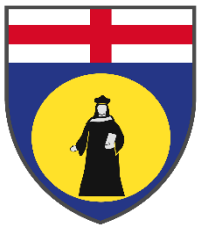
UNIVERSITA' DI UNIGE
SCUOLA DI SCIENZE SOCIALI
DIPARTIMENTO DI ECONOMIA



Tesi di laurea magistrale in

Auditing

AI e continuous auditing per il contrasto alle frodi contabili: una rassegna della letteratura

Relatore: Paola Ramassa

Candidato: Andrea Parodi

Anno accademico
2025/2026

Abstract

La presente tesi consiste in una rassegna della letteratura sull'applicazione dell'intelligenza artificiale e del continuous auditing alla rilevazione delle frodi contabili, valutando le potenzialità di tali strumenti rispetto ai limiti del modello tradizionale di revisione e analizzandone le implicazioni sul ruolo del revisore e sul quadro normativo. Adottando l'approccio della narrative review, la ricerca seleziona 42 articoli tramite estrazione su Scopus, integrati da fonti normative. Il corpus comprende prevalentemente studi empirico-quantitativi (64,3%), con una concentrazione geografica su contesti nordamericani e asiatici che evidenzia un significativo gap nella letteratura riferita al contesto europeo e italiano. I risultati mostrano che il machine learning applicato ai dati contabili grezzi supera i metodi statistici tradizionali nelle false comunicazioni sociali, anticipando la frode fino a due anni prima della sua emersione. Il natural language processing aggiunge un contributo informativo autonomo analizzando il tono linguistico nelle relazioni sulla gestione, migliorando l'accuratezza predittiva del 12-15% rispetto ai soli dati quantitativi. Il continuous auditing, trasformando la logica della revisione da ex-post a tempo reale, si rivela efficace nel rilevare appropriazioni indebite e schemi corruttivi. L'adozione di questi strumenti introduce tuttavia rischi rilevanti, in primo luogo l'automation bias, documentato da una contrazione del 35% dello scetticismo professionale tra i revisori che utilizzano l'IA in modo intensivo. Il quadro normativo internazionale, pur in evoluzione, presenta ancora un ritardo rispetto alla velocità di diffusione tecnologica, delineando la necessità di evolvere verso un modello di revisione ibrido nel quale resta centrale il giudizio professionale del revisore.

This thesis consists of a literature review on the application of artificial intelligence and continuous auditing to financial statement fraud detection, assessing the potential of these tools relative to traditional audit models and analysing their implications for the auditor's role and the regulatory framework. Adopting a narrative review approach, the research selects 42 articles through a systematic Scopus extraction supplemented by regulatory sources. The analysed corpus consists predominantly of empirical-quantitative studies (64.3%), with a geographic concentration in North American and Asian contexts that reveals a significant gap in European and Italian literature. The findings show that machine learning applied to raw accounting data outperforms traditional statistical

methods in detecting financial statement fraud, with models capable of anticipating fraud up to two years before public disclosure. Natural language processing adds independent informational value through the analysis of linguistic tone in management reports, improving predictive accuracy by 12-15% compared to quantitative data alone. Continuous auditing, by shifting audit logic from ex-post to real-time monitoring, proves highly effective in detecting asset misappropriation and corruption schemes. However, the adoption of these tools introduces significant risks, most notably automation bias, documented by a 35% reduction in professional scepticism among auditors who utilize algorithmic systems intensively. The regulatory framework, while evolving, still lags behind the pace of technological diffusion, outlining the necessary transition toward a hybrid auditing model in which the auditor's professional judgment remains central.

Introduzione

L'informazione finanziaria è il fondamento su cui si reggono le decisioni degli investitori, dei creditori e di tutti gli stakeholder che gravitano attorno a un'impresa. Quando questa informazione viene alterata deliberatamente, le conseguenze si propagano ben oltre i confini dell'azienda coinvolta, si alterano i meccanismi di fiducia su cui si fonda il funzionamento dei mercati, si generano danni patrimoniali spesso irreversibili per chi ha fatto affidamento su bilanci falsati e viene meno la credibilità delle istituzioni preposte al controllo. I casi Wirecard e Parmalat, differenti per contesto geografico ma analoghi nelle modalità di manipolazione dell'informazione finanziaria, hanno dimostrato che le frodi contabili di grandi dimensioni non sono eventi eccezionali ma manifestazioni patologiche di vulnerabilità che il modello tradizionale di revisione esterna fatica a intercettare in modo tempestivo.

I dati dell'ACFE documentano che solo il 3% delle frodi occupazionali viene scoperto attraverso l'attività di audit esterno, con la durata media prima della scoperta pari a circa dodici mesi, un arco di tempo sufficiente nella maggior parte dei casi a consolidare il danno in modo significativo. I fallimenti dei meccanismi di controllo sono talvolta riconducibili a gravi carenze nello scetticismo professionale, a negligenze o, nei casi più severi, a condotte conniventi da parte dei soggetti incaricati della verifica. Il modello su cui si fonda la revisione tradizionale (campionamento periodico, controlli ex-post, giudizio esercitato su un sottoinsieme limitato di transazioni) presenta limiti significativi quando si confronta con condotte fraudolente progettate per non essere rilevate da quei controlli specifici.

In questo scenario, la progressiva introduzione delle tecnologie basate sull'intelligenza artificiale offre nuovi strumenti per l'analisi del rischio di revisione. La capacità di estendere le verifiche all'intera popolazione delle transazioni azzerando il rischio di campionamento, l'identificazione di anomalie statistiche non intercettabili mediante procedure manuali e la transizione verso un monitoraggio contabile tempestivo si configurano come risposte tecniche alle criticità strutturali descritte dalla dottrina contabile. I modelli di machine learning, le architetture di natural language processing e i sistemi di continuous auditing non rappresentano meri innesti tecnologici volti al miglioramento dei processi di routine, bensì soluzioni strutturali potenzialmente coerenti

con le specificità dei fattori di rischio che il modello di audit tradizionale fatica a presidiare.

La letteratura documenta che l'adozione di strumenti automatizzati presenta dei rischi. L'automation bias (la tendenza a fidarsi eccessivamente degli output algoritmici riducendo il proprio giudizio critico indipendente) è stato misurato, a seguito di alcuni studi, in una riduzione del 35% dello scetticismo professionale tra i revisori che usano l'IA in modo intensivo. Gli algoritmi producono previsioni accurate ma attraverso processi decisionali opachi, che rendono difficile per il revisore motivare le proprie conclusioni in modo documentabile. I modelli addestrati su dataset di società quotate statunitensi non sono direttamente trasferibili al contesto delle piccole e medie imprese italiane, che operano con principi contabili diversi e in un mercato della revisione strutturalmente differente. Il quadro normativo e regolatorio internazionale (IAASB, PCAOB, EU AI Act) sta cercando di rispondere a queste sfide, ma con tempi che non riescono a stare al passo con la velocità di diffusione tecnologica nella pratica professionale.

