chiave per assicurare una funzione di vigilanza imparziale e obiettiva[14]. La presenza di soggetti non legati operativamente all'impresa consente, infatti, un miglior presidio dei rischi connessi all'autoreferenzialità dei vertici gestionali.
Peraltro, il tema dell'indipendenza, ancor prima dell'introduzione del codice di *corporate governance,* come rilevato in dottrina da Rossi[15] con particolare riferimento alle società di grandi dimensioni (*id est* quelle le cui azioni sono quotate nei mercati regolamentati), si lega a quello che viene considerato il "*più grande problema tecnico della produzione industriale di massa*", vale a dire la "*dissociazione tra proprietà e controllo*". Secondo l'autore lo schema di dissociazione ha trovato piena "reincarnazione" nella "*corporate governance*", sistema che "guadagna consensi pressoché unanimi", anzi viene ormai considerato strumento applicativo indispensabile per la corretta gestione dell'impresa.
In aggiunta al requisito dell'indipendenza, la pluralità di competenze è un ulteriore aspetto rilevante: un CdA dotato di membri con *background* eterogenei, nel senso di multidisciplinari nel campo giuridico, economico, industriale, è maggiormente in

[14] Beasley M. (1996), *An Empirical Analysis of the Relation between the Board of Director Composition and Financial Statement Fraud*, The Accounting Review.
[15] Rossi G. (2008), *Il mercato d'azzardo,* Milano, pagg. 35 ss. L'autore si esprime così, testualmente: "*La storia del diritto societario si nutre da sempre di paradossi, che rendono nella maggior parte dei casi vano qualsiasi tentativo di riforma. Uno dei più tenaci riguarda le società di grandi dimensioni (per essere più precisi, quelle le cui azioni sono quotate nei mercati regolamentati)…omissis…..Lo schema di dissociazione è stato descritto per la prima volta da Adolf Berle e Gardiner Means in Società per azioni e proprietà privata, un classico del 1932. Ha dunque superato il settantacinquesimo anno di età, ma appare in ottima salute".* Tuttavia, l'autore, pur avendo rilevato che in dottrina esiste una copiosa produzione di studi, cui lo stesso ha contribuito, sottolinea "*Che la critica ad un fenomeno mantenga la sua attualità per quarant'anni può significare solo due cose, che l'autore ha avuto una intuizione geniale o che il fenomeno ha una vischiosità ineliminabile*".

grado di cogliere segnali deboli di comportamenti anomali o non conformi, soprattutto in contesti complessi e dinamici[16].
Le *caratteristiche personali e professionali* dei componenti del Consiglio incidono sensibilmente sulla sua efficacia quale organo di prevenzione delle frodi. In particolare, elementi come l'esperienza maturata in contesti analoghi, l'anzianità nel ruolo, il possesso di titoli accademici avanzati e l'appartenenza a reti professionali o istituzionali influenzano la capacità di intercettare anomalie nei comportamenti gestionali e di opporsi, ove necessario, a scelte rischiose o non trasparenti[17].
Secondo alcuni studi empirici, consiglieri dotati di *capitale relazionale elevato* – ovvero coinvolti in altri *board* di amministrazione – sono maggiormente sensibili alla reputazione e meno propensi a tollerare comportamenti fraudolenti che possano comprometterne l'integrità[18]. Allo stesso tempo, la *seniority* e la partecipazione attiva alle riunioni costituiscono indici indiretti del coinvolgimento e della vigilanza esercitata.
La presenza, in strutture più articolate e complesse, di *comitati endoconsiliari*, quali l'*audit committee*, il *comitato per la remunerazione* e quello per i *rischi*, rappresenta un rafforzamento significativo della funzione di controllo del CdA. Tali organismi, laddove correttamente configurati e dotati di autonomia operativa, consentono una supervisione più approfondita e specialistica delle aree maggiormente esposte a rischio di frode, come la redazione del bilancio o la definizione delle politiche retributive[19].
Il *codice di autodisciplina* delle società quotate italiane (Codice di *Corporate Governance*, Borsa Italiana) sottolinea l'importanza di questi organi, raccomandandone la composizione prevalentemente indipendente e la competenza tecnica dei membri. In particolare, l'*audit committee* rappresenta il presidio principale nella verifica dell'efficacia del sistema di controllo interno e nella supervisione dell'attività della funzione di *internal audit*[20].
Il funzionamento effettivo del Consiglio di Amministrazione non può essere misurato soltanto attraverso la sua composizione o la presenza di comitati specializzati: un elemento cruciale risiede nella *qualità e nell'efficacia dei processi decisionali* che in esso si sviluppano. Il processo decisionale del CdA rappresenta il luogo in cui la funzione di indirizzo e controllo dell'organo si traduce in azione concreta, ed è pertanto un indicatore fondamentale della sua capacità di contribuire alla prevenzione delle frodi e alla gestione dei rischi.
L'efficacia di tale processo si misura attraverso una serie di variabili interdipendenti:

- la *frequenza e regolarità delle riunioni*;
- la *qualità delle informazioni ricevute*;
- la *capacità di analisi critica dei consiglieri*;
- la *cultura della trasparenza*;

[16] Palepu K., Healy P. (2008), *Business Analysis and Valuation*, South-Western Cengage.
[17] Zona F., Zattoni A., Minichilli A. (2013), *Board of directors' contribution to strategy: A literature review and research agenda*, *Corporate Governance*: *An* International Review.
[18] Fich E.M., Shivdasani A. (2006), *Are Busy Boards Effective Monitors?* Journal of Finance, 61(2).
[19] Giacomelli S., D'Onza G. (2007), *Sistemi di controllo interno e ruolo dell'audit committee*, Milano.
[20] Codice di *Corporate Governance* (2020), Borsa Italiana.

- e, non da ultimo, la *dinamica interpersonale tra i membri*[21].

In primo luogo, la *frequenza delle riunioni del CdA* deve essere sufficiente a garantire un monitoraggio continuo delle attività aziendali, soprattutto in contesti operativi complessi o in presenza di segnali di disfunzione. Una bassa frequenza delle riunioni può infatti rappresentare un indicatore di scarsa vigilanza, e nei casi peggiori può configurare una responsabilità omissiva da parte degli amministratori. Al tempo stesso, non basta convocare il CdA in modo regolare: è necessario che i consiglieri partecipino attivamente, ponendo domande, sollevando dubbi, esprimendo dissensi quando necessario, ed evitando di svolgere un ruolo meramente notarile.

Come osservato in dottrina[22], l'efficacia del *board* dipende in larga misura dalla *cognitive conflict*, ovvero dalla capacità di attivare un confronto costruttivo e talvolta critico, nel rispetto dei ruoli e dell'indipendenza reciproca.

Altro elemento centrale è rappresentato dalla *qualità delle informazioni fornite ai consiglieri*. Secondo quanto raccomandato da diversi codici di *best practice* – tra cui quello italiano (Codice di *Corporate Governance* di Borsa Italiana) – i consiglieri devono poter disporre di informazioni complete, aggiornate e tempestive, al fine di potersi esprimere con consapevolezza sulle decisioni da assumere[23]. È infatti evidente che un CdA informato in modo parziale o distorto risulta esposto al rischio di ratificare, inconsapevolmente, decisioni lesive dell'interesse sociale o potenzialmente fraudolente.

Il *corretto funzionamento del flusso informativo* implica non solo il rispetto delle scadenze previste per la trasmissione dei documenti (tipicamente almeno 2 giorni prima della seduta), ma anche la chiarezza e l'accessibilità dei contenuti. Le informazioni devono essere esposte in modo trasparente, con una sintesi degli scenari alternativi e dei rischi connessi.

Un ulteriore aspetto determinante riguarda *l'effettiva indipendenza di giudizio dei consiglieri.* La collegialità delle decisioni, pur essendo un valore centrale del modello italiano di *governance*, rischia di tradursi in conformismo se non è accompagnata da un'effettiva libertà di espressione. È necessario evitare che si instauri un clima di *groupthink*, ovvero un'adesione acritica alle posizioni della maggioranza o dell'amministratore delegato, spesso dettata da dinamiche di potere o dalla paura di compromettere relazioni personali[24].

Per prevenire tali distorsioni, la letteratura suggerisce l'adozione di meccanismi di *diversità cognitiva* all'interno del *board* – ovvero la presenza di soggetti con esperienze e prospettive eterogenee – in grado di alimentare un dibattito autentico e di esercitare un controllo effettivo sulle decisioni critiche[25].

---

[21] Spencer Stuart (2010), Italy Board Index.

[22] Forbes D.P., Milliken F.J. (1999), "*Cognition and corporate governance: Understanding boards of directors as strategic decision-making groups*", Academy of *Management* Review, 24(3), pagg. 489-505.

[23] Codice di *Corporate Governance* (2020), Borsa Italiana, Principio IV, art. 4.3.

[24] Janis I.L. (1982), *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, Boston: Houghton Mifflin.

[25] Eisenhardt K.M., Bourgeois L.J. (1988), *Politics of Strategic Decision Making in High-Velocity Environments: Toward a Midrange Theory*, Academy of *Management* Journal, 31(4), pagg. 737-770.

Infine, un elemento spesso sottovalutato, ma cruciale, è la *cultura del CdA*. In un ambiente dove la trasparenza, la responsabilità individuale e il rispetto delle regole sono valori condivisi e praticati, è più probabile che le decisioni vengano assunte nell'interesse dell'impresa e nel rispetto della legalità. Al contrario, una cultura improntata all'opportunismo, all'autoreferenzialità o alla compiacenza può agevolare la diffusione di comportamenti scorretti o addirittura fraudolenti.
La prevenzione delle frodi, dunque, non può prescindere dalla promozione di una cultura della legalità e della responsabilità all'interno del CdA. Tale cultura si costruisce nel tempo, attraverso la selezione accurata dei componenti, la formazione continua, e l'introduzione di sistemi di valutazione periodica dell'operato dell'organo[26].
In conclusione, il processo decisionale del CdA non è soltanto un'espressione formale della *governance*, ma un meccanismo sostanziale attraverso il quale l'impresa può prevenire derive opache, conflitti di interesse e, nei casi estremi, frodi. Pertanto, è necessario che tale processo sia strutturato, informato, partecipativo e guidato da principi di legalità e trasparenza. La qualità delle decisioni assunte dal CdA è, in ultima analisi, la cartina di tornasole dell'efficacia dell'intero *sistema di governance*.

5.4. L'ETICA AZIENDALE: CODICE ETICO, RESPONSABILITÀ E SANZIONI

La dottrina[27] concorda che un *sistema integrato di prevenzione* deve fondarsi su *tre pilastri fondamentali*: *(i) etica aziendale* (con un codice etico formale), *(ii)* un sistema delle responsabilità chiaro e *(iii)* un sistema disciplinare proporzionato. Questi elementi trovano riscontro nella prassi di revisione contabile internazionale[28] e nei principi di *corporate governance*[29] che invitano a radicare il controllo interno in una cultura di integrità. Nel seguito si analizzerà ciascun pilastro, evidenziando come grandi imprese e PMI vi si rapportino, con i relativi punti di forza, criticità e modalità attuative.
L'*etica aziendale* costituisce il fondamento della prevenzione delle frodi. In presenza di una cultura aziendale trasparente e di principi etici condivisi, i controlli interni risultano più efficaci. Come osservato in letteratura[30], un sistema di controllo parte sempre dal *tone at the top*: i vertici aziendali devono incarnare valori etici e trasparenza e non limitarsi a dichiararli a parole.
Il Comitato di *Corporate Governance* sottolinea analogamente che l'adozione di un codice etico formale – affiancato a comunicazioni interne e formazione – favorisce una cultura aziendale coesa e antifrode. In pratica, il codice etico definisce regole di compor-

[26] Minichilli A., Zattoni A., Zona F. (2009), *Making boards effective: An empirical examination of board task performance*, British Journal of *Management*, 20(1), pagg. 55-74.
[27] Chiappetta F. (2017), Diritto del governo societario, Padova.
[28] Principio di revisione internazionale (ISA Italia) 240 "*Le responsabilità del revisore relativamente alle frodi nella revisione contabile del bilancio*".
[29] Sistema di controllo interno CoSO 2013, The Institute of Internal *Audit*.
[30] Bwerinofa-Petrozzello R. (2023), *Preventive fraud with internal controls: a refresher*. Journal of accountancy.

tamento vietate e consentite, dettando i valori aziendali e le aspettative di lealtà verso *stakeholder* e mercato[31].

Grandi imprese. Le società di grandi dimensioni (specialmente quotate) hanno in genere strutture di *governance* più articolate e obblighi normativi stringenti (art. 2392 c.c., Legge n. 262/2005) che spingono all'adozione di codici etici interni. In esse il *Codice di Autodisciplina* raccomanda la presenza di comitati (controllo interno, remunerazione ecc.) che veicolino valori etici, e spesso è previsto il ruolo di un *officer* dedicato (*compliance officer* o dirigente preposto) alla gestione della trasparenza.

La formalizzazione del codice etico è, pertanto, più diffusa: esso viene spesso deliberato dal CdA, divulgato a tutti i dipendenti e rivisto periodicamente; ciò contribuisce a ridurre l'"*opportunità*" di frode, in quanto chiarisce – fin dall'origine – quali comportamenti sono condannati e quali premiati[32]. Un vantaggio delle grandi imprese è la capacità di investire in formazione etica e in canali di *whistleblowing* strutturati, aumentando la consapevolezza del rischio di frode tra il personale.

PMI. Le piccole e medie imprese italiane, per contro, spesso non hanno codici etici formalizzati, poiché 'approccio familiare ed artigianale tipico delle PMI tende a basarsi sulla fiducia personale piuttosto che su regole scritte. Questo modello "*familistico*" può rendere difficile stabilire principi etici condivisi: la concentrazione della proprietà e della gestione familiare limita la *governance* formale e lascia spazio a norme non scritte[33]. Tuttavia, la dotazione di un codice etico – pur semplificato – è consigliabile anche nelle PMI.

In dottrina[34] si suggerisce la creazione da parte della proprietà di un "*codice etico*" che definisca chiaramente la cultura aziendale e i limiti di condotta, prevedendo le misure disciplinari conseguenti. In pratica, nelle PMI il codice etico può essere veicolato attraverso riunioni periodiche, affissione interna o accordi interni: l'importante è che dipendenti e collaboratori siano consapevoli delle linee guida etiche.

Pur con risorse limitate, le PMI possono dunque recuperare parte dei benefici delle grandi imprese, valorizzando la *coesione culturale*: per esempio, stabilendo responsabilità etiche condivise tra il titolare e i quadri o diffondendo la pratica del *feedback* trasparente. La *principale criticità* rimane però la *governance* informale: nei contesti familiari può prevalere la protezione del *management* interno e una tolleranza per "*piccole irregolarità*" non punite, fattori che aumentano il rischio di frode.

Il *secondo pilastro* riguarda la *definizione chiara delle responsabilità interne*. Un sistema di controllo efficace richiede che i compiti aziendali e le deleghe siano distribuiti in modo da evitare conflitti e da consentire controlli incrociati. In termini generali, ciò significa stabilire chi è responsabile delle varie fasi del ciclo informativo e contabile: redazione del bilancio, gestione finanziaria, *compliance*, *reporting* al CdA, *audit* interno, ecc.

---

[31] Scarcia, G. (2019). *Il codice etico nelle imprese: significato, contenuti e funzione organizzativa*, Milano.

[32] Brown, V. L., Hays, J. B., & Stuebs, M. (2020). "*Modeling Integrity and Ethics in Accounting: A Model Curriculum for Faculty.*" Journal of *Business* Ethics, 164(3), pagg. 503-520.

[33] HBR Italia (2016), *I limiti della governance familistica delle PMI italiane,* www.hbritalia.it.

[34] Papadopoulou I. (2020), *The fraud risk in SMEs and the role of Corporate Governance,* www.accountancygreece.gr.

Una corretta struttura organizzativa (organigramma, descrizioni di mansioni, flussi informativi) è indispensabile per mitigare le opportunità di frode. Il modello COSO 2013, su cui si tornerà più diffusamente nel prossimo paragrafo, ad esempio, sottolinea che l'"*environment di controllo*" include la chiarezza dei ruoli e competenze, in modo che nessuna persona sia responsabile da sola di un processo critico senza supervisione.
Grandi imprese.
Nelle grandi aziende la *governance* societaria prevede strumenti formali per separare e controllare le responsabilità. Ad esempio, il CdA può nominare un comitato interno (o comitato di controllo interno e rischi) che vigila sui processi contabili; un *auditor* interno dedicato conduce verifiche periodiche; il *management* è supportato da strutture (es. ufficio *compliance*, *risk management*) con ruoli distinti.
La *segregazione delle funzioni* ("*segregation of duties*") è più facilmente realizzabile: per esempio, la persona che gestisce i crediti non coincide con chi effettua le riscossioni, e così via. Inoltre, nelle imprese quotate il *dirigente preposto alla redazione dei documenti contabili* (*ex* Legge n. 262/2005) è formalmente incaricato di istituire e mantenere il sistema di controllo interno sui documenti contabili. In virtù di questi meccanismi, le grandi imprese possono distribuire meglio la responsabilità fra più livelli gerarchici e organi di controllo (collegio sindacale, revisori esterni), aumentando la probabilità di intercettare anomalie.
Nelle PMI, per limiti di risorse e per modello decisionale famigliare, spesso mancano funzioni dedicate o figure di controllo indipendenti. In molte piccole realtà proprietario e *management* coincidono: come rilevato[35], "*ruoli, responsabilità e decisioni sono concentrate in una sola persona e prese unilateralmente, senza controllo*". Ciò implica che le PMI devono cercare soluzioni alternative: ad esempio, affiancare eventuali figure chiave (amministratore, direttore commerciale) con revisori esterni o consulenti indipendenti; coinvolgere familiari che non svolgono mansioni operative come "*controllori informali*"; stabilire almeno procedure base (approvazione di uscite, riconciliazione di cassa) anche in forma semplificata. Evidentemente, l'assenza di formalità organizzative tipica delle PMI (organigrammi minimi, processi *"artigianali*") genera punti deboli nei controlli.
Ad esempio, senza adeguata delega negozi contrattuali rilevanti possono essere firmati anche informalmente. Tuttavia, la PMI può compensare con vantaggi tipici della struttura snella: decisioni rapide, minor burocrazia, forte coesione del *team*. In pratica, una modalità attuativa tipica è quella di mantenere momenti formali di comunicazione interna, per esempio controlli congiunti di bilancio periodico tra titolare e responsabile amministrativo.
Anche la normativa italiana di *corporate governance* flessibile permette alle PMI di "*comply or explain*" (applicare o motivare non-adozioni) le raccomandazioni, riconoscendo che strutture molto piccole non potrebbero sopportare comitati complessi. La criticità principale resta comunque la bassa separazione dei ruoli, per cui la prevenzione dipende in larga misura dalla diligenza del titolare.

[35] Papadopoulou I. (2020), *The fraud risk in SMEs and the role of Corporate Governance*, cit.

Il *terzo pilastro* è costituito dalle *ricadute sanzionatorie interne*. Un sistema disciplinare chiaro e certo rafforza i vincoli etici e scoraggia la fraudolenza: come evidenzia il Principio ISA 240, quando una frode viene scoperta devono essere applicate misure disciplinari per evitare ripetizioni. In altri termini, la prospettiva di sanzioni (multa interna, licenziamento, sospensione ecc.) costituisce un deterrente fondamentale in una politica antifrode. Analogamente, la dottrina di diritto societario ricorda che il D.Lgs. n. 231/2001 impone alle aziende che adottano un modello organizzativo l'"*istituzione di un adeguato sistema disciplinare*" per sanzionare la violazione delle procedure interne.

Grandi imprese. Nelle grandi organizzazioni è necessario bilanciare il sistema disciplinare aziendale con le normative sul lavoro (statuto dei lavoratori, contratti collettivi). Pertanto, le sanzioni devono essere proporzionate e formalizzate (verbali di contestazione, codice disciplinare, commissioni disciplinari), per evitare contenziosi legali. In genere esistono in HR policy capitoli dedicati all'infrazione del codice etico, con possibili sanzioni crescenti fino al licenziamento.

L'applicazione speditiva delle misure punitivi è essenziale: come osservato[36], se la frode viene scoperta, "*deve essere intrapresa l'azione disciplinare per scoraggiare altri*" e soprattutto rendere evidente che "*gli errori non saranno tollerati*".

Un vantaggio delle grandi imprese è il possibile coinvolgimento di organi esterni (collegio sindacale, revisori, anche autorità di vigilanza) che segnalano le irregolarità e collaborano all'azione correttiva. Inoltre, l'adozione di modelli organizzativi *ex* D.Lgs. n. 231/2001 implica, già, l'obbligo di graduare le sanzioni interne in base alla gravità degli illeciti, dando trasparenza al potenziale rischio disciplinare.

PMI. Nelle PMI il sistema disciplinare tende ad essere più informale: spesso le sanzioni sono decise in modo diretto dall'imprenditore (es. rimprovero verbale, sospensione del *bonus*, licenziamento). Ciò può rendere la deterrenza meno evidente (ad es. un dipendente infortunatosi perché "*non segnalava*" anomalie potrebbe sentirsi trattato ingiustamente). Tuttavia, anche le PMI sono soggette alle regole generali (art. 2106 c.c. e CCNL) che prevedono la proporzionalità delle sanzioni.

La difficoltà sta nel rendere sistematico e uniforme il processo: un codice etico seguito da uno schedule di sanzioni interne aiuta a non improvvisare le reazioni. Come rileva la letteratura, "*un'azienda consapevole dell'esistenza di una policy antifrode e di un sistema di sanzioni rappresenta un forte deterrente, incidendo sul timore di essere scoperti*"[37]. Pertanto, anche nelle PMI è utile esplicitare (anche con semplici documenti o informativa interna) quali atti sono penalizzati e come: ad esempio, prevedendo che l'eventuale scoperta di illeciti contabili darà luogo a provvedimenti disciplinari o legali adeguati.

In sintesi, mentre le grandi imprese devono integrare il sistema disciplinare con le complesse garanzie contrattuali, le PMI possono puntare sulla chiarezza delle regole interne e sulla loro rapida applicazione per tutti i dipendenti, valorizzando la sostenibilità economica del modello di controllo (anche in base alla dimensione contenuta).

---

[36] Bwerinofa -Petrozzello R. (2023), *Preventive fraud with internal controls: a refresher*, cit.

[37] Lorenzini N. (2019), *Frodi aziendali: rischi e strategie.* www.riskcompliance.it.

Un'efficace politica di prevenzione della frode in bilancio richiede un approccio integrato di tipo multifunzione, che operi a più livelli organizzativi. I tre pilastri – etica, responsabilità e disciplina – agiscono in sinergia: l'etica (supportata da un codice di comportamento) crea la cultura di riferimento, un sistema delle responsabilità ben disegnato assicura che i compiti vengano svolti con trasparenza, e un adeguato apparato sanzionatorio applica conseguenze certe in caso di violazione. Se nelle grandi imprese questo sistema può contare su strutture dedicate e formalizzate, nelle PMI va costruito in modo proporzionato alle risorse disponibili, sfruttando la flessibilità decisionale ma senza rinunciare alla chiarezza dei processi.
Ricerche nel campo aziendale evidenziano come la mancata formalizzazione di questi elementi – tipica di molte PMI – costituisca un fattore di rischio rilevante. In definitiva, una *governance* interna solida (anche semplificata) e trasparente, ancorata a valori etici condivisi e accompagnata da controlli incrociati e da conseguenze certe, è il modo migliore per minimizzare il rischio di frodi contabili, tutelando gli *stakeholder* e la reputazione aziendale.

5.5. SISTEMI DI CONTROLLO INTERNO E AUDITING

La prevenzione e il contrasto delle frodi aziendali richiedono un approccio integrato che coinvolge sia robusti sistemi di controllo interno sia efficaci attività di *auditing* (interno ed esterno). Numerosi scandali finanziari hanno evidenziato come lacune nei controlli e nell'attività di revisione possano consentire manipolazioni contabili su larga scala.
Di conseguenza, nel corso degli ultimi decenni si è sviluppata una vasta letteratura teorica e professionale incentrata sul potenziamento dei controlli interni e sul ruolo proattivo dell'auditing nel prevenire, individuare e investigare le frodi societarie. In questo contesto, fondamentale è il contributo del modello CoSO (*Committee of Sponsoring Organizations of the Treadway Commission*) – *Internal Control – Integrated Framework* (più noto come "*CoSO Report*") – e dei suoi successivi aggiornamenti del 2004, 2013 e 2017, che hanno fornito uno *standard* di riferimento internazionale per la struttura dei controlli interni e la gestione dei rischi aziendali[38].
La trattazione che segue, di taglio teorico, esaminerà l'evoluzione di tali f*ramework* e il ruolo chiave sia dei sistemi di controllo interno sia dell'attività di *auditing* nella prevenzione e contrasto delle frodi, con particolare attenzione alle frodi di bilancio. Verranno integrati contributi accademici e istituzionali per delineare un quadro organico e aggiornato della materia, evidenziando come un solido impianto di controlli unito a funzioni di *audit* efficaci costituisca la prima linea di difesa contro i comportamenti fraudolenti in ambito aziendale.

[38] Gasparri G. (2013), *I controlli interni nelle società quotate,* Quaderni Consob.

5.5.1. Sistemi di controllo interno e prevenzione delle frodi

L'alta direzione, nell'ambito della regolazione del sistema aziendale, si trova a operare in contesti di incertezza strategica e di crescente esposizione al rischio. Il SCI (Sistema di Controllo Interno) assume in tal senso una funzione non solo di guida, ma anche di "sistema frenante", ovvero di un sistema di vincoli che ha lo scopo di far conoscere i rischi da evitare e di rimuovere ogni possibilità di giustificare comportamenti in grado di esporre l'impresa a livelli di rischio indesiderabili[39]. Insomma, il SCI deve essere idoneo ad attivare vincoli funzionali ad evitare derive comportamentali che potrebbero compromettere la sostenibilità dell'impresa.
Un sistema di controllo interno adeguato è unanimemente riconosciuto come elemento centrale nella prevenzione delle frodi. Il *controllo interno*, secondo la definizione classica proposta dal CoSO *Report* del 1992, è "*un processo, svolto dal consiglio di amministrazione, dai dirigenti e da altri operatori della struttura aziendale, che si prefigge lo scopo di fornire una ragionevole sicurezza sulla realizzazione dei seguenti obiettivi: efficacia ed efficienza delle attività operative; attendibilità delle informazioni di bilancio; conformità alle leggi e ai regolamenti*".
Questa definizione evidenzia *tre obiettivi fondamentali* – **operatività efficiente, affidabilità del reporting finanziario,** e ***compliance*** **normativa** – che costituiscono le aree in cui i controlli interni devono fornire una ragionevole sicurezza. In particolare, la tutela dell'attendibilità delle informazioni di bilancio è direttamente collegata alla prevenzione delle frodi di natura contabile: un efficace sistema di controlli interni riduce drasticamente le opportunità di manipolare dati finanziari o di aggirare procedure contabili.
Non a caso, il CoSO nacque proprio a seguito dei lavori della Commissione *Treadway (National Commission on Fraudulent Financial Reporting*, 1985-1987) istituita per far luce sul fenomeno delle frodi finanziarie negli Stati Uniti e proporre raccomandazioni; il rapporto finale di tale commissione pose le basi concettuali per un modello integrato di controllo interno volto a prevenire le falsificazioni di bilancio e le pratiche fraudolente.
Da allora, il CoSO è divenuto uno *standard di riferimento* globale sia per le imprese sia per i revisori, fornendo criteri per valutare l'adeguatezza dei sistemi di controllo interno, specialmente in relazione all'informativa finanziaria.
Il modello di controllo interno delineato dal CoSO identifica *cinque componenti interdipendenti* che, operando in modo integrato, creano un *efficace sistema di prevenzione e individuazione delle irregolarit*à. I cinque componenti fondamentali del sistema di controllo interno (CoSO 1992, aggiornato nel 2013) sono:
Ambiente di controllo – il tono etico e l'atmosfera organizzativa instaurata dal *top management* e dagli organi di *governance*. Esso comprende l'integrità e i valori etici aziendali, la filosofia gestionale, la struttura organizzativa, le politiche di gestione del

[39] Così Simons R. (2000), *Performance Measurement and Control System for Implementing Strategy*, Upper Saddle River, N.J., Prentice - Hall. Sul punto, si veda anche Paletta A., *Il controllo interno nella corporate governance*, 2008, Bologna, p. 81.

personale e l'efficacia del consiglio di amministrazione e del *comitato di audit*. Un solido ambiente di controllo crea una cultura aziendale improntata all'onestà e all'etica, riducendo la tolleranza verso comportamenti fraudolenti.
Ad esempio, "*tone at the top*" inadeguato e scarsa enfasi sui valori etici hanno spesso facilitato grandi frodi societarie, mentre un forte esempio etico dai vertici funge da deterrente alle violazioni.
Valutazione dei rischi – il processo di identificazione e analisi dei rischi aziendali, inclusi i rischi di frode, che possono impedire il raggiungimento degli obiettivi. Una valutazione del rischio efficace comprende l'individuazione delle aree e dei processi più esposti a potenziali frodi (ad esempio, settori dell'azienda dove esistono incentivi a manipolare i risultati o vulnerabilità nei controlli) e l'analisi dei fattori interni ed esterni che possono incrementare tali rischi. Nel modello CoSO aggiornato, la valutazione dei rischi di frode è diventata un principio esplicito: il framework del 2013 prevede espressamente che l'organizzazione consideri il potenziale di frode nella valutazione dei rischi. Questo riconoscimento formale – assente nel *framework* originale del 1992 – enfatizza la necessità per il *management* di includere scenari di frode (frodi finanziarie, appropriazioni indebite, corruzione, ecc.) nell'analisi dei rischi, predisponendo adeguati controlli preventivi.
Attività di controllo – le politiche, procedure e prassi operative che assicurano l'esecuzione delle direttive del *management* in risposta ai rischi identificati. Rientrano in questo ambito sia controlli di tipo preventivo (es: segregazione delle funzioni critiche, autorizzazioni approvative, limitazioni di accesso ai sistemi informativi, doppie firme) sia controlli rilevativi (es: riconciliazioni, verifiche a campione, analisi di scostamento, controlli di revisione). Tali attività mirano a ridurre le opportunità di frode, bloccando sul nascere comportamenti anomali oppure segnalando tempestivamente irregolarità prima che possano ingigantirsi. Ad esempio, una rigorosa segregazione dei compiti (nessun singolo dipendente può completare da solo un intero processo finanziario critico) elimina molte possibilità di manipolazione; allo stesso modo, controlli automatizzati sui dati contabili possono segnalare voci sospette o fuori *range* da approfondire. È importante sottolineare che le *attività di controllo devono essere commisurate al livello di rischio*: aree ad alto rischio di frode (come la gestione della tesoreria, le vendite in contanti, gli appalti) richiederanno controlli più stringenti e frequenti.
Informazione e comunicazione – riguarda sia i flussi informativi interni sia la comunicazione verso l'esterno. Un'efficace comunicazione interna assicura che il personale a tutti i livelli conosca le proprie responsabilità di controllo, le politiche anti-frode dell'azienda e le procedure da seguire per segnalare eventuali comportamenti scorretti. Ciò include l'istituzione di canali di *whistleblowing* o linee etiche riservate, attraverso cui dipendenti, fornitori o altri soggetti possano segnalare anonimamente sospetti di frode o irregolarità senza timore di ritorsioni. La comunicazione esterna, invece, concerne lo scambio di informazioni rilevanti con gli *stakeholder* e le autorità: ad esempio, una rendicontazione finanziaria trasparente e veritiera e adeguate comunicazioni agli organi di vigilanza contribuiscono a scoraggiare tentativi di frode di bilancio. In sintesi, questo

componente garantisce che informazioni affidabili e pertinenti circolino adeguatamente dentro e fuori l'organizzazione, supportando sia le decisioni di controllo sia la fiducia del pubblico.

Attività di monitoraggio – rappresentano il processo attraverso cui la direzione aziendale verifica, in modo continuo e/o periodico, che gli altri componenti del controllo interno funzionino efficacemente nel tempo. In pratica, si tratta di attività di supervisione e valutazione *ex post* dei controlli: revisioni interne, ispezioni, *audit* periodici indipendenti, nonché il *follow-up* delle segnalazioni di anomalia. Il monitoraggio continuo avviene nell'operatività quotidiana (ad esempio mediante sistemi di allerta automatizzati o supervisione gerarchica costante), mentre le valutazioni separate sono svolte da funzioni indipendenti – tipicamente l'*Internal Audit* – con cadenza periodica.

Queste verifiche servono a identificare carenze o debolezze nel sistema di controllo interno e a garantire che vengano prontamente corrette. Un efficace monitoraggio, inoltre, aggiorna il sistema di controllo man mano che muta il contesto aziendale, assicurando l'adattamento a nuovi rischi o cambiamenti organizzativi. In ottica anti-frode, le attività di monitoraggio rivestono un ruolo cruciale: da un lato, rilevano eventuali segnali di frode o non conformità sfuggiti ai controlli di linea; dall'altro, fungono da deterrente perché i potenziali frodatori sanno che esiste una vigilanza attiva e indipendente sulle operazioni aziendali.

Questi cinque elementi, operando in sinergia, creano un sistema di controllo interno capace di incidere su due dei tre fattori che, secondo la teoria del "*triangolo delle frodi*", determinano il verificarsi di una frode.

In base a tale teoria – sviluppata negli studi di Donald Cressey e ripresa dalla letteratura successiva, già oggetto di ampio approfondimento nel precedente paragrafo 1.2. ("*Concetti generali di frode aziendale, frodi interne ed esterne; il "triangolo delle frodi"*") – perché una frode si realizzi devono coesistere:

1. una pressione o incentivo che spinge un individuo a delinquere (esigenze finanziarie, obiettivi di *performance* irrealistici, ambizione di arricchimento, ecc.);
2. un'opportunità percepita di poter commettere l'atto illecito senza essere scoperti, sfruttando debolezze del sistema, e
3. la razionalizzazione/atteggiamento dell'individuo che gli consente di giustificare a sé stesso il comportamento fraudolento.

Mentre il primo e il terzo elemento attengono alla *sfera motivazionale e psicologica* del soggetto, l'opportunità di frode dipende in larga parte da *fattori organizzativi* controllabili dall'impresa – *in primis* l'efficacia dei controlli interni. Come sottolineato in letteratura, "*l'opportunità di commettere una frode nasce dalla consapevolezza dell'autore di poter sfruttare i punti deboli esistenti nel sistema dei controlli interni, con la possibilità di celare il crimine ed evitare così la sanzione*"[40].

Sulla base del noto modello del "triangolo della frode", viene proposta una riqualificazione del concetto, orientata alla funzione del sistema di controllo interno. Il SCI si

[40] Gabbioneta, C., Greenwood, R., Mazzola, P., & Minoja, M. (2013). *The influence of the institutional context on corporate illegality*. Accounting, Organizations and Society, 38(6–7), pagg. 484-504.

configura come lo strumento in grado di trasformare situazioni di pressione in contesti imprenditoriali in equilibrio con legalità ed etica.
Il triangolo della frode può essere utilizzato con uno scopo più generale per identificare la funzione del SCI in cui avere un adeguato sistema di controllo interno è altrettanto importante che avere buone strategie. Insomma, come rilevato in dottrina[41] il SCI agisce "nel trasformare una situazione di impresa fuori controllo in una situazione di impresa che coniuga imprenditorialità, etica e legalità".
Ne discende che un sistema di controllo interno robusto riduce drasticamente le opportunità di comportamento fraudolento: procedure ben disegnate e applicate rendono più difficile aggirare le regole o occultare discrepanze, aumentando al contempo la probabilità di rilevare tempestivamente eventuali anomalie. In altri termini, i controlli interni agiscono come un meccanismo di deterrenza: elevano la percezione del rischio di essere scoperti e quindi il costo potenziale della frode per l'agente, scoraggiandolo dal porla in essere. Allo stesso tempo, promuovendo una cultura etica (*ambiente di controllo*) possono influire anche sulla razionalizzazione, creando un contesto valoriale in cui è meno accettabile "*autogiustificare*" comportamenti illegali.

5.5.2. Il modello CoSO e la sua evoluzione (1992-2017)

Il *CoSO Internal Control – Integrated Framework*, pubblicato originariamente nel 1992[42], ha rappresentato il *primo modello organico* per la *progettazione e valutazione dei sistemi di controllo interno*. Esso fu sviluppato con l'obiettivo di fornire linee guida univoche in un'epoca in cui non esisteva ancora una definizione condivisa di controllo interno. Il modello introduceva i *cinque componenti chiave* discussi sopra e presentava una rappresentazione visuale – il *celebre cubo CoSO* – in cui tali componenti (sulle colonne orizzontali) vengono mappati con i *tre obiettivi* (colonne verticali: *Operations, Financial Reporting, Compliance*) e con i *diversi livelli organizzativi dell'azienda* (unità di *business*, divisioni, entità aziendale nel suo complesso).

[41] Così Paletta A., 2008, cit. p. 83.
[42] CoSO, *Internal Control – Integrated Framework*, AICPA, 1992 (trad. it. Il sistema di controllo interno – Quadro integrato).