L'oggetto di questo lavoro è l'intersezione tra questi due piani: le potenzialità degli strumenti tecnologici nell'individuazione delle frodi e i rischi che la loro adozione introduce per la qualità del giudizio professionale del revisore. In quest'ottica, la tesi è volta a perseguire tre obiettivi conoscitivi fondamentali. Il primo consiste nell'analizzare in che modo il machine learning, il natural language processing e il continuous auditing migliorano la capacità di rilevare le frodi rispetto al modello tradizionale di audit. Il secondo mira a individuare quali rischi introduca l'adozione di tali strumenti per la tenuta dello scetticismo professionale e per la qualità complessiva del controllo. Il terzo intende verificare come il quadro normativo internazionale stia cercando di governare e regolamentare questa rapida trasformazione aziendale.

Il metodo adottato si basa su una rassegna della letteratura nella forma di una narrative review, che prevede la selezione di fonti attraverso un'estrazione sistematica su Scopus con una stringa di ricerca articolata su tre domini tematici: il processo di audit, le tecnologie applicate alla revisione e il fenomeno della frode contabile. Dei 711 risultati iniziali, 42 articoli sono stati inclusi nella rassegna finale dopo l'applicazione di cinque criteri di esclusione, tra cui la pertinenza tematica, una finestra temporale a partire dal 2023 e soglie minime di citazioni calibrate per anno di pubblicazione. La scelta della

narrative review rispetto a un protocollo sistematico più rigido è motivata dalla natura frammentata del campo, che si colloca all'intersezione tra tre tradizioni disciplinari distinte (la letteratura di auditing, quella di data science e quella più recente di regolamentazione dell'IA) e dalla rapidità con cui la letteratura si sta evolvendo, con oltre il 57% degli articoli inclusi pubblicato negli ultimi due anni.

La struttura del lavoro si sviluppa in quattro capitoli. Il primo ricostruisce il quadro teorico della frode contabile: definisce la distinzione tra frode ed errore, classifica le tipologie secondo la tassonomia dell'ACFE, ripercorre l'evoluzione dei modelli esplicativi da Cressey a Vousinas, analizza le responsabilità del revisore ai sensi dell'ISA Italia 240 e identifica i limiti strutturali dell'audit tradizionale, concludendo con una prima introduzione al contributo dell'intelligenza artificiale come risposta a quei limiti. Il secondo illustra il protocollo della rassegna della letteratura: la scelta metodologica della narrative review, la costruzione della stringa di ricerca, i criteri di selezione, la classificazione degli articoli per tipologia metodologica, contesto geografico e area disciplinare della rivista. Il terzo analizza in dettaglio i tre strumenti tecnologici principali (machine learning, NLP e continuous auditing) documentandone per ciascuno i risultati empirici, i metodi di ricerca utilizzati negli studi chiave, i campioni analizzati e i limiti applicativi, concludendo con un confronto integrato tra l'efficacia di ciascuno strumento per le diverse tipologie di frode. Il quarto capitolo affronta le implicazioni professionali e normative: la trasformazione del ruolo del revisore, l'automation bias e i bias algoritmici, il quadro regolatorio emergente a livello internazionale e le prospettive del modello ibrido tra giudizio umano e intelligenza artificiale.

I. Le frodi contabili e il ruolo della revisione

1.1 La definizione di frode

Nel linguaggio della revisione contabile, il termine frode assume un significato tecnico preciso, definito nei principi di revisione internazionali (ISA) e recepito nella normativa professionale. Esiste una fondamentale distinzione tra frode ed errore che, pur producendo effetti simili sul bilancio con l'alterazione della sua correttezza, sono due fenomeni che si differenziano per natura, origine e per le implicazioni che ne derivano al revisore.

Il quadro regolatorio internazionale definisce i perimetri di queste fattispecie legandoli direttamente alle responsabilità del revisore (IAASB, 2024). L'errore deriva da un'azione involontaria che può essere un'imprecisione matematica, un'errata applicazione di un principio contabile, una svista nella rilevazione di un'operazione o una stima basata su premesse non corrette ma assunte in buona fede. La frode, al contrario, presuppone che ci sia l'elemento soggettivo del dolo, è un atto intenzionale e consapevole compiuto con lo scopo di ottenere un vantaggio illecito o ingiusto che tipicamente va a danneggiare l'impresa, i soci oppure i suoi stakeholder.

Tale distinzione ha delle conseguenze importanti nel contesto della revisione contabile. Un errore, per quanto possa essere grave e materialmente significativo, tende a manifestarsi in modo non pianificato e di conseguenza tende a lasciare tracce, produrre incongruenze che emergono poi nei normali processi di riconciliazione e di controllo svolti dai team di revisione, e non è strutturato con una logica di occultamento. La frode, a differenza dell'errore, è intrinsecamente finalizzata all'occultamento. Il frodatore, conoscendo i meccanismi di controllo esistenti, agisce deliberatamente per eluderli attraverso la falsificazione di documenti e la manipolazione delle registrazioni contabili. Spesso, il ricorso a schemi collusivi rende estremamente complessa l'identificazione da parte del revisore; è proprio questa intenzionalità che conferisce alla frode una gravità superiore rispetto alla natura involontaria dell'errore (Colbert, 2000).

La definizione tecnica più precisa in materia di Audit è contenuta nell'ISA 240, il principio di revisione internazionale dedicato alle responsabilità del revisore in merito alla frode nell'ambito dell'audit del bilancio. Questo standard distingue la frode dall'errore e individua due tipologie di frode rilevanti ai fini della revisione: le rettifiche derivanti da appropriazione indebita di attività e le rettifiche derivanti da false comunicazioni sociali.

Tale bipartizione riflette differenze nelle modalità di realizzazione, negli effetti sulla veridicità del bilancio e sulle responsabilità del revisore.

Con riferimento alle rettifiche derivanti da appropriazioni indebite, la condotta illecita consiste nel furto o nell'uso improprio di attività patrimoniali dell'impresa; queste operazioni sono spesso seguite dalla manipolazione del bilancio, al fine di occultare l'ammanco e la condotta fraudolenta stessa. L'illecito può manifestarsi attraverso diverse modalità operative: la sottrazione di incassi non registrati, il furto di attività aziendali usate per scopi esclusivamente personali oppure l'induzione dell'entità al pagamento di beni o servizi mai ricevuti. In quest'ultimo caso, l'illecito viene occultato mediante la predisposizione di registrazioni contabili false o documentazione fuorviante, volta a mascherare l'indebito utilizzo delle risorse.

Per quanto riguarda le rettifiche derivanti da false comunicazioni sociali, la condotta fraudolenta si manifesta attraverso la manipolazione, la falsificazione o l'alterazione delle scritture contabili e dei documenti a supporto con cui poi viene redatto il bilancio. Questi comportamenti sfociano nell'omissione di eventi significativi o in un'intenzionale applicazione scorretta dei principi contabili, finalizzate a distorcere la rappresentazione della realtà economica. Identificare questo tipo di frode risulta complicato poiché i trattamenti contabili sono spesso frutto di valutazioni discrezionali e il confine tra una rappresentazione ottimistica ma corretta e una vera e propria frode può essere sottile (ICAEW, 2020).