Tavola 5.1. – **Il cubo CoSO ed i suoi elementi**

Questa struttura a cubo evidenziava che un efficace controllo interno deve permeare l'intera organizzazione, interessando tutte le unità e livelli, e garantire una copertura di controllo su tutti gli obiettivi aziendali principali. Il CoSO 1992 ottenne rapida diffusione a livello internazionale ed è divenuto un paradigma di riferimento sia in ambito manageriale sia in ambito di revisione contabile.
Ad esempio, la definizione CoSO di "*controllo interno*" è stata recepita nello *Statement on Auditing Standards n.78 dell'AICPA* nel 1995 e, in Italia, ha influenzato i codici di autodisciplina e le *best practice* sul governo societario e i controlli (si pensi al Codice di *Corporate Governance* per le società quotate).
Nel 2004, il CoSO ha pubblicato un secondo framework fondamentale: *l'Enterprise Risk Management – Integrated Framework (ERM)*, spesso indicato come "*CoSO Report 2*"[43]. Questo aggiornamento del 2004 ampliò l'orizzonte dal controllo interno tradizionale alla più ampia gestione integrata dei rischi d'impresa. In pratica, l'ERM incorpora il concetto di controllo interno all'interno di un *modello olistico di risk management*, che

[43] CoSO, *Enterprise Risk Management – Integrated Framework*, 2004.

include non solo i rischi legati all'affidabilità del bilancio, ma tutte le categorie di rischio (strategico, operativo, finanziario, di *compliance*, ecc.) che possono pregiudicare il raggiungimento degli obiettivi aziendali.
Il CoSO ERM 2004 mantiene una *struttura a componenti* (otto elementi in questo caso, espansi rispetto ai cinque del modello 1992) e sottolinea l'importanza di processi come l'impostazione degli obiettivi strategici, l'identificazione degli eventi di rischio, la determinazione della risposta al rischio e il monitoraggio continuo. In sostanza, con l'ERM il controllo interno viene integrato nella strategia aziendale: non più un sistema a sé stante focalizzato sul r*eporting* finanziario, ma parte integrante dei processi di pianificazione e gestione dei rischi strategici e operativi dell'impresa.
Dal punto di vista della prevenzione delle frodi, l'ERM ribadisce che i rischi di frode sono rischi aziendali a tutti gli effetti e vanno gestiti con gli stessi rigorosi approcci con cui si gestiscono altri rischi chiave. Ad esempio, *inserire il rischio di frode di bilancio nella mappa dei rischi strategici d'impresa* significa attribuirgli una valutazione di impatto e probabilità, definirne gli *owner* (responsabili) e le *azioni di risposta* (controlli, politiche antifrode, programmi di etica, ecc.), monitorandolo nel tempo.

Tavola 5.2. – **Il cubo CoSO ERM 204**

Il *framework* CoSO ERM ha avuto grande influenza nel promuovere una cultura del *risk management* a livello d'impresa, portando molte organizzazioni a rafforzare i propri

presidi non solo sui rischi finanziari, ma anche su quelli operativi e di *compliance*. È utile notare che lo sviluppo dell'ERM nel 2004 fu – in parte – stimolato da nuove normative emanate in risposta a clamorosi scandali finanziari: ad esempio, negli Stati Uniti la legge Sarbanes-Oxley (SOX) del 2002 impose alle società quotate e ai revisori esterni una valutazione attesta del sistema di controllo interno sulla rendicontazione finanziaria (Section 404), dando forte impulso all'adozione di framework strutturati come il CoSO.
In Europa e in Italia, analoghe istanze di rafforzamento dei controlli interni si sono tradotte in aggiornamenti normativi e di *corporate governance* a metà anni 2000, incoraggiando l'approccio integrato al *risk management* e alla prevenzione delle frodi.
Nel 2013, a vent'anni di distanza dal primo *CoSO Report*, il *framework di Internal Control* è stato oggetto di un sostanziale *aggiornamento* per adeguarlo ai profondi cambiamenti intercorsi nel contesto operativo, tecnologico e regolamentare. *Il CoSO Internal Control – Integrated Framework (2013)*[44] conserva i cinque componenti originari, ma *introduce 17 principi esplicativi* che ne dettagliano i requisiti di efficacia:

- maggiore enfasi sulla definizione chiara degli obiettivi aziendali come precondizione per un controllo efficace (*refresh* degli obiettivi, con ampliamento della categoria "*Reporting*" oltre il bilancio esterno, includendo *reporting* interno e non-finanziario);
- esplicitazione del bisogno di valutare i rischi nuovi ed emergenti (cambiamenti di contesto) e in particolare evidenza alla valutazione dei rischi di frode come principio a sé stante (Principio n.8);
- introduzione dei "*punti di attenzione*" (*points of focus*) per ciascun principio, ossia indicazioni pratiche su elementi da considerare per valutare se il principio è presente e funzionante;
- aggiornamento della terminologia ed integrazione dei temi di IT *governance* e controllo sui sistemi informativi (ad esempio con un principio dedicato ai controlli IT, il n. 11);
- riconoscimento esplicito dell'importanza della *governance* e del ruolo degli organi di controllo indipendenti (come il consiglio e il *comitato audit*) per implementare un sistema di controllo efficace.

Il CoSO 2013, insomma, non stravolge il modello precedente – che si era dimostrato solido – ma lo rafforza e adatta alle esigenze contemporanee: chiarisce che tutti i 17 principi (e dunque i 5 componenti) devono essere presenti e funzionanti per poter affermare che un sistema di controllo interno è efficace; incoraggia un approccio più strutturato alla valutazione di efficacia (ad esempio, prevedendo che l'assenza di uno solo dei principi, se rilevante, può inficiare l'intero sistema); e allinea il *framework* ai nuovi livelli di aspettativa degli *stakeholder*, tra cui vi è la maggiore aspettativa di prevenire e scoprire le frodi nel contesto *post*-crisi finanziaria.
Dal punto di vista pratico, l'aggiornamento del 2013 ha stimolato le imprese ad adottare processi più formalizzati di *fraud risk assessment* e ad integrare meglio i controlli

[44] CoSO, *Internal Control – Integrated Framework* (Updated Edition), 2013.

anti-frode nel disegno dei processi aziendali. Ad esempio, molte organizzazioni hanno introdotto specifici programmi di *whistleblowing*, rafforzato le verifiche di *background* sul personale in posizioni sensibili, e ampliato l'uso di *data analytics* per il monitoraggio di transazioni anomale, in linea con le *best practice* suggerite dal nuovo *framework*.
Infine, nel 2017 il CoSO ha pubblicato un nuovo aggiornamento del *framework di Enterprise Risk Management*, intitolato "*Enterprise Risk Management – Integrating with Strategy and Performance*"[45]. Questo documento sostituisce ed evolve il CoSO ERM del 2004, rispecchiando l'ulteriore maturazione del pensiero sul *risk management* nell'ultimo decennio. La *novità centrale* del CoSO ERM 2017 è *l'esplicito inserimento del risk management nel cuore della pianificazione strategica e della gestione delle performance aziendali.*
In altri termini, il rischio (incluso il rischio di frode) non deve più essere gestito come un'attività separata o un semplice elenco di minacce da mitigare, ma come parte integrante dei processi di formulazione della strategia, di allocazione delle risorse e di misurazione dei risultati.
Il *framework* 2017 enfatizza il *concetto di cultura del rischio*: definisce l'ERM come "la *cultura, le capacità e le prassi integrate con la strategia e l'operatività, che le organizzazioni adottano per gestire i rischi nel processo di creazione, conservazione e realizzazione del valore*". Viene quindi spostato il *focus* sul *concetto di valore*: il *risk management* efficace è quello che aiuta a conseguire gli obiettivi strategici e le *performance* desiderate, mantenendole allineate al livello di rischio ritenuto accettabile dall'organizzazione (*risk appetite*).
Rispetto alla versione 2004, il CoSO 2017 adotta una struttura completamente rivista (non più il cubo a 8 componenti, ma un modello a nastro/fasce che identificano 5 elementi interconnessi del processo di gestione del rischio) e articola 20 principi fondamentali.
Per quanto concerne il tema delle frodi, pur trattandosi di un *framework* di taglio più strategico, l'ERM 2017 ribadisce che *gestire il rischio di frode* è *parte integrante del sistema di gestione dei rischi d'impresa*. In particolare, nella fase di valutazione del rischio, la dirigenza e il consiglio devono assicurarsi di includere esplicitamente i potenziali eventi di frode tra gli scenari considerati, valutandone l'impatto sul modello di *business* e predisponendo piani di risposta (prevenzione, rilevazione, risposta *post*-evento).
Inoltre, il *focus* sulla cultura organizzativa promosso dal CoSO 2017 richiama l'attenzione sull'importanza di valori etici forti e di meccanismi di controllo "*soft*" (come codici etici, formazione, incentivi appropriati) nel dissuadere comportamenti fraudolenti e nel sostenere un ambiente di controllo efficace.
In definitiva, l'evoluzione dei modelli CoSO dal 1992 al 2017 mostra un *progressivo ampliamento di prospettiva*: dal controllo interno focalizzato prevalentemente sul bilancio si è passati a una visione integrata del governo dei rischi, dove la prevenzione delle

[45] CoSO, *Enterprise Risk Management – Integrating with Strategy and Performance*, 2017.

frodi è uno degli obiettivi cardine, da perseguire non solo con procedure operative, ma anche mediante un complessivo allineamento di strategia, cultura e controlli[46].

5.5.3. Il ruolo dell'internal audit nella lotta alle frodi.

Tra gli attori chiave del sistema di controllo interno, la *funzione di Internal Audit* riveste un ruolo cruciale nella prevenzione, rilevazione e contrasto degli episodi di frode aziendale. L'*Internal Audit* è definito dall'Institute of Internal Auditors (IIA) come un'attività indipendente e obiettiva di assurance e consulenza, finalizzata a migliorare le operazioni dell'organizzazione[47].

In relazione alle frodi, la sua importanza discende dal fatto che ogni frode societaria tende ad aggirare o eludere i controlli interni, minandone l'efficacia; di conseguenza, spetta proprio all'*Internal Audit* il compito di *valutare criticamente l'adeguatezza del sistema di controllo interno e di fornire assurance sulla corretta predisposizione ed attuazione dei controlli da parte del management*. In altri termini, gli *internal auditor* agiscono come "*occhi indipendenti*" all'interno dell'azienda, incaricati di verificare che i meccanismi di prevenzione dei rischi – inclusi i rischi di frode – siano progettati in modo appropriato e operino effettivamente come previsto.

L'apporto dell'*Internal Audit* nella gestione del rischio frode può essere analizzato distinguendo *tre macro-aree di intervento*: *prevenzione*, *detection (individuazione*) e *investigazione*. Queste categorie, spesso richiamate in dottrina[48] come *fasi* del c.d. "*fraud auditing*", rappresentano una classificazione delle attività che l'*internal auditor* (in collaborazione con altre funzioni aziendali) può svolgere per fronteggiare il fenomeno fraudolento:

Prevenzione: consiste nell'insieme di attività volte a evitare che una frode abbia luogo. In pratica, gli *internal auditors* contribuiscono a prevenire le frodi innanzitutto identificando proattivamente le aree aziendali più esposte al rischio di comportamenti fraudolenti e valutando le relative modalità potenziali di frode (ad esempio: "*quali tipi di frode potrebbero avvenire nel processo acquisti, e come potrebbero essere perpetrati*?"). Sulla base di queste valutazioni, l'*Internal Audit* fornisce raccomandazioni e consulenza per rafforzare il sistema di prevenzione: può suggerire controlli aggiuntivi, migliorare procedure, colmare lacune organizzative che costituiscono opportunità di frode.

La prevenzione include anche la promozione di una cultura aziendale antifrode: l'*Internal Audit* spesso collabora a programmi di formazione del personale sulla sensibilizzazione ai temi etici, aiuta a sviluppare codici di condotta e contribuisce a far comprendere l'importanza di rispettare le regole. Inoltre, gli internal auditor possono svolgere periodici *fraud risk assessment* insieme al *management*, per aggiornare la mappatura dei rischi di frode e valutare se i controlli posti in essere sono sufficienti a mitigarli. Un

[46] Provasi R. (2020), *Le dinamiche evolutive del sistema di controllo interno*, Milano.

[47] Institute of Internal Auditors (IIA) (2017*), International Standards for the Professional Practice of Internal Auditin*g (Standards).

[48] Pogliani, G., Pecchiari, N., Mariani, M. (2012), *Frodi aziendali: forensic accounting, fraud auditing e litigation*, Milano. pag. 476.

aspetto di prevenzione sempre più rilevante è l'analisi dei dati aziendali (*data analytics*) con finalità preventive: l'IA può sviluppare indicatori di anomalia (*red flags*) e modelli predittivi per segnalare transazioni o andamenti fuori dalla norma, indirizzando controlli mirati prima che una potenziale frode si concretizzi.

Detezione (individuazione tempestiva): poiché il rischio zero non esiste, accanto alla prevenzione è fondamentale la capacità di scoprire velocemente eventuali frodi in atto o già consumate, limitandone i danni. Gli *internal auditor*, grazie alla loro conoscenza approfondita dei processi e ai controlli di monitoraggio che eseguono, sono spesso in una posizione privilegiata per rilevare segnali d'allarme e situazioni anomale indicativi di possibili frodi. Ad esempio, attività di *auditing* regolare possono portare alla luce discrepanze inspiegabili nei registri contabili, riconciliazioni non effettuate, documenti mancanti o alterati, transazioni inusuali con parti correlate, ecc.

Oltre alle tradizionali verifiche, l'*Internal Audit* può impiegare *tecniche specifiche di fraud detection*: *continuous auditing* con strumenti informatici (che esaminano continuamente l'insieme delle transazioni alla ricerca di eccezioni secondo regole predefinite), *digital forensics* su sistemi IT per individuare accessi non autorizzati o tracce di attività illecite, *analisi mirate* su account e scritture contabili sospette.

Importante è anche l'implementazione di canali di segnalazione interna (*whistleblowing*): l'*Internal Audit* spesso gestisce o amministra questi canali, occupandosi di valutare e investigare le segnalazioni ricevute. In sintesi, il ruolo di detection dell'IA si esplica nel monitoraggio indipendente e nell'attenzione costante a possibili sintomi di frode, in modo da intervenire *quanto prima possibile* rispetto al momento di realizzazione dell'atto fraudolento; ciò minimizza le perdite economiche e reputazionali per l'azienda e aumenta le probabilità di recuperare beni o prevenire ulteriori illeciti.

Investigazione: quando emerge un fondato sospetto o un'indicazione concreta che una frode sia avvenuta, l'*Internal Audit* può essere chiamato a condurre o supportare l'indagine interna sul caso. In questa fase, l'obiettivo è raccogliere evidenze, quantificare l'impatto, identificare i responsabili e le modalità della frode, così da intraprendere le opportune azioni correttive, disciplinari o legali. Tipicamente l'IA collabora con altre funzioni aziendali (ad es. l'ufficio legale, la *compliance*, la sicurezza) e, se del caso, con *consulenti esterni specializzati in forensic accounting*. L'*Internal Audit* apporta valore in quanto dispone dell'accesso alla documentazione e ai sistemi aziendali, conoscendo al contempo le procedure interne: ciò consente di ricostruire i fatti con maggiore rapidità ed efficacia.

È fondamentale, tuttavia, che queste investigazioni siano condotte con professionalità e riservatezza, seguendo protocolli formali di *fraud investigation* per assicurare la validità delle prove raccolte e evitare accusatori infondati. Nei casi più complessi, le organizzazioni di grandi dimensioni istituiscono, talvolta, un'apposita *unità di fraud investigation* all'interno dell'*Internal Audit*, composta da specialisti (ad esempio, *Certified Fraud Examiners*) dedicati esclusivamente a indagini di frode. In assenza di tale struttura, comunque, è buona prassi che il *management* ricorra a esperti esterni in materia di frodi quando necessario, così da garantire un approccio investigativo appropriato e competente. L'*In-*

ternal Audit, anche se non sempre dispone di risorse forensi interne, ha il dovere di riconoscere i propri limiti e suggerire l'intervento di specialisti quando la situazione lo richiede – sempre nell'ottica di tutelare al meglio l'azienda e i suoi *stakeholder* dagli effetti di una frode.
Va sottolineato che il *coinvolgimento* dell'*Internal Audit* nelle attività di prevenzione e contrasto delle frodi deve *contemperare due esigenze*:

- mantenere l'indipendenza e obiettività di giudizio (caratteristica fondante dell'IA), evitando di assumere responsabilità gestionali che spettano invece al *management* operativo;
- fornire un supporto proattivo e competente all'organizzazione nel migliorare i propri processi di controllo e risposta ai rischi di frode.

Gli *Standard* Internazionali per la Pratica Professionale dell'*Internal Auditing* emanati dall'IIA delineano bene questo equilibrio. Ad esempio, lo *Standard* 2120.A2 stabilisce che "*l'attività di internal auditing deve valutare la probabilità di frodi ed il modo in cui l'organizzazione gestisce il rischio di frode*". Inoltre, lo *Standard* 1210.A2 richiede che "*gli internal auditor abbiano conoscenze sufficienti per valutare il rischio di frode e le modalità con cui l'organizzazione lo gestisce, ma non ci si attende che posseggano le competenze di una persona la cui responsabilità primaria sia la rilevazione e l'investigazione delle frodi*".
In base a tali principi, l'*Internal Audit* deve quindi:

- conoscere i tipici schemi di frode e le tecniche per rilevarli, valutare criticamente se la struttura di controllo dell'azienda è adeguata a prevenirli;
- segnalare eventuali debolezze o lacune, e supportare l'implementazione di miglioramenti.

Non è compito dell'IA sostituirsi ai responsabili operativi nell'attuare i controlli, né tantomeno assumere il ruolo di organo inquirente in senso stretto (salvo nei limiti delle indagini interne). In pratica, l'IA facilita e verifica che il *management* adotti un efficace *Fraud Risk Management*, fornendo assicurazione indipendente sul fatto che i processi siano progettati e funzionino per tenere sotto controllo il rischio di frode.
Un altro aspetto rilevante è che l'*Internal Audit*, per svolgere efficacemente questo ruolo, deve a sua volta disporre di un *adeguato supporto da parte dell'alta direzione e del consiglio di amministrazione*. Il *messaggio antifrode deve essere sostenuto dal vertice*: il comitato per il controllo interno / comitato *audit* dovrebbe garantire che la funzione di IA abbia sufficiente autorità, risorse e accesso alle informazioni per poter operare.
Solo con un forte mandato dall'alto, infatti, l'*Internal Audit* può incidere realmente, ad esempio raccomandando azioni disciplinari in caso di frodi individuate o promuovendo investimenti in nuovi controlli e tecnologie di prevenzione. In molte giurisdizioni, i *codici di corporate governance* prevedono esplicitamente che il responsabile dell'*Internal Audit* riferisca funzionalmente al comitato *audit* (od organo equivalente) proprio per assicurarne l'indipendenza dal *management* su cui deve vigilare.
Questa *struttura di governance dei controlli* ha dimostrato di essere efficace nel rendere l'azione dell'IA più incisiva anche in materia di frodi, poiché riduce il rischio che segna-

lazioni scomode vengano insabbiate dai dirigenti coinvolti e garantisce un reporting line diretto verso chi può prendere provvedimenti correttivi.
In sintesi, l'analisi evidenzia come sistemi di controllo interno solidi e funzioni di *auditing* efficienti siano pilastri complementari di una strategia organica di prevenzione e contrasto alle frodi aziendali.
I controlli interni – specialmente se implementati secondo modelli riconosciuti come il CoSO e aggiornati alle evoluzioni normative e di contesto – creano un *tessuto difensivo* che *riduce le opportunità di comportamento fraudolento e favorisce una cultura della compliance e dell'etica*. La progressiva raffinatezza dei *framework* (dal 1992 al 2017) ha integrato la gestione del rischio di frode nel più ampio alveo del *risk management* e della *governance* strategica, segno della consapevolezza crescente che la lotta alle frodi non è solo una questione di tecnicismi contabili, ma di visione strategica, cultura aziendale e governo dei processi.
Parallelamente, l'attività di *auditing* – sia interno che esterno – rappresenta lo strumento attraverso cui l'adeguatezza di quei controlli viene costantemente verificata e garantita. L'*Internal Audit*, in particolare, svolge un ruolo insostituibile di sentinella interna: attraverso la valutazione indipendente dei processi e dei presidi di controllo, esso può anticipare le mosse dei potenziali frodatori, individuare le falle prima che siano sfruttate, e promuovere interventi correttivi tempestivi.
Dall'altro lato, la *revisione esterna dei bilanci* fornisce un *controllo aggiuntivo ex post*, assicurando agli investitori che i conti non presentino falsificazioni rilevanti e segnalando all'azienda stessi punti di debolezza su cui intervenire. Nessun sistema è infallibile, e la storia insegna che frodi su larga scala possono verificarsi anche in presenza di controlli formali, specie in caso di collusioni ai livelli apicali. Tuttavia, la *probabilità di prevenire o scoprire le frodi aumenta esponenzialmente quando esiste un forte allineamento tra controlli interni ben congegnati, una funzione di internal auditing autonoma e competente, e una rigorosa attività di revisione contabile indipendente*.
In un'era di crescente complessità e innovazione (si pensi alle sfide poste dalla digitalizzazione, dai *big data*, dall'intelligenza artificiale applicata anche alle frodi), l'azienda deve continuare ad evolvere i propri strumenti di controllo e le proprie pratiche di *audit.* L'adozione di approcci integrati, come quelli propugnati dal CoSO 2017, e l'investimento in tecnologie di *data analytics* e intelligenza artificiale per il monitoraggio, sono esempi di come si possa potenziare ulteriormente la capacità di vigilare sui fenomeni fraudolenti.
Resta, comunque, *centrale il fattore umano*: etica, competenza e professionalità di chi progetta i controlli, di chi li attua e di chi li verifica sono la *vera linea di difesa contro le frodi*. In definitiva, il messaggio che emerge dalla teoria e dalle migliori prassi è chiaro: la prevenzione e il contrasto efficace delle frodi richiedono una visione olistica – in cui sistemi di controllo interno e *auditing* operino in concerto – e un impegno costante dell'organizzazione a coltivare una cultura della trasparenza e della legalità, senza abbassare la guardia di fronte ai rischi emergenti di comportamenti scorretti.

5.6. I MODELLI ORGANIZZATIVI ED IL "SISTEMA 231" NELL'AMBITO DELLA RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI

Il D.Lgs. 8 giugno 2001, n. 231 ha introdotto, per la prima volta, nel nostro ordinamento la responsabilità amministrativa degli enti per alcuni reati commessi nell'interesse o a vantaggio degli stessi. La disciplina colpisce sia le società di capitali e persone, fondazioni, consorzi ecc., sia associazioni non riconosciute (escluse le Pubbliche amministrazioni ordinarie).
Il presupposto posto a base della responsabilità dell'ente è la commissione di un reato presupposto (tra cui rientrano anche i reati societari di falsità in bilancio) da parte di un soggetto apicale o sottoposto. Tuttavia, l'ente può liberarsi da tale responsabilità laddove dimostri di aver adottato, prima del fatto, un modello organizzativo idoneo a prevenire il reato commesso.
In particolare, l'art. 6 del Decreto stabilisce che l'organo dirigente può evitare la *colpa di organizzazione* provando di aver adottato ed efficacemente attuato un modello adeguato al tipo di reati verificatisi; ciò implica anche l'istituzione di un Organismo di Vigilanza (OdV) dotato di poteri autonomi di controllo sul funzionamento del modello.
In relazione alle frodi in bilancio, è importante sottolineare che il D.Lgs. n. 231/2001 include tra i reati presupposto quelli di false comunicazioni sociali (falso in bilancio) previsti dal Codice civile (artt. 2621, 2622 ss. c.c.). Questi delitti colpiscono le condotte fraudolente dirette a falsificare i dati economico-patrimoniali dell'azienda.
In caso di condanna dell'amministratore-apicale (o di altro soggetto) per false comunicazioni, l'ente può essere chiamato a rispondere (art. 25-*ter* del Decreto) se dimostra che il reato è stato commesso nel suo interesse o vantaggio.
Proprio su questo punto la giurisprudenza richiede che il giudice accerti l'"*interesse dell'ente*": non basta la mera commissione del reato, ma occorre provare che l'ente ne abbia ricevuto un ingiusto profitto[49].
Il *Modello di Organizzazione, Gestione e Controllo (MOG*) previsto dal D.Lgs. n. 231/2001 è un insieme organico di regole, protocolli e schemi organizzativi finalizzati a prevenire i reati presupposto. Si tratta di un vero e proprio *sistema di compliance aziendale*, articolato tipicamente in una *parte generale* e in una (o più) *parti speciali*. Nella parte generale il modello definisce il codice etico, i ruoli e le responsabilità, le procedure di formazione e informazione interne, il sistema disciplinare e il processo di segnalazione di illeciti (*whistleblowing*).
Vi è inoltre l'istituzione dell'OdV – dotato di autonomia di funzione rispetto agli organi apicali – con il compito di vigilare sull'effettiva applicazione del modello. Nella parte speciale, invece, sono definiti in dettaglio i protocolli operativi per le *attività a rischio*, che descrivono i *processi sensibili potenzialmente esposti a reato*, i controlli interni ivi previsti e le modalità di intervento in caso di anomalie; affinché il modello possa

[49] Cass. pen., Sez. I, 29 ottobre 2015, n. 43689. In merito alla nozione di "interesse dell'ente" si veda, più diffusamente, Santoriello C. (2023), *Responsabilità da reato degli enti: problemi e prassi,* Milano, pagg. 30 ss.

funzionare da esimente, il Decreto richiede che sia strutturato in modo *idoneo a prevenire reati della specie di quello verificatosi*.
In concreto questo significa che il modello deve prevedere, a seconda delle dimensioni e dell'attività dell'ente, misure idonee a garantire l'osservanza delle leggi e a "*scoprire ed eliminare tempestivamente situazioni di rischio*"[50].
Ad esempio, si richiede che il *MOG contempli*:

1. **L'analisi dei rischi ("*risk* assessment")**: individuare le aree aziendali maggiormente esposte a frodi contabili (es. processi di bilancio, valutazione delle rimanenze, *revenue recognition*, operazioni con parti correlate). Tale mappatura deve focalizzarsi sui reati di bilancio e sugli eventuali meccanismi fraudolenti.
2. **Protocolli operativi**: norme e procedure finalizzate a disciplinare le transazioni critiche. Questi protocolli costituiscono il "cuore" del modello, poiché descrivono chi fa che cosa nel processo contabile, quali documenti devono essere approvati e da chi, e come gestire le informazioni finanziarie.
3. **Verifica periodica e aggiornamento**: il modello va controllato e rivisto in modo continuativo, con *audit* interni o interventi dell'OdV. Ogni volta che emergono violazioni, mutamenti organizzativi o nuovi rischi, occorre modificare il MOG.
4. **Sistema disciplinare**: l'ente deve prevedere sanzioni per chi viola le procedure interne. Ciò garantisce che il rispetto del modello non resti formale ma sia effettivamente applicato.

Adottando un modello organizzativo a norma, l'ente crea un meccanismo di controllo interno permanente. In una prospettiva multidisciplinare, esso integra la dimensione giuridica (artt. 6-7, D.Lgs. n. 231/2001) con strumenti aziendalistici di *governance* e *audit*. Infatti, un buon MOG contribuisce al rafforzamento della *governance* d'impresa e della trasparenza gestionale, e mette a sistema funzioni diverse (*management, internal audit*, revisori interni, OdV) in un *approccio di compliance coerente*.
In quest'ottica il MOG non è uno scritto fine a sé stesso, ma uno strumento attivo di prevenzione e monitoraggio: ad esempio la parte generale può includere un sistema di segnalazioni interne (*whistleblowing*) per intercettare tempestivamente anomalie contabili, mentre l'OdV assicura autonomia di verifica sulle attività sensibili (anche attraverso il controllo degli atti degli amministratori).
I modelli 231 svolgono un ruolo cruciale nella prevenzione delle frodi contabili e del falso in bilancio. In primo luogo, essi obbligano l'azienda a svolgere un'analisi anticipata dei rischi correlati al bilancio e ad attivare controlli adeguati. Ad esempio, attraverso la *mappatura dei processi di chiusura contabile e budget*, il MOG può identificare possibili punti critici (es. manipolazione delle previsioni di vendita, sopravvalutazione delle giacenze, falsificazione di operazioni straordinarie) e, quindi, prevedere *audit* mirati su tali aree.

[50] Nucci G. (2017), "*Responsabilità amministrativa delle società e degli enti: le specifiche del 'sistema 231'",* in *www.riskcompliance.it*. Sul punto, si veda più diffusamente Di Fiorino E., Santoriello C. (2021), *L'organismo di vigilanza nel sistema 231,* Pisa.

In secondo luogo, il modello istituisce *meccanismi organizzativi* (ruoli, responsabilità, autorizzazioni) che ridistribuiscono i poteri decisionali e introducono deleghe di firma, segregazione dei compiti e procedure di approvazione che limitano il potenziale di abuso. In pratica, nessun soggetto può operare unilateralmente senza supervisione (ad es. due firme autorizzative per impegni contabili rilevanti).
Inoltre, il MOG incentiva la *formazione e sensibilizzazione dei dipendenti* sul tema delle frodi. Con corsi *ad hoc* (e spesso con il codice etico aziendale) i dirigenti e il personale apicale vengono istruiti sui reati di bilancio e sulle regole aziendali, aumentando la consapevolezza dei rischi. Un'adeguata *cultura aziendale* è infatti fondamentale: un modello funzionale implica un vero *compliance* culture, in cui i vertici societari e gli organi di controllo (collegio sindacale, revisori) cooperano nell'individuare segnali di allarme.
Tali controlli interni e di *governance*, se efficaci, possono far emergere segnali deboli di frode e attivare tempestivamente contromisure. Nello specifico del bilancio, ciò significa che l'ente dimostra di aver preso tutte le cautele ragionevoli per prevenire manipolazioni contabili. Di conseguenza, in caso di indagine penale, un modello adeguato e applicato costituisce una *forte leva di difesa*: può infatti ridurre il rischio di sanzioni e persino portare all'esonero da responsabilità se il reato è stato commesso nonostante il MOG efficace.
L'efficacia del MOG 231 nel contrasto alle frodi in bilancio emerge integrando vari punti di vista. Dal *punto di vista giuridico*, il Decreto 231 definisce le *regole del gioco*: come visto, esso collega la responsabilità dell'ente alla commissione di reati finanziari e alle modalità organizzative che li consentono.
La dottrina giuridica sottolinea che il legislatore non intende punire l'ente con responsabilità oggettiva: è quindi fondamentale provare in concreto che l'ente poteva prevedere e impedire il reato attraverso il proprio sistema di controlli; perciò l'adeguatezza del modello e l'effettività dell'OdV diventano criteri decisivi in giudizio.
Dal *punto di vista organizzativo-aziendale*, il MOG è parte integrante della *corporate governance*. Gli amministratori e i manager devono collaborare per disegnare e far funzionare il modello: ad esempio, assegnando compiti precisi (ruoli di controllo interno, funzioni di *compliance*, *audit* interno) e predisponendo flussi informativi trasparenti tra i vertici e gli organismi di controllo.
L'*approccio multidisciplinare* raccomandato da Confindustria[51] enfatizza anche la connessione fra MOG, etica aziendale e *compliance* a livello *enterprise risk management*. In pratica, la prevenzione delle frodi contabili richiede che i processi amministrativi-finanziari siano disegnati con logiche antifrode (separazione di mansioni, *check* sui dati, approvazioni gerarchiche) e che tali logiche siano incorporati nelle procedure aziendali *standard*.
Infine, sotto *il profilo del controllo interno e auditing*, il Modello 231 funziona come un presidio coordinato di controlli. L'OdV, che controlla la *compliance* del modello, di fatto collabora (pur avendo compiti diversi) con gli altri organi di vigilanza: collegio

[51] Confindustria (2021); *Le nuove linee guida 231 di Confindustria per la costruzione dei modelli di organizzazione, gestione e controllo*, www.confindustria.it/documenti.

sindacale, revisori legali, *internal audit*. Ad esempio, un *auditor interno* periodicamente verifica la coerenza delle scritture contabili e riferisce i risultati anche all'OdV per integrare le informazioni di controllo.
Analogamente, i bilanci e le relazioni contabili sono sottoposti a revisione contabile esterna che incrocia le procedure interne. In questo modo si crea un sistema di *control audit a più livelli*: se emergono incongruenze, anche attraverso segnalazioni di dipendenti (*whistleblowing*), l'OdV può avviare approfondimenti. La combinazione di regole giuridiche, pratiche gestionali e controlli tecnici rende il Sistema 231 un vero *sistema di prevenzione* delle frodi in bilancio.
In sintesi, i modelli di organizzazione ai sensi del D.Lgs. n. 231/2001 rappresentano *strumenti strutturati di compliance e controllo* che – se ben progettati e applicati – consentono di ridurre significativamente il rischio di illeciti contabili. Integrando aspetti legali, organizzativi e di *internal audit*, essi alimentano un circolo virtuoso: la cultura del rispetto delle norme e l'efficienza dei controlli prevengono abusi nei bilanci, mentre la loro esistenza e funzionalità costituiscono un elemento chiave nelle decisioni giudiziarie in materia di responsabilità dell'ente.

5.6.1. La valutazione giudiziaria del MOG e casi pratici esemplari

Quando si parla di *valutazione giudiziale* del MOG, evidentemente, si fa riferimento all'adeguatezza ed idoneità a prevenire i reati presupposto. Tuttavia, la dottrina di recente[52], ad oltre vent'anni di applicazione della norma, ha precisato che l'impianto presenta dei punti di crisi riconducibili ad:

- assenza nel corpo normativo di criteri e parametri definiti ed oggettivi;
- costi di implementazione, funzionamento del "Sistema 231";
- incertezza in merito all'obbligatorietà del MOG.

I suddetti elementi producono effetti: *(i)* nella direzione dell'ente che si deve dotare del MOG; *(ii)* nella direzione dell'autorità giudiziaria che deve valutare adeguatezza ed idoneità.
Quanto sopra, proprio in ragione del fatto che la normativa sulla 231 non individua uno *standard* organizzativo assoluto che funzioni da elemento di garanzia sull'agire dell'ente, inteso come assetto di *compliance* da far obbligatoriamente proprio per mettersi al riparo in caso di commissione del reato presupposto (*benchmark*). Tale carenza trascina con sé *due tipologie di insidie*:

1. Il ricorso ad *ampia discrezionalità* da parte del singolo magistrato nella valutazione di adeguatezza del MOG.
2. L'obiettivo perseguito dalla legge che rappresenta l'esito cui deve mirare l'ente non è l'eliminazione del rischio della commissione di illeciti, bensì la *riduzione del rischio* che venga commesso un illecito nell'attività d'impresa.

Intanto, proprio a definire una cornice di intervento che tende ad arginare le suddette problematiche, bisogna chiaramente affermare che non è affatto corretta l'equazione

[52] Per una disamina più ampia si veda: Santoriello C. (2023), *Responsabilità da reato degli enti: problemi e prassi,* Milano, pag. 475.

dell'inidoneità del MOG a fronte di ogni evento che fa emergere la commissione di un reato. Insomma, è errato – nella valutazione giudiziale del modello – perseguire la formula (retorica) del *rischio zero*.
Secondo la dottrina aziendalistica[53],il livello di adeguatezza delle misure nei sistemi di controllo dei rischi fa riferimento al rapporto costi/benefici; il punto di pareggio tra il costo e il beneficio, in termini aziendali, definisce il livello di rischio accettabile in quanto un'ulteriore protezione dal rischio non risulterebbe economicamente vantaggiosa. Questo concetto è stato ripreso e sistematizzato in continuità con i principi definiti dal *framework CoSO – Committee of Sponsoring Organizations of the Treadway Commission*, secondo il quale: "*Il controllo interno non può garantire l'eliminazione totale del rischio, ma può fornire una ragionevole sicurezza, commisurata al rapporto costi/benefici delle misure di controllo attivate*".
In generale, la normativa stabilisce che il reato non può essere imputato se, unitamente ad altre condizioni, esiste un sistema di prevenzione tale da non poter essere aggirato, se non fraudolentemente. Con la stessa logica si fissa anche il livello di *rischio accettabile.*
Pertanto, ai fini della valutazione giudiziale del momento, occorrerà – dapprima – in concreto ed in una prospettiva *ex ante*, verificare la completezza del MOG in relazione al processo di *risk assessment*. Vale a dire, se l'ente è stato in grado di determinare correttamente quale fosse il livello di rischio da fronteggiare, individuando la tipologia di reato presupposto.
Successivamente, si dovrà procedere analizzando la prescrizione organizzativa in relazione all'area di attività la cui inosservanza ha portato al verificarsi del reato presupposto.
Al terzo *step*, è necessario verificare la concreta possibilità per l'ente di integrare il contenuto dell'assetto organizzativo con le cautele ritenute mancanti e reputate necessarie poste in diretta relazione con l'illecito. In questa fase, occorrerà prestare molta attenzione al fatto che le ulteriori misure organizzative fossero effettivamente esigibili dai vertici dell'azienda in quanto compatibili con la struttura imprenditoriale.
Definiti i criteri della valutazione giudiziaria del MOG, si espongono – sinteticamente – alcuni **casi pratici esemplari**.

- **Tribunale di Milano 22 aprile 2024, n. 1070 (Caso "BT Italia")**. In questo recente processo il Tribunale meneghino si è pronunciato sul reato di false comunicazioni sociali consumato nell'ambito di operazioni bancarie complesse. L'analisi della sentenza mostra come il giudice abbia valutato in concreto l'efficacia del modello organizzativo dell'ente. In particolare, la società imputata aveva adottato un MOG nel 2006 e lo aveva aggiornato nel 2016. Gli esperti avevano contestato la versione vigente del 2011, priva di parte speciale dettagliata. Tuttavia, i giudici hanno concluso che il modello adottato (aggiornato poi nel 2016) era *efficacemente strutturato*. Nel corso del procedimento emerse che il modello 2016 conteneva protocolli di prevenzione per i settori sensibili (canali di circolazione di de-

[53] Cattaneo M. (2003), *Controlli interni e responsabilità sociale dell'impresa*, in "Controllo di gestione e responsabilità"; anche Migliaccio G. (2011), *Controllo interno e responsabilità penale dell'ente*, Torino.

naro, comunicati stampa ecc.) già predisposti nel 2013 e poi richiamati nel documento 2016.

In parole semplici, il Tribunale ha ritenuto che il MOG prevedesse adeguate misure di *risk assessment* e controlli interni sulle attività a rischio fraudolento, compresi i flussi finanziari. Di conseguenza è stata esclusa la responsabilità penale dell'ente ai sensi dell'art. 6 D.Lgs. n. 231/2001. Come sintetizza la *press review*, "*con la sentenza n. 1070/2024 il Tribunale di Milano ha escluso la responsabilità della società riconoscendo l'idoneità del modello organizzativo adottato*".

Tale pronuncia riafferma un principio consolidato: la sola commissione del reato non comporta automaticamente colpa di organizzazione dell'ente se il modello era ben progettato e applicato.