Questi comportamenti hanno degli impatti sulla rappresentazione veritiera e corretta del bilancio che è uno degli aspetti fondamentali da verificare per il revisore e soprattutto è il riferimento normativo di fondo nell'ordinamento contabile italiano ed europeo. Quando la frode ha ad oggetto le comunicazioni sociali, l'intero impianto informativo del bilancio risulta compromesso dalla presenza di poste attive sopravvalutate, passività sottostimate, ricavi gonfiati o costi occultati per ottenere un risultato di bilancio migliore. La ripercussione va a coinvolgere anche gli stakeholder (investitori, azionisti, creditori) che potrebbero prendere decisioni economiche sulla base di un bilancio non corretto. Nel caso delle appropriazioni indebite, invece, l'impatto sul bilancio dipende dalla materialità e dal modo in cui la sottrazione viene contabilizzata e nascosta. Talvolta le somme sottratte sono relativamente modeste e non incidono sulla rappresentazione veritiera e corretta nel suo complesso, ma in altri casi, soprattutto

quando la frode persiste nel tempo, l'effetto cumulato può diventare significativo e richiedere una rettifica sostanziale dei conti.

La distinzione tra frode ed errore non ha solo rilievo concettuale ma produce effetti molto diversi e concreti sul grado di scetticismo professionale che il revisore è tenuto a manifestare nell'esercizio della propria attività. Il principio ISA 240 richiede che il revisore mantenga un atteggiamento di scetticismo professionale per tutta la durata dell'incarico, riconoscendo la possibilità che nel bilancio possano esistere errori significativi dovuti a frodi, indipendentemente dall'esperienza passata circa l'onestà e l'integrità del management. Lo scetticismo professionale è definito come un atteggiamento che richiede una mente critica, la capacità di essere vigili rispetto a condizioni che possano indicare possibili inesattezze dovute a errore o frode, e una valutazione critica delle prove di revisione. Questa è una delle sfide della professione del revisore, il quale deve applicare uno scetticismo genuino in un contesto in cui i rapporti professionali con il management tendono a generare fiducia, e in cui le conferme possono indurre a interpretare le evidenze a supporto delle spiegazioni fornite dai soggetti revisionati. Il principio ISA 240 rafforza ulteriormente il concetto dicendo che il revisore deve affrontare ciascun incarico con uno sguardo rinnovato, evitando che l'esperienza accumulata negli anni precedenti con quel cliente attenui l'applicazione del giudizio critico. Vengono inoltre introdotti elementi applicativi che chiariscono come alcune condizioni tipiche degli incarichi di revisione possano generare pressioni che ostacolano il corretto esercizio dello scetticismo (IAASB, 2024).

La SEC (Securities and Exchange Commission), ente federale incaricato della supervisione e regolamentazione delle società quotate in borsa negli Stati Uniti, ha sottolineato con preoccupazione che molti revisori tendono a inquadrare le proprie responsabilità in termini di ciò che non gli viene richiesto, piuttosto che concentrarsi sugli obblighi positivi di pianificare e svolgere la revisione in modo da ottenere ragionevole sicurezza circa l'assenza di errori significativi dovuti a frodi. Questo atteggiamento incide sulla mentalità del revisore e può ridurre concretamente la probabilità di rilevare le frodi (Munter, 2022).

Il quadro risulta ancora più preoccupante se si considera la dimensione del fenomeno, secondo quanto riportato dai dati dell'ACFE (2024), organizzazione che si dedica a combattere la frode e l'inganno, le organizzazioni perdono in media il 5% dei

propri ricavi annui a causa delle frodi occupazionali, con una perdita media per singolo caso pari a 1,7 milioni di dollari. Dato particolarmente rilevante per la revisione è anche la componente temporale: la durata media prima che una frode venga scoperta è di dodici mesi, una circostanza che evidenzia la natura furtiva e sofisticata di questi schemi. L'errore contabile tende ad emergere con lo svolgimento dei normali processi di riconciliazione e controllo svolti dalle aziende e dal revisore, la frode invece può restare nascosta per lungo tempo proprio perché chi la commette agisce con piena consapevolezza dei meccanismi di verifica che vengono svolti, e li aggira attraverso falsificazione dei documenti, collusione tra soggetti o manipolazione delle registrazioni. Le procedure di audit standard volte a raccogliere prove di revisione possono rivelarsi inefficaci per rilevare una frode che preveda, ad esempio, la collusione per falsificare documentazione al punto da indurre il revisore a ritenere valide prove che non lo sono (Tümmler, 2026).

L'ISA 240 chiarisce che la valutazione da parte del revisore circa la materialità di una frode, o di una sospetta frode, richiede l'esercizio del giudizio professionale, tenendo conto sia di fattori quantitativi che qualitativi. Una rettifica che non è materiale quantitativamente potrebbe esserlo qualitativamente come può essere il caso di una frode commessa dal top management. La frode può manifestarsi con importi modesti ma protrarsi nel tempo o con condotte che segnalano una disfunzione grave nel sistema dei controlli interni dell'azienda e nell'integrità del management.

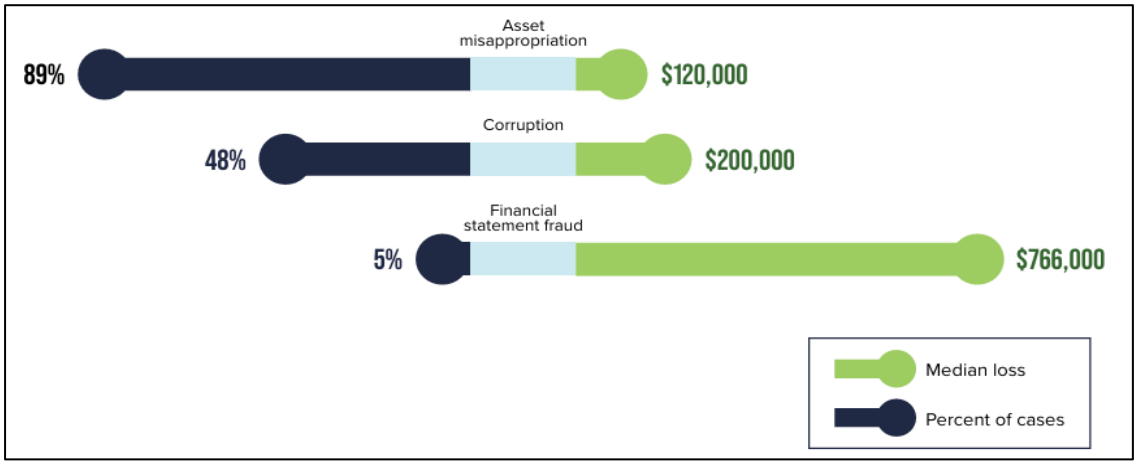
1.2 La classificazione delle fattispecie di frode secondo l'ACFE

Un'altra importante definizione di frode viene proposta con la classificazione elaborata dall'Association of Certified Fraud Examiners (ACFE), organizzazione internazionale che dal 1996 pubblica con cadenza biennale il ''Report to the Nations'', una ricerca sul fenomeno delle frodi occupazionali a livello globale. La classificazione che viene proposta dall'ACFE è un punto di riferimento importante sia per la letteratura accademica che per la prassi professionale della revisione contabile, costituisce la base su cui si fondano molti degli approcci metodologici alla valutazione del rischio di frode nell'attività di audit.

Secondo l'ACFE (2024), la frode occupazionale, intesa come condotta fraudolenta di un soggetto interno all'organizzazione ai danni dell'organizzazione stessa, si articola in

tre macrocategorie: l'appropriazione indebita di attività (asset misappropriation), la corruzione (corruption) e le false comunicazioni sociali (financial statement fraud). La presenza di una di queste categorie non esclude la presenza di una delle altre, nel 35% dei casi analizzati dal Report to the Nations 2024 si riscontra una sovrapposizione tra appropriazione indebita e corruzione.

Grafico 1.1: Relazione tra frequenza e perdita mediana per tipologia di frode



Fonte: ACFE, 2024: P. 10

Tra le tre categorie, quella più diffusa è l'appropriazione indebita, presente secondo i dati riportati dall'ACFE nell'89% dei casi analizzati con una perdita mediana per caso di 120.000 dollari. È la tipologia di frode più vicina al dipendente comune, in quanto non richiede necessariamente l'accesso alle leve del bilancio né una posizione particolare all'interno dell'organizzazione, ma sfrutta il controllo diretto sulle risorse aziendali, come possono essere denaro contante, inventario, attrezzature o dati, per sottrarne una parte a proprio vantaggio. L'ACFE classifica diverse sottotipologie di appropriazione indebita tra cui le più frequenti risultano essere le frodi sulla fatturazione e la deviazione di pagamenti destinati all'organizzazione, le quali risultano anche tra le più difficili da individuare siccome possono essere occultate attraverso la creazione di fornitori fittizi, la duplicazione di fatture reali o la collusione con soggetti esterni. La condotta illecita è spesso accompagnata da un'attività di falsificazione documentale finalizzata a mascherare la sottrazione e a rendere invisibile ai controlli ordinari l'uso illecito delle risorse aziendali. L'appropriazione indebita, pur essendo la categoria più frequente, non sempre

porta a rettifiche significative sul bilancio nel suo complesso, la perdita mediana è relativamente contenuta rispetto alle altre tipologie. Nonostante ciò, la sua pervasività e la sua tendenza a perdurare nel tempo prima che venga scoperta fa sì che il revisore debba prestare attenzione non solo alle anomalie quantitativamente rilevanti, ma anche a schemi ricorrenti e apparentemente minori che, considerati nel loro insieme, possono segnalare un problema sistemico nei controlli interni.

La corruzione rappresenta la seconda categoria per frequenza. Secondo l'ACFE è uno schema in cui un dipendente abusa della propria influenza in una transazione commerciale in modo da violare i propri doveri verso il datore di lavoro, al fine di ottenere un vantaggio diretto o indiretto, come nei casi di tangenti o conflitti di interesse. Nel Report to the Nations 2024, la corruzione è presente nel 48% dei casi analizzati, con una perdita mediana di 200.000 dollari per caso. I dati evidenziano una percentuale minore rispetto al caso precedente ma una maggiore soglia di perdita media. La corruzione si può manifestare in diverse forme: conflitti di interesse non dichiarati, corruzione attiva e passiva, estorsione economica, accordi collusivi in sede di gare d'appalto (bid rigging) e schemi di kickback, nei quali un dipendente riceve compensi occulti da fornitori o clienti in cambio di condizioni commerciali favorevoli per questi ultimi e svantaggiose per l'organizzazione di appartenenza. Per il revisore la corruzione è una pratica particolarmente difficile da individuare in quanto non si manifesta necessariamente attraverso anomalie nelle registrazioni contabili, bensì la transazione può essere perfettamente documentata, registrata in modo formalmente corretto e al giusto valore, eppure essere il frutto di un accordo corruttivo che non emerge dai libri contabili. Ciò significa che i tradizionali test sui saldi e sulle transazioni possono risultare inefficaci nella sua rilevazione e per questo motivo sono necessarie ulteriori procedure orientate alla comprensione del contesto e delle dinamiche di business in cui opera l'azienda revisionata.

La categoria meno frequente ma più costosa delle tre sono le false comunicazioni sociali; secondo il Report to the Nations 2024 sono presenti soltanto nel 5% dei casi, ma producono la perdita mediana più elevata: 766.000 dollari per caso. Non si tratta di sottrarre risorse all'organizzazione, ma di alterare la rappresentazione della sua situazione economica, patrimoniale e finanziaria per ingannare i destinatari del bilancio. L'ACFE le definisce schemi in cui un dipendente causa intenzionalmente l'inesattezza o l'omissione

di informazioni materiali nei rendiconti finanziari dell'organizzazione, ad esempio attraverso la registrazione di ricavi fittizi, la sottostima delle spese dichiarate, o la sopravvalutazione artificiale delle attività. Ci sono svariati casi di questa tipologia che hanno segnato l'evoluzione della normativa contabile e di revisione a livello internazionale, tra cui il caso Enron (2001) dove il management fu in grado di presentare bilanci artefatti attraverso l'adozione di tecniche contabili creative, nascondendo perdite e attività tossiche all'interno di entità a destinazione specifica e celando transazioni con parti correlate agli stakeholder rilevanti. Il revisore esterno, Arthur Andersen, non solo non rilevò le irregolarità, ma fu successivamente coinvolto nella vicenda per aver distrutto documenti rilevanti ai fini delle indagini, con conseguenze devastanti (Brickey, 2003).
Sul versante europeo viene individuato come caso importante quello di Parmalat (2003). Lo scandalo portò alla luce un deficit di circa 14 miliardi di euro nei conti della società frutto di frodi, cattiva gestione e del totale fallimento dei meccanismi di controllo. Tra le azioni fraudolente principali si segnala la costituzione di un fondo fittizio negli Stati Uniti, all'interno del quale avrebbero dovuto essere custoditi 5 miliardi di dollari che, nella realtà, si rivelarono del tutto inesistenti (Cambaza, 2024).

In base ai dati riportati nel Report to the Nations 2024, il frodatore non è sempre un criminale di professione, potrebbe essere un lavoratore integrato nell'organizzazione, spesso con una posizione di fiducia consolidata nel tempo. Questo complica la professione del revisore che non può fare affidamento a un profilo di criminale facilmente riconoscibile, poiché nella maggior parte dei casi la frode è commessa da persone che non destano alcun sospetto. Inoltre, viene sottolineato come chi lavora da più tempo in un'organizzazione conosce bene i meccanismi di controllo interno, sa dove si trovano le vulnerabilità del sistema e ha costruito nel tempo un livello di fiducia che riduce la probabilità di essere sottoposto a verifiche stringenti e di conseguenza i dipendenti con maggior anzianità possono causare maggiori danni all'azienda rispetto a chi è entrato da meno tempo. Stessa cosa la si può verificare nel caso di differenza di grado, chi possiede un ruolo gerarchico maggiore causa perdite molte maggiori rispetto ai dipendenti di livello inferiore (Veno, 2024).