- **Cassazione, Sez. pen. I, 10 dicembre 2015, n. 43689 (Caso "A.S. Roma S.p.A.")**. In questo famoso caso di falso in bilancio nel settore calcistico la Corte ha precisato il principio dell'"interesse o vantaggio" dell'ente. I fatti riguardavano operazioni di trasferimento di calciatori sovrapprezzati con l'obiettivo di manipolare il bilancio della società sportiva. La Cassazione, investita del ricorso, ha annullato la pronuncia di merito e stabilito che la responsabilità dell'ente sussiste solo se è provato che il falso abbia prodotto un vantaggio economico effettivo per la società. In pratica, "non è sufficiente che la fattispecie delittuosa sia stata realizzata da un soggetto apicale nell'ambito dell'ente per ritenere quest'ultimo automaticamente responsabile".

  Questo caso illustra indirettamente il ruolo del MOG: se l'ente dimostra che le manipolazioni erano dirette esclusivamente all'interesse personale dell'amministratore e non hanno inciso sulla gestione dell'azienda, la colpa di organizzazione non può essere affermata. Un modello organizzativo adeguato dovrebbe infatti impedire tali scelte unilaterali nei bilanci societari.
- **Cassazione, Sez. pen. VI, 15 giugno 2022, n. 23401 (Caso "Impregilo")**. Pur non trattandosi di frodi di bilancio, questa pronuncia delle Sezioni Unite è rilevante per i Modelli 231. La Corte ha confermato che per escludere la responsabilità dell'ente non basta che il MOG esista, ma occorre valutarne la concretezza ed efficacia in relazione al fatto di reato. Nel caso Impregilo (aggiotaggio e manipolazione di comunicati stampa) il modello prevedeva, ad es., la doppia firma su comunicati finanziari e autorità multiple per ogni attività a rischio. I giudici hanno ritenuto "adeguate a prevenire i reati di comunicazione" le prescrizioni aziendali e hanno quindi dichiarato idoneo il modello adottato. Come sottolinea il commento, ciò conferma che la clausola esimente del 231 trova applicazione solo se il modello è applicato virtuosamente e dimostra concretamente di aver limitato il rischio di reato.

Questi esempi evidenziano come il *Sistema 231* si intrecci con casi reali di frode contabile: un modello organizzativo solido e attuato non solo rafforza la prevenzione delle frodi, ma, in caso di indagine, costituisce il fondamento per l'esonero dell'ente. Al

contrario, l'assenza di un tale modello – o la sua elusione fraudolenta – rende l'ente più vulnerabile a sanzioni.
Di seguito, una tabella riassuntiva dei principali profili di censura emergenti in sede giudiziale relativamente ai Modelli di Organizzazione, Gestione e Controllo (MOG) *ex* D.Lgs. n. 231/2001, corredati da riferimenti giurisprudenziali significativi:

Tavola 5.3. – **Sintesi principali profili di censura MOG**

Profilo di censura	Descrizione del rilievo	Riferimenti giurisprudenziali/ dottrina
Scollamento tra modello teorico e prassi aziendale	Il MOG risulta formalmente ben strutturato, ma privo di reale impatto operativo: non è integrato nei processi aziendali quotidiani	Trib. Milano, sent. 22 aprile 2024, n. 1070: richiede che il modello sia "il supporto materiale del dovere organizzativo".
Mancato aggiornamento del MOG e dei Protocolli Speciali	Il modello non evolve con le modifiche organizzative, normative o di *business*; i protocolli restano obsoleti o censurabili.	Cass. n. 38025/2022: la mera nomina dell'OdV non basta, serve che il modello sia reso "operativo" e aggiornato.
Inadeguatezza della matrice dei rischi	La *risk assessment* è generica o non aggiornata, mancanti correlazioni con presidi e protocolli concreti.	Trib. Milano n. 1070/2024: richiede protocolli specifici, dinamici e proporzionati al rischio.
Assenza di flussi informativi tra azienda, OdV e organi di controllo	Mancano *report* periodici strutturati e documentati fra OdV, vertici aziendali e organi di controllo, vanificando le funzioni preventive.	Cass., Sez. VI, 7 ottobre 2022, n. 38025: il modello necessita di un "efficiente sistema di flussi informativi".
OdV inefficace o inattivo	L'Organismo di Vigilanza, pur formalmente costituito, non esercita controlli né riunioni sistematiche.	Trib. Milano, II Sez. pen., 7 apr. 2021: l'OdV "omette i dovuti accertamenti" e pochi incontri su 30 sedute previste.

5.7. LE FIGURE DI CONTRASTO AL MECCANISMO DELLE FRODI

A questo punto, dopo aver analizzato il profilo oggettivo degli strumenti di prevenzione, è utile procedere ad una disamina dei soggetti cui può essere attribuita una specifica funzione di contrasto alle frodi.

5.7.1. Il fraud manager ed il fraud auditor

Il *fraud manager* aziendale – ossia il responsabile interno della prevenzione e gestione delle frodi – riveste un ruolo chiave nel sistema di controllo interno delle società. Questa figura, sebbene non sempre espressamente prevista da disposizioni normative, si

occupa di progettare e attuare misure organizzative volte a prevenire, rilevare e contrastare frodi di natura contabile e operativa all'interno dell'impresa.
In concreto, il *fraud manager* conduce periodiche valutazioni del rischio di frode, elabora procedure e controlli preventivi (ad esempio separazione delle funzioni, verifiche sui dati di bilancio, monitoraggio di transazioni anomale) e promuove una cultura aziendale improntata all'etica e alla tolleranza zero verso gli illeciti. Rientrano tra le sue funzioni anche la formazione dei dipendenti sui temi dell'integrità finanziaria e l'implementazione di canali di *whistleblowing* interni per le segnalazioni riservate di illeciti, nonché la conduzione di indagini interne in caso di sospette irregolarità. In tal modo, il *fraud* manager opera da presidio specializzato a supporto degli organi societari, collaborando strettamente con la funzione di internal *audit*, con il collegio sindacale o comitato di *audit* e con il vertice amministrativo (es. Direttore Finanziario), al fine di assicurare la correttezza delle scritture contabili e la conformità alle normative antifrode applicabili.
Dal punto di vista normativo, l'ordinamento italiano non impone la nomina di un *fraud manager* in senso stretto, ma predispone vari strumenti che ne implicano le funzioni. Un riferimento cruciale è il D.Lgs. 8 giugno 2001, n. 231, che ha introdotto la responsabilità "amministrativa" delle società per reati commessi nel proprio interesse: tale Decreto incentiva le imprese a dotarsi di modelli organizzativi idonei a prevenire i reati societari, tra cui rientrano oggi anche le falsità di bilancio.
In effetti, a partire dagli scandali finanziari dei primi anni 2000 (su tutti il caso Parmalat), il legislatore ha rafforzato la tutela penale del bilancio: la Legge 27 maggio 2015, n. 69 ha inasprito le pene per il reato di false comunicazioni sociali (falso in bilancio) e lo ha incluso tra i reati presupposto del D.Lgs. n. 231/2001, così che una frode contabile rilevante espone l'ente a sanzioni se non ha adottato adeguati protocolli preventivi.
In questo contesto, la presenza di un efficace sistema di *fraud management* interno diviene essenziale anche per esonerare o attenuare la responsabilità della società. Le aziende italiane, specie quelle di maggiori dimensioni, hanno dunque sviluppato programmi di *compliance* secondo il Modello 231, che includono una mappatura dei rischi di frode e corruzione, l'adozione di *policy* e procedure interne, la formazione del personale e la predisposizione di sistemi di segnalazione e monitoraggio continuo.
In parallelo, per le società quotate in Borsa, la Legge n. 262/2005 (c.d. "*Legge sul risparmio*") ha introdotto la figura del dirigente preposto alla redazione dei documenti contabili societari (art. 154-*bis* TUF), un dirigente aziendale obbligatorio cui sono attribuite per legge funzioni di supervisione sulla corretta tenuta della contabilità e sulla adeguatezza dei controlli interni finanziari. Tale figura – spesso coincidente con il CFO o altra risorsa dirigenziale apicale – deve rilasciare insieme agli amministratori dichiarazioni formali sull'attendibilità del bilancio, assumendo anche responsabilità personale in caso di omissioni o negligenze.

Ulteriori presidi normativi settoriali rafforzano la prevenzione delle frodi: si pensi, ad esempio, al settore bancario e finanziario, dove le disposizioni di Vigilanza di Banca d'Italia richiedono sistemi di controllo interno particolarmente rigorosi, oppure al settore pubblico, ove il *Responsabile per la prevenzione della corruzione e della trasparenza* (RPCT) ha compiti analoghi in chiave di antifrode e anticorruzione nell'ente.
Anche il Codice civile richiama implicitamente doveri di prevenzione: gli amministratori hanno obblighi di diligente organizzazione e controllo sull'andamento gestionale (artt. 2381, 2392 c.c.), la cui violazione può comportare responsabilità civili verso la società, ad esempio qualora omettano di approntare adeguati controlli scongiurando frodi pregiudizievoli per il patrimonio sociale.
In ambito europeo UE, manca una disciplina specifica sul "*fraud manager*" aziendale, ma negli ultimi anni l'Unione ha emanato norme volte a potenziare i meccanismi di prevenzione e scoperta delle frodi all'interno delle organizzazioni. Un provvedimento di particolare rilievo è la Direttiva UE n. 2019/1937 in materia di *whistleblowing*, che impone agli Stati membri di introdurre obblighi per le imprese medio-grandi di attivare canali interni di segnalazione degli illeciti e misure di tutela dei segnalanti. Tale Direttiva – attuata in Italia con il D.Lgs. n. 24/2023 – mira a favorire l'emersione tempestiva di frodi e irregolarità attraverso le denunce interne, ponendo in capo alle società la responsabilità di gestire con riservatezza ed efficacia le segnalazioni ricevute.
Sul versante della regolazione contabile, l'UE già dal 2006 ha armonizzato gli obblighi di controllo contabile con la Direttiva n. 2006/43/CE (oggi sostituita dalla Direttiva n. 2014/56/UE e dal Regolamento UE n. 537/2014), imponendo alle società di interesse pubblico di istituire comitati per il controllo interno e la revisione, incaricati di monitorare il processo contabile e l'efficacia dei controlli interni. Inoltre, il quadro normativo europeo prevede reazioni coordinate alle frodi che ledono interessi finanziari sovranazionali: la Direttiva UE n. 2017/1371 (c.d. *Direttiva PIF – Protection of Financial Interests*) ha introdotto una definizione comune dei reati di frode in ambito UE e sanzioni minime, richiedendo agli Stati membri di criminalizzare condotte come il falso in bilancio quando incidano sugli interessi finanziari dell'Unione.
In attuazione di tale Direttiva è stata istituita la Procura Europea (EPPO), autorità sovranazionale competente a indagare e perseguire frodi e altri reati finanziari gravi che coinvolgano il bilancio dell'UE.
Questi sviluppi mostrano un rafforzamento dell'approccio preventivo-repressivo a livello europeo, sebbene focalizzato soprattutto sulla tutela degli interessi finanziari pubblici: essi indirettamente sollecitano anche le imprese a dotarsi di efficaci programmi di *fraud compliance*, sapendo che le violazioni rilevanti (ad es. frodi IVA transfrontaliere, malversazioni di fondi UE, falsi bilanci per ottenere sovvenzioni) saranno oggetto di cooperazione investigativa e sanzioni uniformi nei vari Paesi membri. Passando agli ordinamenti extra-UE, si riscontrano modelli avanzati di disciplina del *fraud management*, in particolare negli Stati Uniti e nel Regno Unito, che spesso fungono da riferimento internazionale.

Negli USA, a seguito di scandali clamorosi come Enron e WorldCom che nei primi anni 2000 misero in luce diffuse manipolazioni contabili, il legislatore federale varò il Sarbanes–Oxley Act del 2002 (SOX) per rispristinare la fiducia nei mercati[54]. Tale legge ha imposto alle società quotate *standard* rigorosi di controllo interno e a*ccountability* del *management*: in particolare, la *Section* 404 del SOX richiede agli amministratori di effettuare una valutazione annuale sull'efficacia del sistema di controllo interno finanziario e di riferirne nel bilancio, in modo da garantire l'accuratezza delle informazioni finanziarie fornite agli investitori.
Contestualmente, le *Sections* 302 e 906 del SOX obbligano CEO e CFO a certificare personalmente la veridicità del bilancio e l'adeguatezza dei controlli, rendendoli penalmente responsabili in caso di false certificazioni. Queste misure normative – unitamente al potenziamento dei poteri della *Securities and Exchange Commission* (SEC) e alla creazione di un organismo di vigilanza sui revisori (il PCAOB) – hanno spinto le imprese statunitensi a investire fortemente nella *corporate compliance* e nei controlli antifrode.
Oggi presso molte società USA sono istituiti appositi *fraud risk management programs*, spesso affidati a *Chief Compliance Officers* o *Internal Auditors* con qualifiche di *Certified Fraud Examiner*, al fine di garantire un monitoraggio costante delle aree di rischio, anche attraverso sofisticati sistemi di *data analytics* e verifiche forensi.
Dal punto di vista giurisprudenziale, va segnalato che il dovere degli amministratori di attivarsi per prevenire violazioni è stato riconosciuto anche nel diritto societario statunitense: la nota sentenza *In re Caremark International Inc.* (Delaware Chancery Court, 1996) ha delineato l'obbligo di *oversight dei board of directors*, stabilendo che la mancata istituzione di un adeguato sistema informativo e di controllo interno può costituire una violazione dei doveri fiduciari degli amministratori.
Su questa scia, recenti pronunce negli USA (*ad es. Marchand v. Barnhill, Delaware Supreme Court, 2019*) hanno ulteriormente sottolineato la responsabilità dei vertici societari nel vigilare su rischi "*mission-critical*" per l'azienda, fra i quali rientra certamente il rischio di frode nei bilanci.
Nel Regno Unito, l'approccio alla prevenzione delle frodi societarie è tradizionalmente imperniato su principi di buona *governance* e *self-regulation*, ma si sta gradualmente trasformando attraverso interventi normativi specifici. Il *UK Corporate Governance Code* affida espressamente al board il compito di stabilire i valori etici dell'impresa e di promuovere la *tone at the top*, ossia un orientamento etico proveniente dai vertici che pervada la cultura aziendale.
Le società britanniche, soprattutto se quotate, sono tenute (in base al principio *comply or explain)* a valutare annualmente l'efficacia dei propri controlli interni e sistemi di gestione dei rischi, comunicandone gli esiti agli azionisti. Già con il *Bribery Act 2010*, il Regno Unito ha introdotto un modello di responsabilità oggettiva delle persone giuri-

[54] Sul punto, si veda quanto diffusamente argomentato nel paragrafo 2.1.3 "*Il Sarbanes-Oxley Act ed il rafforzamento della trasparenza e della responsabilità nelle pratiche contabili*".

diche per omissione di adeguate misure anticorruzione (*failure to prevent bribery*), prevedendo una difesa fondata sull'adozione di adeguate procedure da parte dell'azienda.
Tale impostazione viene ora estesa anche alle frodi: nel 2023 è stato approvato l'*Economic Crime and Corporate Transparency Act*, che introduce il reato di *failure to prevent fraud* applicabile alle imprese. In base a questa nuova fattispecie, a partire dal 1° settembre 2025 le grandi organizzazioni britanniche potranno essere ritenute penalmente responsabili se un proprio dipendente, *partner* o rappresentante commette una frode con l'intento di favorire l'azienda, a meno che l'ente provi di aver adottato misure di prevenzione "ragionevoli" al momento del fatto.
Esempi di condotte rilevanti includono false rappresentazioni rivolte a clienti o investitori, manovre contabili fraudolente o pratiche commerciali ingannevoli commesse a vantaggio della società.
L'obiettivo dichiarato di questa riforma è promuovere una cultura aziendale proattiva nella lotta alle frodi, analogamente a quanto avvenuto con la normativa anticorruzione del 2010, inducendo le imprese a dotarsi di solidi programmi anti-frode e a nominare figure dedicate alla verifica della conformità.
In prospettiva comparatistica, l'evoluzione britannica richiama da vicino il modello italiano del D.Lgs. n. 231/2001 (pur inserendosi nel diverso contesto del *common law*): in entrambi i sistemi la presenza di efficaci procedure organizzative interne funge da esimente o attenuante della responsabilità dell'ente, sottolineando la centralità di un *fraud management* diligente. Inoltre, sul piano dei controlli esterni, il Regno Unito dispone di un organismo specializzato, la *Serious Fraud Office* (SFO), deputato alle indagini e ai procedimenti per frodi gravi, che spesso interagisce con i *fraud officers* aziendali nell'ambito di *self-reporting* o accordi di clemenza (come i *Deferred Prosecution Agreements* applicati, ad esempio, nel caso Tesco 2017 relativo a false comunicazioni al mercato).
In sintesi, la figura del *fraud manager* aziendale, pur con differenti qualifiche e basi giuridiche nei vari ordinamenti, emerge come elemento cardine di un moderno sistema di *corporate governance* orientato alla trasparenza e alla legalità.
L'ordinamento italiano, attraverso un *mix* di obblighi legali (si pensi al dirigente preposto *ex* art. 154-*bis* TUF) e incentivi alla *compliance* (Modello 231/2001), riconosce la necessità di presidiare internamente il rischio di frode in bilancio. A livello europeo, le direttive recenti in materia di whistleblowing e tutela degli interessi finanziari comuni spingono nella medesima direzione, rafforzando gli strumenti preventivi e sanzionatori disponibili. Gli ordinamenti anglosassoni, dal canto loro, offrono esempi di approcci complementari: quello statunitense, più prescrittivo, fondato su stringenti obblighi di controllo interno e responsabilità personale del *top management*; quello britannico, storicamente *soft law*, ma ormai anch'esso orientato verso la tipizzazione di specifiche omissioni sanzionabili in capo alla persona giuridica.

Tali tendenze convergenti indicano come il *fraud management* sia divenuto parte integrante delle buone prassi aziendali a livello globale: dalle *best practice* elaborate da organismi internazionali (si vedano, ad esempio, le linee guida COSO-ACFE sul *fraud risk management*) fino agli interventi legislativi nazionali, si afferma l'idea che le società debbano dotarsi di strutture e processi atti a prevenire e scoprire tempestivamente le frodi.

Il fraud manager – quale "*sentinella*" interna della legalità finanziaria – incarna questa esigenza, contribuendo a proteggere l'integrità dei bilanci e la fiducia degli *stakeholder*, in linea con i principi di correttezza gestionale e trasparenza informativa condivisi nei principali sistemi giuridici internazionali.

Il *fraud auditor* è un professionista, esterno all'azienda, specializzato *nell'identificazione, prevenzione e analisi delle frodi finanziarie all'interno di un'organizzazione*. La sua attività si concentra sull'esaminare i processi contabili e operativi per individuare segnali di frode o irregolarità e prevenire il verificarsi di comportamenti illeciti.

- *Cosa fa un Fraud Auditor?*
    1. **Analisi preventiva**: Valuta i rischi di frode nei processi aziendali e implementa controlli interni per mitigarli. Rivede procedure aziendali, politiche interne e sistemi di controllo per garantirne l'efficacia.
    2. **Controlli mirati**: Conduce verifiche specifiche su transazioni, registri finanziari, e altri documenti aziendali per individuare segnali di frode. Monitora attività sospette o non conformi alle politiche aziendali.
    3. **Identificazione delle frodi**: Riconosce schemi fraudolenti, come false fatturazioni, appropriazioni indebite o manipolazioni contabili. Usa tecniche analitiche avanzate, come l'analisi dei dati e dei flussi di cassa, per identificare anomalie.
    4. **Consulenza e formazione**: Aiuta l'azienda a sviluppare programmi di formazione per sensibilizzare i dipendenti sui rischi di frode. Fornisce suggerimenti per migliorare i controlli interni e ridurre la vulnerabilità a comportamenti fraudolenti.
    5. **Supporto investigativo**: In caso di sospette frodi, collabora con l'azienda o con autorità esterne per raccogliere prove e assistere nelle indagini.