La classificazione elaborata dall'ACFE, che considera sia le tre tipologie principali di frode sia chi le commette, costituisce uno strumento operativo di orientamento nella valutazione del rischio da parte del revisore in modo che possa allocare le proprie risorse

e la propria attenzione in modo proporzionale alla natura e all'entità del rischio specifico dell'azienda che sta revisionando. Tuttavia, lascia aperta una domanda di fondo sulle motivazioni per cui si froda, questione a cui i modelli teorici sulla genesi del fenomeno tentano di rispondere a partire dal contributo di Donald Cressey e dal suo triangolo della frode.

1.3 L'evoluzione dei modelli sulla genesi del fenomeno

Tra gli aspetti più rilevanti nello studio delle condotte fraudolente figura la comprensione delle determinanti comportamentali che spingono un individuo a commettere l'illecito, più nello specifico, quali sono le condizioni che rendono possibile e in qualche modo prevedibile una condotta fraudolenta. Intorno alla seconda metà del Novecento si è sviluppata una ricerca di modelli teorici in grado di comprendere il fenomeno, che si è affinata negli anni passando da spiegazioni incentrate sul contesto generale a framework sempre più attenti alle caratteristiche individuali del soggetto agente. I modelli sulla genesi della frode hanno avuto, e continuano ad avere, ricadute sulle metodologie di valutazione del rischio adottate dai revisori e sull'impostazione stessa dei principi di revisione internazionali poi seguiti dai revisori.

Il contributo iniziale da cui prende avvio questa tradizione è quello di Donald R. Cressey, criminologo americano che nel 1953, sulla base di un'ampia ricerca empirica condotta su soggetti condannati per appropriazione indebita, elaborò quello che sarebbe diventato il modello più influente nella storia dello studio della frode occupazionale ''Il triangolo della frode''. Lo studio identifica tre fattori chiave che devono convergere affinché si verifichi una frode: pressione (pressure), opportunità (opportunity) e razionalizzazione (rationalization). Questo modello, derivato dall'analisi di interviste con soggetti che avevano violato posizioni di fiducia, rappresenta ancora oggi il punto di riferimento fondamentale tanto per la ricerca accademica quanto per la pratica professionale.

Il primo fattore chiave è la pressione, definito da Cressey anche come problema finanziario non condivisibile, la quale rappresenta la motivazione che spinge il soggetto verso la condotta illecita. Può essere pressione di natura economica, l'individuo ha dei problemi finanziari che tende a non condividere con gli altri, oppure derivante dal non riuscire a raggiungere degli obiettivi di performance con il timore di perdere il proprio

status o la propria posizione o per soddisfare delle aspettative esterne.
Secondo fattore è l'opportunità, componente strutturale del triangolo che rappresenta la possibilità di risolvere segretamente tali problemi violando una posizione di fiducia. Essa esiste indipendentemente dalla volontà del singolo e dipende dalla presenza di vulnerabilità nei sistemi di controllo interno dell'organizzazione. Può manifestarsi nella forma di una scarsa segregazione dei compiti, di un sistema di autorizzazione non adeguato e lacunoso, di controlli di accesso inefficienti o di una cultura organizzativa che scoraggia le verifiche. Senza un'opportunità concreta, le pressioni e le razionalizzazioni rimangono ininfluenti ai fini della realizzazione della frode.
Infine, terzo fattore è la razionalizzazione, ossia la componente psicologicamente più complessa del modello siccome è impossibile leggere la mente del soggetto. Gli individui che commettono una frode possiedono una particolare disposizione mentale che consente loro di giustificare o scusare le proprie azioni. Molti frodatori, nelle fasi successive alla scoperta, esprimono l'idea di aver agito sapendo che il comportamento era illegale, ma attribuendogli una connotazione diversa da quella di un reato, giustificazioni che consentono al frodatore di mantenere un'immagine positiva di sé pur agendo in modo illecito. Sono particolarmente frequenti nei casi in cui il soggetto non ha precedenti penali e si percepisce come una persona onesta (Roffia et al., 2025).

Il triangolo della frode assume particolare importanza come modello per la valutazione del rischio di frode, ma costituisce solo uno degli elementi di un piano complessivo di valutazione del rischio di revisione. Il modello è stato formalmente recepito nei principi professionali: l'ISA 240 e il suo equivalente americano SAS 99 si fondano esplicitamente sulla logica del triangolo per strutturare le procedure di valutazione del rischio che il revisore deve adottare in fase di pianificazione dell'incarico. Questo dimostra la solidità e l'importanza che ha avuto lo studio di Cressey, il quale a distanza di anni dalla sua elaborazione rimane il fondamento teorico imprescindibile di qualsiasi approccio sistematico alla prevenzione e alla rilevazione della frode.

Nonostante la solidità e la longevità, il triangolo di Cressey è stato oggetto di critiche principalmente per la sua tendenza a focalizzarsi sul contesto in cui la frode avviene e per il fatto che tende a trascurare le caratteristiche individuali del frodatore. Il triangolo della frode cattura la situazione fraudolenta in misura molto maggiore rispetto alla persona, sono presenti la pressione che si concentra sulle sollecitazioni che l'autore

subisce e l’opportunità che riflette la solidità dei controlli nell’organizzazione. Entrambi questi elementi descrivono il contesto e non il soggetto. Per colmare questa lacuna David T. Wolfe e Dana R. Hermanson, nel 2004, proposero sulle pagine del CPA Journal un'estensione del modello originale, introducendo un quarto elemento: la capacità (capability) in quello che viene chiamato ‘’il diamante della frode’’. Questa rappresenta le competenze e le abilità che deve avere il soggetto per commettere la frode, si può parlare di posizioni di autorità nell’azienda che consentano di avere influenza sugli altri e di eludere i controlli, le competenze tecniche che permettono di individuare e sfruttare le debolezze dei sistemi contabili, la capacità di mentire in modo convincente e l'abilità di gestire lo stress derivante dalla condotta illecita senza manifestare segnali di allarme evidenti.

Per illustrare concretamente questo elemento, si consideri un'azienda i cui controlli consentano la possibilità di registrare ricavi prematuramente attraverso la modifica delle date dei contratti di vendita. Questa opportunità di frode diventa un rischio concreto se il CEO dell'azienda, sottoposto a intensa pressione per aumentare le vendite, dispone delle competenze tecniche per comprendere la debolezza del controllo, può costringere il CFO e il responsabile commerciale a manipolare le date, e riesce a mentire ad analisti e al consiglio di amministrazione riguardo alla crescita dell'azienda. Senza un soggetto dotato di tali capacità, la debolezza del controllo resterebbe un'opportunità non sfruttata.
Il contributo del ‘’diamante della frode’’ ha avuto anch’esso un impatto significativo sulla ricerca soprattutto accademica; il suo messaggio centrale, che la frode è prima di tutto un problema di persone e che la capacità del soggetto agente è una variabile determinante quanto le condizioni di contesto, ha trovato ampia conferma anche nei dati empirici dell'ACFE analizzati nel paragrafo precedente, dove si è visto come le frodi più costose siano invariabilmente associate a soggetti con maggiore anzianità e posizioni gerarchiche elevate.

L’evoluzione di questa teoria, tuttavia, non si ferma. Negli anni ulteriori ricerche hanno portato ad un estensione del modello, aggiungendo nuove dimensioni nel tentativo di far emergere aspetti del comportamento fraudolento non individuati negli studi precedenti. Si passa, dai tre elementi di Cressey nel 1953, alle estensioni successive con ‘’il diamante della frode’’ che introduce la capacità, ‘’il pentagono della frode’’ che aggiunge l’arroganza e infine ‘’l’esagono della frode’’ che incorpora la collusione.

Il pentagono della frode, proposto da Crowe Horwath nel 2011, aggiunge al modello del diamante un quinto elemento, l'arroganza. Sottolinea il ruolo della fiducia eccessiva in sé stessi o di un senso di invulnerabilità nel compiere comportamenti illeciti, elemento che si manifesta tipicamente nei soggetti che ricoprono posizioni di potere e che sviluppano la convinzione di essere al di sopra delle regole e delle procedure di controllo, di non poter essere scoperti o che, quand'anche lo fossero, nessuno oserebbe perseguirli. Ciò spiega perché alcune frodi vengono perpetrate in modo quasi sfrontato, con scarsa attenzione all'occultamento, da parte di soggetti che si percepiscono come intoccabili all'interno dell'organizzazione. Dal punto di vista della revisione questo elemento ha implicazioni significative, l'arroganza del management può essere un indicatore della tendenza a ignorare i controlli interni, un fattore di rischio che i principi ISA impongono al revisore di considerare esplicitamente (Barlacu et al., 2025).

A seguito dello studio di Vousinas nel 2019, il modello è stato ulteriormente arricchito da un sesto elemento, la collusione. Questa descrive la cooperazione tra più soggetti, sia interni che esterni all'organizzazione, finalizzata alla realizzazione e all'occultamento della frode. Spesso le frodi più gravi e più difficili da rilevare sono frutto di un'azione coordinata tra più soggetti che coinvolgono anche diversi livelli gerarchici e talvolta anche soggetti esterni.

L'evoluzione dei modelli teorici sulla genesi della frode, dal triangolo all'esagono della frode, riflette un percorso di progressiva complessificazione nella comprensione del fenomeno. Ogni estensione del modello originale ha contribuito a individuare aspetti che il framework precedente lasciava in ombra spostando l'attenzione sulle caratteristiche individuali e relazionali del frodatore. Questo ha implicazioni dirette per il revisore in quanto la valutazione del rischio di frode non può limitarsi all'analisi delle vulnerabilità dei sistemi di controllo interno, ma deve necessariamente tener conto del profilo dei soggetti chiave all'interno dell'organizzazione, delle dinamiche di potere, dei segnali comportamentali e delle pressioni a cui il management è sottoposto. Nonostante la loro importanza i modelli analizzati non sono degli strumenti predittivi in senso assoluto ma risultano importanti per la valutazione del rischio di revisione, offrono una struttura concettuale per organizzare la valutazione del rischio in modo sistematico identificando le aree con maggiore vulnerabilità e calibrando l'intensità delle procedure di revisione in risposta agli allarmi rilevati.

Negli ultimi anni l'interesse si è molto spostato verso strumenti tecnologici in grado di integrare la valutazione qualitativa del revisore con un'analisi quantitativa sistematica dei dati transazionali. I sistemi di intelligenza artificiale e di continuous auditing non sostituiscono il giudizio professionale fondato sui modelli teorici, ma lo integrano con la capacità di elaborare grandi volumi di dati alla ricerca di pattern anomali che potrebbero segnalare la presenza delle condizioni descritte dal triangolo, dal diamante o dai modelli più recenti.

1.4 Le responsabilità del revisore e il principio ISA Italia 240

La figura del revisore legale rappresenta il fulcro dell'analisi sul contrasto alle condotte illecite. Comprendere con precisione quali siano le responsabilità del revisore in materia di frode, e soprattutto quali siano i confini di tali responsabilità, è essenziale per inquadrare correttamente il dibattito sui limiti dell'audit tradizionale e per valutare il contributo che i sistemi tecnologici di nuova generazione possono offrire al rafforzamento della funzione di controllo.

In Italia, la disciplina della revisione legale dei conti è regolata principalmente dal Decreto Legislativo 27 gennaio 2010, n. 39, emanato in attuazione della Direttiva 2006/43/CE relativa alle revisioni legali dei conti annuali e dei conti consolidati. Il decreto ha rappresentato un momento di discontinuità significativa rispetto al quadro normativo preesistente poiché ha raccolto in un unico testo tutte le disposizioni in materia di revisione legale precedentemente frammentate tra il Codice Civile, il Testo Unico della Finanza e le discipline speciali di settore.

Sul versante specifico dello scetticismo professionale, il D.lgs. 39/2010, all'articolo 9, definisce lo scetticismo professionale come un atteggiamento caratterizzato da un approccio dubitativo, dal costante monitoraggio delle condizioni che potrebbero indicare una potenziale inesattezza dovuta a errore o frode, nonché da una valutazione critica della documentazione inerente alla revisione. Questa definizione normativa costituisce il fondamento giuridico su cui si basano i principi di revisione internazionali adottati in Italia, i cosiddetti ISA Italia, che sviluppano i contenuti operativi con un livello di dettaglio maggiore.

Il principio cardine in materia di frode è il principio di revisione internazionale ISA Italia 240, intitolato "Le responsabilità del revisore relativamente alle frodi nella revisione

contabile del bilancio", entrato in vigore per le revisioni dei bilanci relativi ai periodi amministrativi aventi inizio dal 1° gennaio 2015. È il principio di revisione fondamentale che disciplina il ruolo e le responsabilità del revisore nel contesto della possibile presenza di frodi o errori che possano inficiare in modo significativo l'affidabilità del bilancio d'esercizio. Esso non opera in isolamento ma si raccorda con altri principi della famiglia ISA Italia, in particolare con l'ISA Italia 200, che definisce gli obiettivi generali del revisore e il concetto di ragionevole sicurezza, con l'ISA Italia 315, che disciplina l'identificazione e la valutazione dei rischi di errori significativi attraverso la comprensione dell'impresa, e con l'ISA Italia 330, che regolamenta le risposte del revisore ai rischi identificati e valutati.