Nella Tavola 5.4. che segue si anticipano le principali differenze che distinguono i ruoli del *fraud auditor* e del *forensic accountant*:

Tavola 5.4. – **Le differenze dei ruoli di *fraud auditor* e del *forensic accountant***

5.7.2. Il *whistleblower*

Nell'attuale architettura dei sistemi di prevenzione delle frodi aziendali, la figura del *whistleblower* si è progressivamente imposta come uno degli strumenti più efficaci non solo per l'emersione degli illeciti, ma anche per il consolidamento di una cultura organizzativa orientata alla legalità, alla trasparenza e alla responsabilità sociale d'impresa. In particolare, nel contesto normativo italiano, il ruolo del *whistleblower* acquista rilievo strategico nella cornice del D.Lgs. 8 giugno 2001, n. 231, che disciplina la responsabilità amministrativa degli enti per reati commessi nel loro interesse o a loro vantaggio da soggetti apicali o sottoposti alla direzione e vigilanza degli stessi.
Il D.Lgs. n. 231/2001, infatti, prevede che gli enti possano essere esonerati dalla responsabilità se dimostrano di aver adottato ed efficacemente attuato modelli di organizzazione, gestione e controllo (Modelli 231) idonei a prevenire i reati indicati dal Decreto (art. 6). All'interno di tali modelli, la previsione di idonei canali di segnalazione e la protezione del segnalante costituiscono elementi imprescindibili per garantire l'effetti-

vità del sistema di *compliance*. In tal senso, l'istituto del *whistleblowing* si integra funzionalmente nel *sistema 231* come meccanismo di *early detection* e *internal audit*, capace di segnalare in tempo reale anomalie e condotte potenzialmente illecite, prima che si traducano in reati rilevanti ai fini della responsabilità dell'ente[55].

Di particolare rilevanza, nell'ambito del D.Lgs. n. 231/2001, è la categoria dei reati societari – tra cui si annoverano le false comunicazioni sociali, l'ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza, l'aggiotaggio, l'impedito controllo e la corruzione tra privati – i quali rappresentano, secondo l'art. 25-*ter* del Decreto, reati-presupposto della responsabilità dell'ente.

Le frodi in bilancio, in particolare, rientrano tipicamente nella fattispecie di false comunicazioni sociali (artt. 2621 e 2622 c.c.), e la loro individuazione precoce è spesso possibile solo grazie all'intervento di figure interne che, in virtù della loro posizione, sono in grado di percepire irregolarità prima che queste si riflettano nei documenti contabili ufficiali[56]. È in tale contesto che il *whistleblower* agisce come un attore cardine del sistema di prevenzione e controllo.

La Direttiva UE n. 2019/1937, recepita in Italia dal D.Lgs. 10 marzo 2023, n. 24, ha imposto un ulteriore rafforzamento dei canali di segnalazione e delle tutele nei confronti del segnalante, estendendo significativamente l'ambito applicativo delle misure di *whistleblowing* anche al settore privato. Il Decreto del 2023 modifica sostanzialmente il quadro previgente (introdotto dalla Legge n. 179/2017), imponendo a tutti i soggetti giuridici del settore privato con almeno 50 dipendenti – nonché a tutti gli enti che adottano modelli *ex* D.Lgs. n. 231/2001 – l'istituzione di canali di segnalazione interni, la garanzia della riservatezza del segnalante e la protezione da ritorsioni, nonché l'obbligo di gestione diligente delle segnalazioni[57].

La funzione del *whistleblowing*, pertanto, non si limita alla mera trasmissione dell'informazione: essa assume una valenza proattiva nella costruzione e nel rafforzamento del *sistema 231*, contribuendo alla concreta implementazione del principio di responsabilità preventiva dell'ente. Il *whistleblower* agisce come un sensore etico e un presidio operativo, capace di segnalare disallineamenti tra condotta effettiva e condotta conforme ai protocolli interni. Inoltre, la presenza di una politica di *whistleblowing* formalizzata e promossa dalla dirigenza costituisce uno dei *compliance indicator* più significativi ai fini della valutazione di efficacia del modello organizzativo da parte del giudice, in sede di eventuale processo 231[58].

Va infine rilevato che, secondo numerosi studi empirici, le segnalazioni interne rappresentano il canale più efficace nella scoperta delle frodi aziendali, superando per incidenza persino i controlli esterni e le revisioni contabili.

---

[55] Viganò, G. (2021). *La responsabilità da reato degli enti. Modelli organizzativi e compliance 231*. Torino.

[56] Wells, J. T. (2017). *Corporate Fraud Handbook: Prevention and Detection* (5th ed.). Wiley.

[57] Di Rosa, C. (2023). *Il nuovo whistleblowing nel settore privato: effetti e implicazioni del D.Lgs. 24/2023*. Rivista di Diritto delle Imprese, 4, pagg. 85-112.

[58] Gargantini, M. (2022). *Compliance e diritto penale d'impresa: una lettura sistemica del modello 231*. Diritto Penale Contemporaneo.

L'*Association of Certified Fraud Examiners* (ACFE)[59], offre uno dei database più ampi e affidabili a livello globale in materia di frodi aziendali, analizzando oltre 2.100 casi verificatisi in 133 Paesi. Lo studio dimostra in modo inequivocabile che il *whistleblowing* rappresenta il canale più efficace per la rilevazione delle frodi, superando strumenti formali di controllo interno, *audit* esterni o notifiche da parte delle autorità regolatorie. Secondo i dati ACFE 2022, il 42% delle frodi è stato rilevato attraverso una segnalazione (*tip*), di cui più della metà proveniente da dipendenti interni all'organizzazione (circa il 55% dei tip totali). Questo dato evidenzia l'importanza di un ambiente aziendale che promuova attivamente la cultura della segnalazione e che garantisca meccanismi sicuri e riservati per il *whistleblowing*.

Tavola 5.5. – **Principali canali di rilevazione delle frodi aziendali**

Canale di rilevazione(Fonte ACFE 2022)	Percentuale
Segnalazione (Tip)	42%
Audit interno	16%
Revisione contabile esterna	4%
Controlli di gestione	12%
Altro	26%

Questo dato è ancora più rilevante se confrontato con la bassa percentuale di frodi scoperte tramite *audit* esterni (solo il 4%), sottolineando come i meccanismi di vigilanza tradizionali non siano sempre sufficienti per intercettare fenomeni di natura fraudolenta, specie quelli più sofisticati in ambito contabile e societario[60].
Le aziende dotate di programmi di *whistleblowing* efficaci e di canali anonimi di segnalazione presentano perdite medie da frode inferiori del 50% rispetto a quelle che ne sono prive. Secondo l'ACFE, infatti, le organizzazioni con canali strutturati hanno registrato una perdita mediana da frode di $100.000, contro i $200.000 delle organizzazioni prive di tali strumenti.
Queste evidenze confermano che il *whistleblowing* agisce non solo come strumento di rilevazione, ma anche come deterrente sistemico: la consapevolezza dell'esistenza di un canale attivo di segnalazione riduce l'incentivo alla commissione dell'illecito.
Un ulteriore dato significativo riguarda la preferenza per l'anonimato: oltre il 56% dei segnalanti ha scelto di rimanere anonimo. Questo sottolinea l'importanza di garantire non solo canali facilmente accessibili, ma anche solidi meccanismi di tutela della riservatezza e protezione dalle ritorsioni[61]. Le aziende che hanno integrato nei propri sistemi di *whistleblowing* elementi di protezione giuridica e procedurale del segnalante hanno visto un tasso di segnalazione significativamente più alto.

[59] ACFE (2022), "*Report to the Nations on Occupational Fraud and Abuse*", cit.
[60] Wells, J. T. (2017). *Corporate Fraud Handbook: Prevention and Detection*, cit.
[61] Miceli, M. P., Near, J. P., & Dworkin, T. M. (2008). *Whistle-blowing in Organizations. Routledge*.

Il dato è confermato anche nell'ambito italiano, dove l'adozione di strumenti di *whistleblowing* strutturati è correlata a una minore incidenza di reati societari e a una più alta propensione alla *self-disclosure* da parte delle imprese coinvolte[62].
Nel contesto italiano, l'integrazione dei dati empirici ACFE con la logica del D.Lgs. n. 231/2001 rafforza ulteriormente l'urgenza di istituzionalizzare il *whistleblowing* come componente strutturale del modello organizzativo. Le aziende che adottano canali di segnalazione efficaci non solo riducono il rischio di sanzioni derivanti da reati-presupposto (come le false comunicazioni sociali), ma dimostrano anche un'effettiva adesione a *standard* di *governance* virtuosa.

5.7.3. La funzione dell'Organismo di Vigilanza nella prevenzione delle frodi aziendali e di bilancio

L'Organismo di Vigilanza (OdV), introdotto dal D.Lgs. n. 231/2001, rappresenta uno snodo essenziale nel sistema di controllo interno dell'impresa, con specifico riguardo alla prevenzione delle frodi aziendali, comprese quelle di bilancio. La sua istituzione e il corretto funzionamento sono condizioni imprescindibili per l'efficacia del modello organizzativo adottato dagli enti e per l'eventuale esonero da responsabilità in caso di commissione di reati presupposto.
Secondo la normativa, l'OdV è l'organismo autonomo e indipendente cui è affidato il compito di vigilare sul funzionamento, sull'osservanza e sull'aggiornamento del modello di organizzazione, gestione e controllo (art. 6, D.Lgs. n. 231/2001). Sebbene la legge delinei in termini generali le attribuzioni dell'OdV, la prassi e la dottrina ne hanno ampliato e precisato i contenuti.
L'OdV assume una funzione di controllo sistemico, che non si limita alla verifica formale dell'applicazione delle misure previste nel modello, ma si estende alla valutazione sostanziale della loro efficacia preventiva, al fine di evitare condotte illecite, incluse le frodi contabili.
In questa prospettiva, l'OdV deve assicurare:

- *la coerenza tra il modello e i comportamenti organizzativi effettivamente adottati;*
- *l'adeguatezza delle misure previste in rapporto ai rischi-reato;*
- *la continuità della vigilanza e la capacità del modello di adattarsi a mutamenti normativi, organizzativi e di business.*

L'OdV gioca un ruolo chiave nella prevenzione delle frodi in bilancio, operando in sinergia con le altre funzioni di controllo (*Internal Audit, Compliance, Risk Management*) e con gli organi societari. In particolare, l'attività di vigilanza sulle aree a rischio, tra cui quelle contabili e finanziarie, consente all'OdV di individuare tempestivamente eventuali anomalie o segnali di allarme che potrebbero preludere a fenomeni fraudolenti.

[62] Brunetto, D. (2020). Whistleblowing e prevenzione dei reati societari: un'analisi empirica sulle aziende italiane. *Economia & Management*, 6, pagg. 95-109.

L'efficacia dell'azione antifrode dell'OdV dipende anche dalla strutturazione dei flussi informativi ricevuti, i quali devono essere tempestivi, completi e affidabili e devono includere:

- *report* periodici delle funzioni operative e di controllo sulle attività svolte;
- informazioni su criticità rilevate nei processi contabili e di *reporting*;
- segnalazioni *ad hoc* (*whistleblowing*) su comportamenti anomali o sospetti.

Attraverso questi canali, l'OdV esercita un controllo proattivo, contribuendo a creare un ambiente di controllo interno solido e orientato alla trasparenza e alla legalità.
La sentenza Impregilo della Corte di cassazione[63] ha rappresentato un punto di svolta interpretativo, valorizzando il concetto di "colpa di organizzazione" come specifica forma di colpa riferita all'ente, configurata dalla violazione di una regola cautelare auto-normata e idonea, se rispettata, a prevenire il reato. In tale cornice, l'OdV assume una funzione centrale nel garantire che il modello sia non solo formalmente adottato, ma anche concretamente attuato ed efficace.
Il giudice, ai fini dell'esonero dell'ente da responsabilità, dovrà valutare:

- se il modello contenesse regole cautelari idonee;
- se l'OdV abbia esercitato una vigilanza effettiva e non solo formale;
- se l'eventuale reato sia avvenuto eludendo fraudolentemente il modello e le attività dell'OdV.

Laddove si riscontri un'"omessa o insufficiente vigilanza", l'efficacia preventiva del modello viene meno, e l'ente può essere ritenuto responsabile.
L'OdV si configura dunque come una funzione di controllo specialistico e indipendente, cruciale nella prevenzione delle frodi aziendali. Attraverso un'attività sistematica di verifica, monitoraggio e aggiornamento, l'OdV contribuisce a garantire l'effettività del modello organizzativo, nonché la conformità dell'operato aziendale agli *standard* etici e normativi. La sua efficacia, tuttavia, dipende dalla reale autonomia, dalla disponibilità di risorse, dalla qualità dei flussi informativi e dalla cultura della legalità diffusa nell'ente.
In un contesto in cui il rischio di frodi in bilancio può derivare da condotte complesse e difficilmente individuabili, l'azione dell'OdV rappresenta uno dei principali presìdi di tutela per la trasparenza dell'informazione finanziaria e per l'affidabilità del sistema impresa.

5.7.4. Il ruolo del revisore e dell'organo di controllo

Il nostro ordinamento contempla una duplice linea di difesa contro le condotte fraudolente rappresentata da organi / soggetti che – a pieno titolo – si interfacciano con l'organo di governo societario e con la struttura aziendale: da un lato il revisore legale dei conti, soggetto indipendente incaricato della revisione del bilancio, e dall'altro l'organo di controllo interno (collegio sindacale o sindaco unico) deputato alla vigilanza sulla gestione sociale.

[63] Cass. pen., Sez. VI, 15 giugno 2022, n. 23401.

Entrambi rivestono un ruolo cruciale nella prevenzione e individuazione delle irregolarità contabili, pur operando con funzioni e prospettive differenti; non fosse altro che, mentre il primo (revisore o società di revisione) è un soggetto esterno all'impresa, il secondo è un organo dell'impresa.

La figura del revisore legale dei conti è disciplinata principalmente dal D.Lgs. 27 gennaio 2010, n. 39 (attuativo della Direttiva n. 2006/43/CE), che ha riformato la revisione contabile introducendo principi allineati agli *standard* internazionali. Il revisore legale (che può essere una persona fisica o una società di revisione) ha il compito istituzionale di esprimere un *giudizio professionale* sull'*attendibilità* del bilancio d'esercizio (e consolidato, se previsto) attraverso lo svolgimento di una revisione legale conforme ai principi di revisione emanati a livello nazionale (ISA Italia) e alle disposizioni di legge.

Questo *incarico, di natura contrattuale*, si fonda su un rapporto di mandato professionale con la società revisionata, ma assume al contempo rilevanza pubblicistica in quanto la relazione di revisione è destinata ai soci e ai terzi per valutare la fedeltà del bilancio. Il revisore deve pianificare ed eseguire le procedure di *audit* con professionalità e *scetticismo professionale*, riconoscendo sin dall'inizio "*la possibilità che si verifichi un errore significativo attribuibile a fatti o comportamenti irregolari, compresi frodi o error*i" (art. 9, comma 2, D.Lgs. n. 39/2010).

I Principi ISA richiedono infatti un approccio dubbioso e una costante allerta verso segnali di potenziali inesattezze dovute a illeciti; ciò implica verifiche critiche della documentazione contabile e valutazioni indipendenti delle stime aziendali, così da non accettare passivamente le rappresentazioni fornite dalla direzione.

Il Principio di revisione internazionale ISA 240 (*The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements*), recepito in Italia nella versione *ISA Italia 240*, costituisce la base normativa di riferimento in tema di responsabilità del revisore nella rilevazione delle frodi nell'ambito dell'attività di *audit*. Esso si fonda sul riconoscimento di un *principio cardine*: la revisione contabile, pur non essendo una procedura di investigazione forense, deve essere pianificata e condotta in modo tale da *garantire una ragionevole sicurezza* sul fatto che il bilancio non contenga errori significativi dovuti a frode o a errore.

Il Principio ISA 240 introduce una distinzione fondamentale tra *errore* e *frode*. L'errore è definito come una rappresentazione finanziaria inesatta non intenzionale, dovuta, ad esempio, a una svista, a una errata interpretazione dei dati, o a un'applicazione sbagliata dei principi contabili. La frode, invece, presuppone un elemento di intenzionalità, configurandosi come un atto doloso compiuto da uno o più componenti della direzione, della *governance* o da terzi.

La rilevanza di questa distinzione è duplice: sul piano operativo, poiché implica approcci di verifica diversi; e sul piano giuridico, poiché il dolo può generare profili di responsabilità ulteriori, anche penali, sia in capo agli autori della frode, sia in capo al revisore qualora si dimostri connivenza, tolleranza consapevole o grave negligenza.

Il principio individua specifici *obblighi professionali* in capo al revisore, articolati nelle *seguenti fasi*:

1. PIANIFICAZIONE DEL LAVORO E VALUTAZIONE PRELIMINARE DEL RISCHIO DI FRODE: il revisore è tenuto a discutere con i membri del team di revisione le modalità attraverso cui la direzione o altri soggetti potrebbero perpetrare frodi. Devono essere identificati e valutati i *fraud risk factors* quali:
   - incentivi/pressioni (es. obiettivi di bilancio aggressivi);
   - opportunità (es. debolezze nei controlli interni);
   - atteggiamenti/razionalizzazioni (es. cultura aziendale tollerante verso pratiche scorrette).
2. VALUTAZIONE DEL CONTROLLO INTERNO E DEI PRESIDI ANTIFRODE: il revisore deve valutare se il sistema di controllo interno della società sia adeguato a prevenire e rilevare frodi. Particolare attenzione va posta ai processi di approvazione delle scritture, alla segregazione delle funzioni, alla gestione delle operazioni straordinarie e ai rapporti con parti correlate.
3. IMPLEMENTAZIONE DI PROCEDURE DI AUDIT MIRATE: quando emergano aree a rischio, il revisore è tenuto a:
   - progettare procedure di revisione più estese e specifiche (es. test a sorpresa, analisi retrospettiva delle stime contabili);
   - ottenere conferme esterne (banche, clienti, fornitori);
   - effettuare interviste strutturate al *management* e al personale operativo.
4. RICHIESTA DI DICHIARAZIONI SCRITTE ALLA DIREZIONE: il revisore deve richiedere dichiarazioni formali circa:
   - l'assenza di conoscenza di frodi;
   - l'integrità del bilancio;
   - l'attendibilità delle informazioni fornite. Laddove tali dichiarazioni siano omesse o ritenute inattendibili, il revisore deve considerare l'impossibilità di esprimere un giudizio.
5. VALUTAZIONE DELLE RISPOSTE DELL'IMPRESA AI RISCHI IDENTIFICATI: se la direzione non adotta misure adeguate per contenere i rischi di frode, il revisore deve considerare l'impatto sul proprio giudizio professionale e sulla relazione di revisione.
6. DOCUMENTAZIONE DELLE PROCEDURE SVOLTE E DELLE CONCLUSIONI: l'ISA 240 impone che tutte le valutazioni relative ai rischi di frode, alle procedure adottate e ai risultati ottenuti siano documentate in maniera completa e coerente nel fascicolo di revisione.