La prima chiarificazione dell'ISA Italia 240 riguarda la delimitazione delle responsabilità del revisore. Esiste un divario storico, definito come expectation gap, tra ciò che il pubblico si aspetta dal revisore in materia di rilevazione delle frodi e ciò che il revisore è effettivamente tenuto a fare. La responsabilità primaria del revisore non è prevenire o scoprire ogni singola frode, ma ottenere una ragionevole sicurezza che il bilancio nel suo insieme non contenga errori significativi dovuti sia a frodi che a errori. Il concetto di ragionevole sicurezza implica che, a causa delle limitazioni intrinseche della revisione, come la necessità di campionamento e il rischio che le frodi siano abilmente occultate, una sicurezza assoluta non è raggiungibile. La responsabilità primaria per la prevenzione e la rilevazione delle frodi spetta alla direzione aziendale e ai responsabili delle attività di governance, i quali sono tenuti a predisporre sistemi di controllo interno adeguati e a promuovere una cultura organizzativa orientata all'integrità (Peta, 2021).

Nonostante ciò, le responsabilità del revisore in materia di frode non sono affatto trascurabili. Nell'acquisire una ragionevole sicurezza che il bilancio non contenga errori significativi dovuti a frodi, il revisore è responsabile di mantenere lo scetticismo professionale durante tutto il corso della revisione, considerando la possibilità di forzatura dei controlli da parte della direzione e tenendo presente il fatto che le procedure di revisione efficaci nell'individuazione degli errori dovuti a comportamenti o eventi non intenzionali possano essere meno efficaci nell'individuare le frodi (ISA Italia 240). Il revisore non può semplicemente applicare al rischio di frode le stesse procedure che adotta per il rischio di errore, deve sviluppare un approccio specificamente calibrato sulla natura intenzionale e occultata della condotta fraudolenta. In termini operativi, l'ISA Italia

240 richiede al revisore di adempiere a tre categorie principali di obblighi. La prima è l'identificazione e la valutazione dei rischi di errori significativi dovuti a frodi, che deve avvenire attraverso un processo strutturato che comprende indagini presso la direzione, la comprensione delle pressioni a cui l'impresa è soggetta, l'analisi delle opportunità di frode offerte dalle caratteristiche del sistema di controllo interno, e la discussione collegiale all'interno del team di revisione. La seconda è la progettazione e l'esecuzione di procedure di revisione specificamente orientate a rispondere ai rischi di frode identificati, che possono differire sensibilmente dalle procedure standard previste per il rischio di errore. La terza categoria è la gestione adeguata delle frodi identificate o sospettate nel corso della revisione, che include la comunicazione alla direzione e ai responsabili delle attività di governance, e in determinate circostanze la segnalazione alle autorità competenti.

La prescrizione relativa allo scetticismo professionale dell'ISA Italia 240 è la più importante e difficile da applicare nella pratica. Il revisore deve mantenere lo scetticismo professionale per tutta la durata della revisione, tenendo presente la possibilità che un errore significativo dovuto a frodi possa comunque sussistere, a prescindere dall'esperienza precedentemente acquisita circa l'onestà e l'integrità della direzione dell'impresa e dei responsabili delle attività di governance.

Nella pratica lo scetticismo professionale si manifesta in una serie di comportamenti concreti. Il revisore oltre a svolgere un'analisi della documentazione, deve agire operativamente attraverso tutte le fasi della revisione. Nel momento in cui emergono informazioni incoerenti, in particolare se confrontate con quelle provenienti da fonti esterne, il revisore ha l'obbligo di indagarne le cause, evitando di accettare superficialmente quanto dichiarato dalla direzione. Questo implica interrogarsi sistematicamente sulla coerenza interna delle informazioni ricevute, sulla plausibilità delle spiegazioni fornite dal management, sulla solidità degli elementi probativi acquisiti e sulla loro capacità di reggere a un esame critico. Lo scetticismo professionale non va confuso con una presunzione di disonestà nei confronti del management, si tratta piuttosto di un approccio mentale che consente al revisore di mantenere un'apertura critica alle evidenze, evitando sia l'eccesso di fiducia sia l'eccesso di sospetto.

Un aspetto di particolare rilievo, su cui l'ISA Italia 240 pone attenzione specifica, riguarda il rischio di management override, ovvero, la possibilità che i vertici aziendali

neutralizzino o eludano i controlli interni facendo leva sulla propria posizione di autorità. Questo rischio è considerato dal principio una minaccia presente in qualsiasi revisione, indipendentemente dalla valutazione complessiva del sistema di controllo interno dell'azienda. Il revisore è pertanto tenuto ad adottare procedure specificamente volte a identificare eventuali forzature dei controlli da parte della direzione, anche in presenza di un sistema di controllo interno formalmente adeguato.

La disciplina dello scetticismo professionale delineata dall'ISA Italia 240 rappresenta molto più di una prescrizione tecnica, essa è l'espressione di una consapevolezza profonda che il revisore non può limitarsi a verificare la conformità formale delle scritture contabili, ma deve mantenere in ogni momento una disposizione mentale critica e attiva, capace di interrogarsi sulla plausibilità di ciò che gli viene presentato e di riconoscere i segnali di una possibile condotta fraudolenta. Tuttavia, tra le prescrizioni del principio e la realtà operativa della revisione esiste uno scarto significativo. Lo scetticismo professionale è un atteggiamento mentale, e come tale è soggetto a tutte le pressioni cognitive e relazionali che caratterizzano il lavoro del revisore nella pratica quotidiana come possono essere la familiarità che viene maturata nel tempo col cliente o la pressione sui tempi e i costi per svolgere l'incarico o il timore di mettere in discussione affermazioni del management che non si è in grado di dimostrare con prove concrete. Questi fattori non annullano il valore del principio, ma ne limitano l'efficacia applicativa. Da queste considerazioni nasce la necessità di una riflessione riguardante i limiti metodologici dell'audit tradizionale in modo tale da comprendere le motivazioni per cui risulta necessario valutare i nuovi elementi tecnologici, i quali possono aiutare a colmare questo gap integrando il giudizio professionale del revisore con capacità analitiche più avanzate.

1.5 I limiti dell'audit tradizionale

Nonostante un impianto normativo così articolato e una letteratura teorica così sviluppata, sono molte le frodi che continuano a non essere rilevate tempestivamente attraverso i canali tradizionali della revisione esterna. Molte delle frodi vengono scoperte per delle segnalazioni informali, piuttosto che tramite la revisione esterna, e questo non è dovuto alla negligenza dei revisori o del loro scarso impegno, bensì a limiti strutturali e metodologici che caratterizzano il modello classico di audit. Tali criticità vengono

analizzate in modo sistematico articolandoli in quattro direttrici principali: il limite del campionamento, il limite della periodicità e dell'approccio ex-post, il limite cognitivo connesso all'esercizio dello scetticismo professionale e il problema strutturale dell'expectation gap. La comprensione di questi limiti è il presupposto necessario per valutare in modo fondato le potenzialità e i rischi dell'intelligenza artificiale.