Il revisore ha un *obbligo* preciso *di comunicazione* degli indizi o sospetti di frode:
- *Ai livelli superiori della direzione o*, se coinvolti, direttamente *all'organo di controllo* (collegio sindacale);
- *Alle autorità competenti*, nei casi previsti dalla legge (es. società quotate, enti vigilati).

Il principio prevede che la *relazione di revisione* venga modificata ove:
- la frode accertata abbia effetto materiale sul bilancio;
- la direzione non collabori nell'approfondimento degli indizi;
- il revisore ritenga che il bilancio non rappresenti in modo veritiero e corretto la situazione aziendale.

In tali casi, il revisore potrà:
a) esprimere un giudizio negativo;
b) rilasciare una dichiarazione di impossibilità ad esprimere un giudizio;

c) dimettersi dall'incarico ove ritenga compromessa l'integrità del sistema informativo aziendale.

L'ISA 240 riconosce esplicitamente che l'attività di revisione ha limiti intrinseci, e che una frode ben congegnata può risultare difficile da individuare, specie in presenza di collusioni ai vertici o sofisticate operazioni di occultamento. Tuttavia, questo non esonera il revisore dal mantenere uno *scetticismo professionale continuo*: esso deve essere l'atteggiamento mentale pervasivo che guida l'intero *audit*.

Il revisore deve diffidare delle spiegazioni non documentate, esaminare criticamente le incongruenze, e non dare per scontata la buona fede della direzione, soprattutto in presenza di indicatori di rischio.

Il principio fornisce inoltre esempi pratici di *red flags* (segnali d'allarme), tra cui:

- risultati economici eccessivamente positivi rispetto al settore;
- operazioni infragruppo opache;
- stime soggettive non supportate da analisi;
- pressioni a chiudere l'*audit* in tempi brevi.

L'assenza di segnalazioni da parte dei sistemi interni di controllo non esime il revisore dall'attivarsi: il principio chiarisce che il revisore non può fare affidamento esclusivo sulle dichiarazioni del *management*, ma deve ottenere evidenze probatorie sufficienti e appropriate attraverso test e verifiche indipendenti.

Oltre all'ambito operativo, il principio ha una valenza preventiva a livello sistemico: il rispetto rigoroso delle regole dell'ISA 240 da parte dei revisori costituisce un deterrente importante alla perpetrazione di frodi, in quanto aumenta il rischio di scoperta per i potenziali frodatori. Come osservato in dottrina, "*la qualità dell'audit dipende dalla capacità del revisore di percepire e interpretare i segnali atipici del comportamento della governance aziendale e non dalla sola osservanza formale delle procedure*"[64].

In conclusione, l'ISA Italia 240 rappresenta uno dei pilastri fondamentali per assicurare la trasparenza e l'affidabilità dell'informativa finanziaria. Il suo rispetto rigoroso costituisce non solo un adempimento tecnico, ma una garanzia di tenuta del sistema fiduciario su cui si fonda il mercato e la responsabilità sociale dell'attività di revisione.

Quanto al ruolo dell'organo di controllo, va rilevato che, nelle società di capitali di maggiori dimensioni composto da un collegio sindacale (tipicamente tre o cinque membri) o, nei casi consentiti, da un sindaco unico, esso è investito di una generale *funzione di vigilanza* sulla gestione della società.

Gli artt. 2403 e 2403-*bis* c.c. delineano i compiti di tale organo: "*Il collegio sindacale vigila sull'osservanza della legge e dello statuto, sul rispetto dei princìpi di corretta amministrazione, e in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento*".

[64] Ferraris G., "ISA 240 e il ruolo del revisore nella scoperta delle frodi", in *Rivista di Contabilità e Revisione*, n. 3/2023, pag. 215.

Tale previsione impone al collegio un ruolo attivo e dinamico nella prevenzione delle frodi, che si concreta in un controllo non meramente formale o episodico, bensì continuativo e sostanziale, in grado di cogliere *segnali di disfunzione sistemica o anomalie contabili* idonee a preludere a manipolazioni di bilancio[65]. La funzione di vigilanza si estende non solo ai profili organizzativi e procedurali, ma anche alla qualità delle informazioni generate dal sistema amministrativo-contabile, con un *focus* sull'attendibilità dei dati trasmessi all'organo amministrativo, ai soci e al mercato.
Fondamentale in questa prospettiva è l'obbligo per il collegio sindacale di presidiare i *flussi informativi* che si articolano *sia in senso orizzontale* – con le altre funzioni di controllo interno e con soggetti terzi rilevanti per la *governance* aziendale – *sia in senso verticale*, verso l'organo amministrativo e l'assemblea.
Tra i principali interlocutori del collegio vi sono:

- il revisore legale dei conti, con cui è previsto un obbligo legale di reciproco scambio di informazioni rilevanti (art. 2409-*septies* c.c.);
- il dirigente preposto alla redazione dei documenti contabili societari (art. 154-*bis* TUF);
- l'organismo di vigilanza *ex* D.Lgs. n. 231/2001;
- le funzioni aziendali di *compliance*, *risk management* e internal *audit*;
- i comitati endoconsiliari, ove istituiti (es. comitato controllo e rischi);
- il responsabile *whistleblowing* ove previsto, soprattutto ai sensi del D.Lgs. n. 24/2023.

La tempestività, l'integrità e la tracciabilità di tali flussi rappresentano precondizioni essenziali affinché l'organo possa intercettare segnali di rischio frode o devianze comportamentali nella gestione societaria. In tal senso, il collegio deve anche esercitare un controllo sull'efficacia dei canali di segnalazione interna (*whistleblowing*) e sulle misure adottate a seguito delle denunce ricevute.
L'obbligo di attivazione dell'organo di controllo si intensifica ulteriormente qualora emerga la presenza di gravi irregolarità nella gestione. L'art. 2409 c.c. prevede in tal caso che il collegio sindacale debba informare senza indugio l'organo amministrativo, formulando le proprie osservazioni e proposte. Ove non siano adottati provvedimenti idonei e tempestivi, o ove le irregolarità risultino strutturali, il collegio è tenuto a presentare denuncia al Tribunale, il quale potrà adottare provvedimenti conservativi o sostitutivi, inclusa la revoca degli amministratori o la nomina di un commissario[66].
L'inattivazione del collegio, in presenza di segnali oggettivi di criticità, può configurare una grave violazione dei doveri con conseguenze sul piano civile, disciplinare e, nei casi più gravi, penale (ad es. concorso omissivo in falso in bilancio o bancarotta fraudolenta)[67].

---

[65] Galizzi A. (2023), *Ruolo, doveri e responsabilità del collegio sindacale: una nuova era,* www.dirittodellacrisi.it.
[66] Cian V., "Il potere di denuncia al tribunale ex art. 2409 c.c.: natura, presupposti ed effetti", in *Giurisprudenza Commerciale*, 2019, I, pagg. 412 ss.
[67] Cass. pen., Sez. V, 9 febbraio 2021, n. 20867, in Cass. pen. 2021, 5, pag. 1935, con nota di L. Santalucia, *La posizione di garanzia del sindaco e il concorso omissivo nei reati societari*.

In buona sostanza, il collegio sindacale svolge una funzione di interconnessione tra i diversi organi di controllo e rappresenta l'unico soggetto dotato contemporaneamente di poteri informativi, ispettivi, segnalatori e, in taluni casi, autorizzatori. La sua efficacia dipende dalla capacità di presidiare le interrelazioni tra i presidi di legalità, nonché di attivare percorsi di escalation in presenza di anomalie. Ne deriva che la prevenzione delle frodi passa anche – e soprattutto – da un collegio sindacale vigile, competente e indipendente, in grado di cogliere le discontinuità informative, le incoerenze gestionali e le resistenze al controllo.

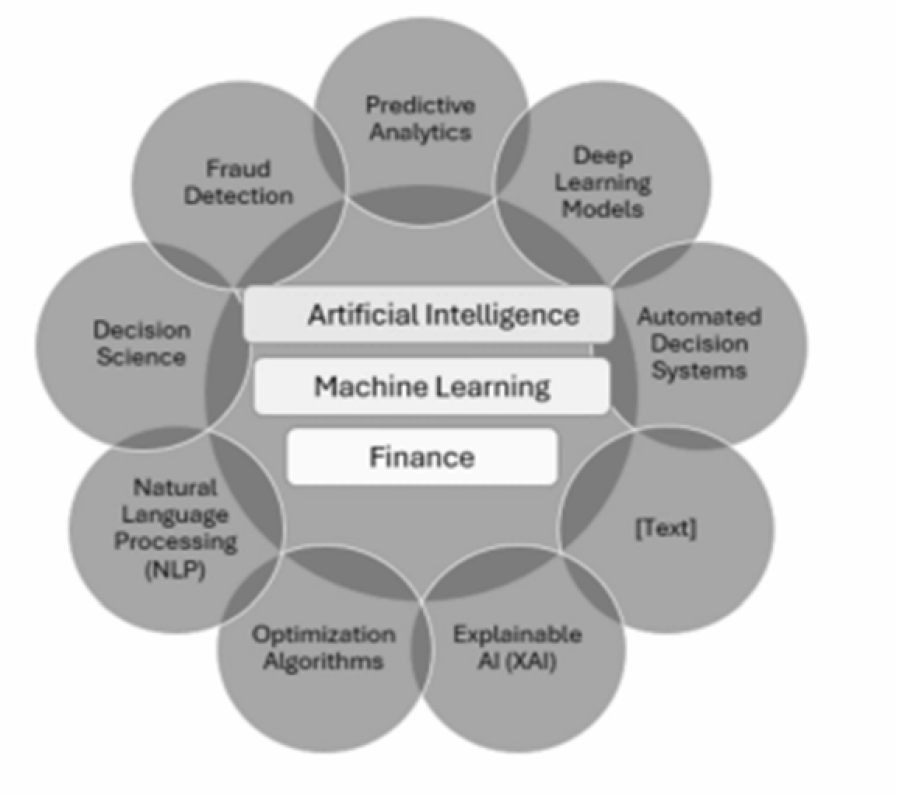
5.8. USO DELL'INTELLIGENZA ARTIFICIALE COME STRUMENTO DI PREVENZIONE

5.8.1. L'intelligenza artificiale e la sua evoluzione

L'Intelligenza Artificiale (IA), in senso lato, può essere definita come l'insieme di sistemi capaci di replicare, emulare o supportare funzioni cognitive tipiche dell'intelligenza umana – quali apprendimento, riconoscimento di *pattern*, pianificazione e ragionamento. L'evoluzione dell'IA si è articolata in diverse ondate: dalla logica simbolica e i sistemi esperti (anni '70-'80) fino agli attuali modelli neurali profondi, resi possibili dall'incremento esponenziale di potenza computazionale, disponibilità di big data e sviluppo di nuove architetture (es. *Transformers*).
Negli ultimi anni i modelli di *deep learning* hanno conosciuto un'adozione sempre più ampia grazie alla loro capacità di elaborare enormi quantità di dati e riconoscere schemi complessi[68].

[68] Farhina Sardar Khan et altri (2025), *Model-agnostic explainable artificial intelligence methods in finance: a systematic review, recent developments, limitations, challenges and future directions,* Artificial Intelligence Review in https://*link*.springer.com/article/10.1007/s10462-025-11215-9.

Tavola 5.6. – **Caratteristiche principali dell'intelligenza artificiali in più domini**



La c.d. *AI generativa* (con modelli come GPT-4, Claude, Gemini) ha segnato una discontinuità radicale: tali modelli sono in grado di processare linguaggio naturale, codice, immagini e dati numerici, fungendo da *assistenti cognitivi* ad ampio spettro. In ambito contabile, ciò si traduce nella possibilità di automatizzare operazioni documentali, generare sintesi finanziarie, proporre diagnosi di incongruenze nei bilanci, elaborare raccomandazioni su rischi potenziali.
Questa rapida evoluzione tecnologica spinge il settore contabile a esplorare nuovi strumenti per automatizzare procedure tradizionalmente manuali, pur tenendo conto delle sfide di affidabilità e trasparenza intrinseche alle reti neurali avanzate.

5.8.2. L'intelligenza artificiale nella revisione contabile e nell'analisi antifrode

Ancor prima della larga diffusione e proliferazione di sistemi IA che stanno avendo nell'attualità, va rilevato che alcuni sistemi muniti di intelligenza artificiale sono stati

utilizzati già dagli anni '90 da differenti società di revisione, ad esempio *Audit Planning* Advisor di Deloitte, Planet di PwC e WinProcess di Arthur Andersen. Non tutti questi sistemi, d'altronde, sono andati a buon fine e si sono dimostrati efficaci.
In particolare, nel 1995, Arthur Andersen creò un sistema in grado di presiedere la valutazione del rischio congiunto alle aziende clienti, il quale però non ha riservato conclusioni positive. Successivamente, l'intelligenza artificiale ha continuato a essere presente nel mondo della revisione contabile, pur senza grande successo, a causa della mancanza di imparzialità dell'utente. Pertanto, in seguito sono stati sviluppati nuovi approcci basati sull'intelligenza artificiale per svolgere i compiti legati alla revisione legale dei conti.
La letteratura identifica come metodi dell'intelligenza artificiale la crescita di algoritmi genetici, utili per conformare il comportamento del revisore su decisioni relative, ad esempio, alle frodi. Lo studio condotto da Lendsberg[69] costituisce un contributo significativo nell'ambito dell'applicazione dell'intelligenza artificiale, e in particolare della programmazione genetica, alla previsione della continuità aziendale e al rischio di insolvenza.
Relativamente alla valutazione del rischio, sono state introdotte le reti neurali, utili per permettere ai revisori di svolgere ad esempio l'attività sopra nominata. Inoltre, le reti neurali, secondo uno studio di Ramamoorti et al.[70], permettono all'i*nternal auditing* di ampliare la capacità dei revisori interni di teorizzare delle raccomandazioni sul controllo dei processi.

---

[69] Lensberg, Aadne, Eilifsen e McKee (2006), "*Bankruptcy theory development and classification via genetic programming*", European Journal of Operational Research. Gli autori si sono proposti di:
- Migliorare i modelli di classificazione delle aziende in termini di rischio di bancarotta.
- Superare i limiti dei modelli tradizionali (es. regressione logistica, Z-score di Altman) tramite tecniche evolutive ispirate alla teoria darwiniana.
Lensberg et al. hanno utilizzato la *Genetic Programming* (GP) per sviluppare modelli predittivi in grado di:
a) evolvere formule matematiche o strutture logiche complesse che discriminano tra imprese sane e imprese a rischio fallimento;
b) apprendere direttamente dai dati senza vincoli aprioristici sulla forma della funzione (a differenza, ad esempio, della regressione logistica che assume relazioni lineari o specifici *pattern* funzionali).
I modelli basati sulla GP hanno mostrato prestazioni superiori o comparabili ai modelli tradizionali in termini di accuratezza predittiva. La tecnica è stata in grado di catturare interazioni n*on line*ari e relazioni complesse tra variabili finanziarie spesso trascurate da approcci più rigidi.
Si è evidenziato come la GP potesse essere uno strumento promettente per lo sviluppo teorico e pratico della classificazione aziendale e della valutazione della continuità. Questo studio è rilevante per l'ambito della valutazione della continuità aziendale perché:
1) fornisce strumenti predittivi più sofisticati per identificare segnali precoci di crisi aziendale;
2) contribuisce alla diagnostica predittiva che può supportare sia i revisori sia i manager nella formulazione del giudizio di continuità;
3) mostra il potenziale della IA per automatizzare e raffinare le analisi di rischio, rendendo i processi decisionali più robusti.

[70] Ramamoorti et al. (1999), "*Research Opportunities in Internal Auditing*", The Institute of Internal Auditors Research Foundation (IIARF).

Nella revisione contabile l'IA viene oggi utilizzata per superare i limiti del campionamento tradizionale: algoritmi sofisticati possono analizzare intere popolazioni di dati contabili (anziché singoli campioni) e segnalare anomalie e schemi sospetti. In pratica, strumenti di *data analytics* consentono di identificare transazioni anomale, tendenze insolite o incongruenze quantitative nei registri finanziari.
Ad esempio, tecniche di *machine learning* non supervisionato sono impiegate per il *data mining*, riconoscendo autonomamente *trend* nascosti e *outlier*[71] nei dati grezzi. Tali approcci facilitano la scoperta di errori materiali e potenziali frodi che sfuggirebbero ad analisi manuali. Inoltre, tecnologie come la *Robotic Process Automation* (RPA) automatizzano attività ripetitive (raccolta dati, riconciliazione contabile, generazione di *report*), migliorando l'efficienza del processo di *audit*.
Insomma, nel campo della revisione, l'IA non rappresenta una mera innovazione tecnologica, ma una rivoluzione epistemologica che consente al revisore di trasformare i propri strumenti di lavoro da reattivi a predittivi. Le applicazioni pratiche includono:

- ***Audit* analitico avanzato**: strumenti basati su algoritmi di *machine learning* possono esaminare l'intero libro contabile, individuando correlazioni atipiche, variazioni statisticamente significative, scostamenti da parametri attesi o comportamenti transazionali *fuori norma* rispetto allo storico dell'impresa.
- ***Audit* continuo**: attraverso sensori digitali integrati nei sistemi ERP e applicazioni basate su *cloud analytics*, è oggi possibile monitorare flussi contabili in tempo reale (o quasi), applicando modelli predittivi su margini, costi e *cash flow* per intercettare tempestivamente derive potenzialmente fraudolente.

Esempio pratico
Una società di revisione che impiega una piattaforma AI per analizzare le scritture giornaliere di una multinazionale del *retail* scopre che, in alcuni punti vendita, i margini lordi dichiarati sono superiori di oltre due deviazioni *standard* rispetto alla media regionale. L'analisi automatica delle note integrative associate mostra una ricorrenza di commenti redatti con linguaggio ripetitivo e scarsamente informativo. L'IA suggerisce una revisione manuale: emergono operazioni fittizie di vendita/reso incrociate con società controllate non consolidate, costituenti frode sistemica.

ChatGPT è un modello linguistico generativo basato su reti neurali di tipo *Transformer* che, addestrato su grandi contenuti di testo, può generare risposte in linguaggio naturale a domande complesse. Un recente *report*[72] indica che professionalità fiscali e contabili considerano ChatGPT un potenziale fattore di trasformazione del settore: ad esempio, è stato addestrato anche sul codice tributario statunitense e può rispondere a complesse questioni fiscali in pochi secondi.

[71] *Outlier* è un termine utilizzato in statistica per definire, in un insieme di osservazioni, un valore anomalo e aberrante, ossia un valore chiaramente distante.
[72] Thomson Reuters Institute (2023), *ChatGPT and Generative AI within Accounting Firms and Corporate Tax Departments: tax professionals recognize ChatGPT's potential, but are mindful of the risks.*

Applicato all'*audit*, ChatGPT può supportare diverse attività: generare bozze di relazioni di revisione, automatizzare documentazione e reportistica, eseguire calcoli di campionamenti ipotetici o analizzare descrizioni testuali delle transazioni contabili, interpretare normative ISA, suggerire procedure di *audit* in base a casistiche descritte, creare *script* per l'analisi in Python o SQL, e generare *checklist* di controllo.
In particolare, ChatGPT è capace di riconoscere *pattern* testuali e generare codice di analisi dati: studi divulgativi mostrano che può aiutare a individuare anomalie nei *dataset* contabili e flaggare possibili frodi, ad esempio creando *script* in *Python* per il rilevamento di *outlier*.
Inoltre, l'interazione in tempo reale con il modello può assistere i revisori nella valutazione dei rischi: attraverso domande sul sistema di controllo interno e l'ambiente aziendale, ChatGPT può evidenziare aree critiche su cui focalizzare le indagini[73].

Esempi operativi

- **Generazione automatica di domande di *audit***: un revisore può chiedere a ChatGPT di generare domande per l'intervista con il CFO su transazioni straordinarie rilevate nel bilancio. Le domande possono essere orientate al Principio ISA 540 ("Stime contabili") o ISA 240 ("Responsabilità del revisore riguardo alle frodi").
- **Validazione descrittiva di anomalie**: il revisore carica su foglio di calcolo un dataset con centinaia di transazioni. Dopo aver identificato 10 transazioni sospette, le descrive a ChatGPT. Il modello, riconoscendo *pattern* tipici (es. fatturazioni cicliche senza giustificazione operativa), fornisce spiegazioni plausibili che il revisore verifica documentalmente.
- **Supporto normativo**: in caso di dubbi su obblighi comunicativi di frodi alla *governance*, ChatGPT può richiamare rapidamente i riferimenti al Principio ISA 265 ("*Comunicazione delle carenze di controllo interno*").

Tuttavia, l'uso operativo di ChatGPT pone importanti questioni etiche e pratiche. In primo luogo, gli *auditor* non devono affidarsi incondizionatamente alle risposte del modello: è necessario validare manualmente i risultati, interpretare i dati forniti nel contesto aziendale e riconoscere i limiti intrinseci del modello (*bias di training*, possibili *hallucinations* di dati inesistenti). Nella tabella che segue sono descritte le opportunità e minacce di ChatGPT per quanto riguarda l'*Audit* IT:

[73] Dilmegani C. (2025), *ChatGPT in Audit: 5 Use cases, Benefits and Challenges* in www.research.aimultiple.com.

Tavola 5.7. – **ChatGPT Benefits and Concerns in IT Auditing (*)**

ChatGPT Pros (Benefits)		ChatGPT Cons (Concerns)	
Opportunities	**Description**	**Threats**	**Description**
Enhanced Efficiency	ChatGPT automates tasks, speeds up data analysis, and increases auditor productivity.	Ethical Concerns	Ensuring unbiased algorithms and addressing ethical implications of Al· based decision-making net to impact the objectivity and fairness of audit conclusions and recommendations.
Real-Time Monitoring	ChatGPT can act as a real-time monitoring tool, detecting security breaches and unauthorized access.	Security and Privacy Risks	Protecting sensitive data and securing access to ChatGPT to prevent breaches concerning that ChatGPT may process sensitive and confidential information during data analysis and communication, necessitating robust safeguards to protect against data breaches or unauthorized access.
Enhanced Data Analytics	ChatGPT's analytical capabilities and in uncovering patterns and trends in large datasets.	Lack of Contextual Understanding	Auditors should exercise caution and validate ChatGPT's outputs with human judgment.
Improved Risk Assessment	ChatGPT assists auditors in assessing risks and identifying vulnerabilities more effectively.	Overreliance on Al	Maintaining a balanced approach and not solely relying on ChatGPT for critical decision-making. Thus, auditors should exercise their professional judgment, validate outputs, and supplement them with their own expertise to ensure accurate and appropriate conclusions.
Data Analysis Skills	ChatGPT can assist IT auditors in analyzing large volumes of data to gain experience in utilizing Al-powered tools tor efficient data processing,	Inaccurate or incomplete information	Responses from ChatGPT may be generated without fully understanding the specific context of the audit engagement.

ChatGPT Pros (Benefits)		ChatGPT Cons (Concerns)	
Opportunities	**Description**	**Threats**	**Description**
Technical Knowledge	ChatGPT consists of a wide range of technic.al concepts and terminology. Thus, auditors can expand their technical knowledge base, such as natural language processing, machine learning, and Al algorithms.	Limited Domain Expertise	ChatGPT may lack specialized knowledge and industry-specific expertise that auditors possess which can impact audit complex scenarios.
Critical Thinking	ChatGPT's responses require auditors to exercise critical thinking concerning to validate and interpret the accuracy of the generated information, considering audit objectives.	Legal and Compliance Considerations	Al in auditing may raise legal and compliance concerns, such as data protection regulations, confidentiality agreements, and intellectual property rights. it should not violate any obligations.

(*) Tabella mutuata da Diogo Reis L.C. (2023), *ChatGPT and IT Auditing: Opportunities, Threats and Challenges,* www.isaca.org.

In secondo luogo, vi sono rischi per la *privacy* e la sicurezza delle informazioni: i dati sensibili inviati a ChatGPT potrebbero essere registrati o riutilizzati per ulteriore addestramento, violando *standard* come il GDPR. In effetti, la normativa UE prevede il diritto alla cancellazione dei dati personali (dir. 17 del GDPR), mentre ChatGPT conserva e utilizza le conversazioni degli utenti ai fini di apprendimento.
Di conseguenza, le imprese devono adottare adeguate misure di controllo: cifratura delle comunicazioni, anonimizzazione dei dati inseriti, controlli di accesso rigorosi e policy interne sull'uso di AI. Infine, esistono rischi di abuso esterno: ad esempio, la stessa tecnologia ChatGPT può essere sfruttata da malintenzionati per creare *phishing* sempre più sofisticati o *malware* "polimorfi" in continuo aggiornamento, difficili da rilevare.
Nella Tavola 5.8. che segue sono indicate una serie di raccomandazioni per mitigare i rischi di ChatGPT nell'*audit* IT:

Tavola 5.8. – **Raccomandazioni per mitigare i rischi nell'utilizzo ChatGPT (*)**

- Implement robust security measures for web servers hosting ChatGPT, such as strong access controls, regular security updates, and encryption of data in transit and at rest.
- Follow industry best practices for server hardening and configuration management.
- Utilize strong authentication mechanisms, such as multi-factor authentication, to restrict access to the ChatGPT server.
- Implement role-based access controls to ensure that only authorized individuals, such as auditors or administrators, can interact with the system.
- Encrypt sensitive data both during transmission and storage. Utilize secure communication protocols, such as HTTPS, to protect data in transit.
- Employ encryption techniques, like disk-level or file-level encryption, to safeguard data stored on the server.
- Minimize the amount of sensitive data stored on the server to reduce the potential impact of a data breach.
- Store only the necessary data required for the auditing process, and regularly purge or anonymize data that ls no longer needed.
- Design a secure network architecture that segregates the ChatGPT server from other critical systems or databases.
- Implement firewalls, intrusion detection systems, and network monitoring to detect and prevent unauthorized access attempts.
- Conduct regular security audits and penetration testing to identify vulnerabilities in the server infrastructure and address them promptly.
- Engage external security experts to perform independent assessments and validate the security posture of the system.
- Establish clear policies and procedures for handling sensitive data within the ChatGPT system.
- Define guidelines tor data retention, access controls, data transfer, and secure disposal of data to ensure compliance with relevant regulations and industry standards.
- Implement monitoring systems to detect any unauthorized access attempts or suspicious activities.
- Establish an incident response plan to handle security incidents effectively and minimize their impact.
- Regularly review and update the plan based on emerging threats and lessons learned.
- Review the privacy and security policies of the Al technology provider, including how they handle and protect customer data.
- Ensure that the provider has robust security measures in place to safeguard sensitive information.
- Evaluate whether the Al technology provider complies with relevant data protection regulations and industry standards.
- Look for certifications or audits that demonstrate their commitment to data privacy and security, such as ISO 27001 or SOC2.
- Clarify the terms of data ownership and how the Al techno1ogy provider handles the data entered into the system.
- Ensure that the provider respects customer data confidentiality and does not use or share it for purposes other than providing the agreed-upon services.
- Inquire about the transparency and explainability of the Al models used by the provider.
- Understand how they address potential biases, ensure fairness, and provide explanations for the Al's decisions or outputs.
- Establish clear legal agreements with the Al technology provider that address data protection confidentiality, and intellectual property rights.
- Work with legal professionals to ensure that the agreements adequately protect your interests as an IT auditor.
- Consider the reputation and track record of the Al technology provider.

- Seek references or case studies from other organizations that have used their services and inquire about their experiences with data protection and trustworthiness.
- Conduct regular audits or assessments or the AI technology provider's security controls and processes, which can help verify their adherence to privacy and security standards and identify any potential gaps or concerns.
- Maintain open and transparent communication channels with the AI technology provider.
- Establish a relationship where you can discuss any concerns, seek clarifications, or report any issues related to data protection or trust.

(*) Tabella mutuata da Diogo Reis L.C. (2023), *ChatGPT and IT Auditing: Opportunities, Threats and Challenges*, www.isaca.org.

Riassumendo, ChatGPT e strumenti analoghi offrono agli *auditor* opportunità di automazione e *insight* avanzati (nei test antifrode e nella reportistica), ma devono essere integrati con supervisione umana e adeguati controlli di *governance.*
Nondimeno, il settore mostra anche riserve: la natura di *scatola nera* di molti algoritmi (in particolare quelli non supervisionati) genera incertezza e può confliggere con i principi di accuratezza, tracciabilità e verificabilità propri della contabilità. In sintesi, l'IA offre oggi capacità avanzate di analisi dei dati contabili, ma richiede revisori adeguatamente formati che validino i risultati e interpretino criticamente gli output tecnologici.

5.8.3. Tecniche avanzate di AI applicate alla revisione contabile: Big Data, Machine Learning e Blockchain

L'adozione di *Big Data* e tecniche di *analytics* consente ai revisori di estrarre informazioni da ingenti moli di dati contabili e finanziari. L'analisi predittiva e descrittiva di dati storici aiuta a prefigurare transazioni future e a individuare tempestivamente segnali di allarme. In pratica, le revisioni possono sfruttare due approcci principali: un *approccio induttivo* (esplorativo) per comprendere l'azienda e valutare rischi complessivi, e un *approccio deduttivo* per confermare ipotesi di rischiosità al termine del processo di revisione. I *Big Data* possiedono infatti anche un potere predittivo, consentendo di definire aspettative sul piano contabile e anticipare possibili incoerenze (es. previsione di vendite o costi futuri).
Le tecnologie di *Machine Learning* e *Deep Learning* sono utilizzate per automatizzare compiti di classificazione e clusterizzazione dei dati contabili. Ad esempio, algoritmi di apprendimento supervisionato possono essere addestrati su bilanci noti (fraudolenti e corretti) per riconoscere modelli di frode, mentre algoritmi non supervisionati identificano gruppi di transazioni simili e *outlier* irregolari. Tali metodi consentono di ampliare l'analisi oltre le procedure *standard*: all'interno di grandi *dataset*, le reti neurali possono individuare correlazioni nascoste e relazioni di causalità non evidenti, accelerando la scoperta di anomalie. Parallelamente, la tecnologia *blockchain* viene studiata come supporto alla revisione: grazie all'immutabilità e alla disponibilità immediata delle transazioni registrate, essa permette di condurre *audit* continui e in tempo reale, riducendo i tempi di raccolta dati e documentazione.

In particolare, i principali approcci includono:

- **Machine Learning supervisionato**: addestramento di modelli predittivi sulla base di bilanci corretti e fraudolenti. Algoritmi come *Random Forest* o *SVM* possono classificare nuove aziende in base al rischio di alterazione contabile.
- **Unsupervised learning**: tecniche come l'analisi delle componenti principali (PCA), *clustering K-means* o *autoencoder* neurali aiutano a identificare transazioni "anomale" rispetto alla distribuzione storica.
- **Blockchain auditing**: l'adozione di contabilità su blockchain consente verifiche incrociate immediate, *audit trail* automatici, e immutabilità dei dati – riducendo drasticamente le opportunità di manomissione.

Qui di seguito, un sintetico esempio operativo.

> Un'impresa *fintech* integra nel proprio sistema ERP una *blockchain permissioned* (es. *Hyperledger*) per le registrazioni contabili. Ogni pagamento è validato e firmato digitalmente dal sistema. Il revisore, grazie a un nodo di lettura, può verificare in autonomia le registrazioni finanziarie con *timestamp* e confrontarle con le transazioni bancarie, eliminando così il rischio di duplicazione o frodi *post-eventum*.

In buona sostanza, l'integrazione di *Big Data*, *Machine Learning* e *Blockchain* promette una revisione più efficace ed esaustiva, sebbene richieda competenze avanzate e adeguamenti normativi (ad esempio *standard* per l'analisi dei dati).

5.8.4. Intelligenza artificiale spiegabile (XAI) in ambito contabile

A mano a mano che i modelli di IA si fanno più complessi, cresce la necessità di esplicitare i criteri delle loro decisioni. Nel contesto della revisione contabile, la trasparenza delle decisioni algoritmiche è fondamentale per soddisfare i requisiti di affidabilità e rendicontazione. Recenti studi sottolineano che la mancanza di spiegabilità delle reti neurali rappresenta un ostacolo nei settori regolamentati: nel finance la trasparenza delle decisioni è di primaria importanza, e la scarsa esplicabilità genera preoccupazioni sull'uso di modelli *black-box*[74].

Per questo motivo è emersa la disciplina della **XAI** (*Explainable AI*), che comprende tecniche volte a rendere interpretabili i risultati dei modelli di apprendimento automatico.

In letteratura sono state proposte diverse metodologie XAI per l'*audit*; infatti, alcune applicazioni illustrano l'uso di approcci *model-agnostic* come **LIME** (Local Interpretable Model-agnostic Explanations) e **SHAP** (Shapley Additive Explanations) per spiegare in modo locale le predizioni di un modello volto a valutare il rischio di errori materiali[75].

Tali strumenti forniscono contributi qualitativi che aiutano i revisori a comprendere quali variabili hanno influenzato maggiormente una predizione (ad esempio, quali voci

[74] Yeo W.J. et altri (2025). *A comprehensive review on financial explainable AI,* Artificial Intelligence Review. https://doi.org/10.1007/s10462-024-11077-7.

[75] Zhang, Chanyuan (Abigail) & Cho, Soohyun & Vasarhelyi, Miklos, 2022. "*Explainable Artificial Intelligence (XAI) in auditing*," International Journal of Accounting Information Systems, Elsevier, vol. 46(C).

di bilancio hanno contribuito a segnalare una potenziale frode). Altre soluzioni, come alberi di regole appresi automaticamente o reti simboliche (*neural-symbolic*), cercano di bilanciare accuratezza e interpretabilità esplicita dei criteri decisionali.
In particolare:

- **SHAP (Shapley Additive Explanations**): calcola il contributo marginale di ogni variabile nella predizione. Applicabile a modelli di rischio frode per comprendere quali voci (es. crediti, immobilizzazioni) hanno inciso su una classificazione anomala.
- **LIME (Local Interpretable Model-Agnostic Explanations**): genera modelli lineari locali approssimanti il comportamento del modello black-box nei dintorni del dato specifico.
- **Anchors e Counterfactuals**: forniscono esempi del tipo "se questa variabile avesse avuto valore X invece di Y, l'esito sarebbe cambiato?", utili per scenari di *audit* forense.

Una esemplificazione pratica:

> Una società utilizza un modello di AI per segnalare potenziali frodi tra le fatture fornitore. Un revisore scopre che tre transazioni sono state classificate come rischiose. Applicando SHAP, emerge che il peso determinante è il campo "*fattura in orari non lavorativi*" e "*importo esatto ricorrente*". Il revisore verifica e scopre una rete di autofatturazioni create durante i fine settimana da una partita IVA intestata a un *ex* dipendente.

Uno studio recente[76], propone un quadro matematico di XAI per *audit* regolamentari, in cui l'esplicabilità del modello viene trattata come un vincolo quantificabile nell'ottimizzazione: usando misure basate sulla teoria dell'informazione e valori di *Shapley*[77], si bilanciano *performance* predittive e vincoli di trasparenza richiesti dalle normative.

[76] Desai, Hrishikesh, (2024). "*Reimagining Compliance: Explainable AI Models for Financial Regulatory Audits*". Available at SSRN: https://ssrn.com/abstract=5230527 or http://dx.doi.org/10.2139/ssrn.5230527.

[77] La teoria dell'informazione e i valori di Shapley sono due concetti provenienti da ambiti diversi — rispettivamente dalla matematica/statistica e dalla teoria dei giochi — ma sono sempre più spesso utilizzati insieme, soprattutto nel campo dell'intelligenza artificiale e dell'interpretabilià dei modelli predittivi (*explainable* AI). La teoria dell'informazione, fondata da Claude Shannon (1948), si occupa della quantificazione, trasmissione ed elaborazione dell'informazione. I concetti chiave includono:
- *Entropia* (H): misura dell'incertezza associata a una variabile casuale. Più alta è l'entropia, maggiore è l'informazione potenziale trasportata.
- *Information gain* (guadagno informativo): misura della riduzione di entropia dovuta alla conoscenza di una variabile (usato, ad esempio, per costruire alberi decisionali).
- *Mutual information* (informazione mutua): misura la quantità di informazione condivisa tra due variabili.
Nel contesto dei modelli predittivi, la teoria dell'informazione permette di valutare quanto un attributo contribuisce alla riduzione dell'incertezza nella previsione di un *output*.
I valori di Shapley provengono dalla teoria cooperativa dei giochi (Shapley, 1953) e permettono di assegnare in modo equo il "*valore*" generato da una coalizione di giocatori a ciascun partecipante, tenendo conto del contributo marginale di ognuno.
Applicati ai modelli di machine learning, i valori di Shapley:
- Attribuiscono a ogni variabile indipendente (feature) una parte del merito (o della responsabilità) per una determinata previsione del modello.
- Sono model-agnostic, cioè non dipendono dall'architettura del modello.
- Garantiscono equità, simmetria, efficienza e additività nel modo in cui il contributo viene assegnato.

Nonostante questi progressi, i metodi XAI attuali hanno ancora importanti limiti. Ad esempio, poche tecniche affrontano aspetti cruciali come l'equità o l'affidabilità del modello: molti sistemi producono spiegazioni solo locali (attinenti al singolo caso) senza fornire una visione globale dei ragionamenti interni. Inoltre, come osserva una recente rassegna in ambito finanziario, migliorare equità, affidabilità e causalità delle spiegazioni rimane un campo di ricerca emergente con metodi ancora poco sviluppati. In pratica, risulta difficoltoso produrre una spiegazione "una-taglia-per-tutti"; diventa quindi essenziale adattare gli strumenti XAI alle esigenze degli utilizzatori (ad es. regolatori, manager interni, revisori), tenendo conto dei limiti intrinseci (*bias* di ottimizzazione, volatilità delle spiegazioni) e della necessità di formazione specialistica per interpretarli correttamente. In definitiva, l'IA spiegabile rappresenta una promettente strada per aumentare la fiducia nei modelli di *audit*, ma va integrata con criteri di controllo e responsabilità umana per garantire reale trasparenza e *accountability* nel processo di revisione.