Il fondamento metodologico dell'audit tradizionale è il campionamento. Il campionamento risponde all'impossibilità oggettiva di esaminare la totalità delle transazioni registrate dell'azienda per una questione di tempi e costi; per questo il revisore ne seleziona, tramite svariati metodi possibili, un sottoinsieme rappresentativo su cui applicare le procedure di verifica. Dopo aver svolto le procedura sul campione selezionato, vengono estese al resto della popolazione di riferimento le conclusioni tratte sul sottoinsieme, escluse quelle riguardanti le anomalie. Questo approccio è razionale ed economicamente giustificato siccome un'analisi della totalità delle transazioni richiederebbe risorse e tempi incompatibili con costi e durata dell'incarico di revisione. Tuttavia, questa necessità pratica introduce il rischio di campionamento (sampling risk), ovvero la possibilità che le conclusioni tratte dal team di audit sulla base del sottoinsieme selezionato differiscano da quelle che si sarebbero ottenute esaminando l'intera popolazione contabile. Il rischio di individuazione (detection risk) si scompone in due componenti: il rischio non derivante da campionamento (non-sampling risk), legato a errori di valutazione del professionista o a falsificazioni documentali complesse, e il rischio di campionamento. Quest'ultimo è un rischio strutturale intrinseco all'approccio ex-post tradizionale; l'unico modo per azzerarlo completamente consiste nell'estensione delle procedure di verifica alla totalità delle transazioni. È precisamente in questo spazio metodologico che si innesta il contributo delle nuove tecnologie di data analytics, capaci di eliminare il sampling risk attraverso il testing massivo dei database aziendali.

Le procedure di audit standard volte a raccogliere prove di revisione possono rivelarsi inefficaci per rilevare un errore intenzionale che preveda, ad esempio, la collusione tra membri del management, dipendenti dell'azienda o soggetti esterni come possono essere clienti e fornitori finalizzati alla falsificazione della documentazione al punto da indurre il team di revisione a ritenere valide prove che non lo sono. Il campionamento porta ad analizzare parte delle registrazioni della società però non rileva comportamenti fraudolenti deliberatamente concentrati in aree specifiche, oppure

occultati attraverso tecniche di falsificazione documentale che rendono le singole operazioni apparentemente conformi agli standard attesi. La capacità del revisore di rilevare frodi nei bilanci dipende in misura significativa dalla sua abilità di identificare segnali di rischio nell'ambito delle procedure di pianificazione (Hogan et al., 2008). La selezione dei campioni è spesso guidata da criteri di significatività monetaria e di rischio delle registrazioni, per questo le transazioni di importo modesto hanno meno probabilità di essere estratte nel campione nonostante la possibilità che siano fraudolente. L'utilizzo di strumenti di analisi dei dati di audit può migliorare la qualità e l'efficienza della revisione attraverso una più efficace identificazione di transazioni o pattern inusuali nei dati finanziari e attraverso test più completi e approfonditi di intere popolazioni di dati, piuttosto che facendo affidamento su metodi di campionamento. Questo risulta uno degli argomenti più validi per chi sostiene l'introduzione di tecnologie di analisi massiva dei dati nell'ambito della revisione.

Il secondo limite strutturale dell'audit tradizionale è di natura temporale. La revisione legale del bilancio è un processo periodico che si concentra in un periodo definito dell'anno, al termine dell'esercizio o in prossimità della data di approvazione del bilancio, e produce un giudizio che riguarda un arco temporale passato. L'approccio ex-post implica che quando una frode viene rilevata dal revisore è quasi certamente già in corso da svariati mesi se non da anni. Il revisore raccoglie evidenze, verifica i controlli e riporta i risultati settimane o mesi dopo che gli eventi si sono verificati. Quanto più a lungo una frode persiste prima di essere scoperta, tanto maggiore è il danno che produce. I frodatori sono pienamente consapevoli della periodicità dei controlli a cui sono sottoposti consentendogli di modulare la propria condotta in funzione della revisione concentrando le operazioni fraudolente nei periodi in cui la sorveglianza è meno intensa, normalizzare le poste contestate in prossimità della chiusura dell'esercizio, e riprendere la condotta illecita una volta superato il momento di maggiore attenzione.

È possibile riscontrare un terzo limite di natura cognitiva già introdotto nel capitolo precedente, lo scetticismo professionale. L'esercizio dello scetticismo professionale è ostacolato da vari meccanismi organizzativi che la letteratura ha ampiamente documentato, il primo di questi è il cosiddetto confirmation bias, la tendenza naturale degli individui a cercare e ricordare le informazioni in modo da confermare le proprie convinzioni precedenti. Quando un revisore ha maturato negli anni una valutazione

positiva del management di un cliente, il confirmation bias lo induce inconsciamente a interpretare i segnali ambigui in modo favorevole, a dare peso sproporzionato alle evidenze che confermano la propria percezione di affidabilità del cliente, e a sottovalutare o ignorare gli indicatori che potrebbero suggerire una condotta fraudolenta. L'economista Hammersley nel 2011 ha identificato il confirmation bias come uno dei principali ostacoli cognitivi all'esercizio efficace dello scetticismo professionale, sottolineando che esso è particolarmente pericoloso proprio perché il revisore non ne è consapevole.

Un secondo meccanismo critico è quello della pressione relazionale e commerciale dovuta al fatto che il revisore opera in un contesto in cui il cliente è anche colui che corrisponde il compenso professionale e che può decidere di revocare l'incarico. Come conseguenza è stato provato che i revisori tendono ad essere più scettici verso i clienti che rappresentano una quota minore dei loro ricavi, e meno scettici, inconsapevolmente, verso i clienti più importanti. Questa dinamica non implica necessariamente comportamenti scorretti in senso pieno, ma introduce una distorsione sistematica nello scetticismo che può avere effetti rilevanti sulla qualità del giudizio professionale.

Si può citare come elemento limitante anche il rischio di familiarity bias per cui si ha tendenza a fidarsi delle persone che si conoscono da lungo tempo. La professione dell'audit tipicamente minimizza l'importanza del proprio ruolo nella rilevazione delle frodi e continua a sottolineare il ruolo del management in modo da avere meno responsabilità legali nel caso in cui sorgano ed evitare eventuali richieste di risarcimento. È stato evidenziato come il ruolo dell'audit interno nella rilevazione delle frodi risulta maggiormente efficace con l'utilizzo di approcci tecnologici per l'identificazione dei rischi. Questi studi suggeriscono che gli strumenti tecnologici possono contribuire a ridurre l'influenza dei bias cognitivi offrendo al revisore segnali oggettivi e quantitativamente fondati su cui focalizzare la propria attenzione.

Ultimo limite da considerare, più di natura sociale e istituzionale, riguarda il cosiddetto audit expectation gap. Questo è il divario tra ciò che il pubblico si aspetta dalla revisione in materia di rilevazione delle frodi e ciò che la revisione è effettivamente in grado di offrire, concetto introdotto da Liggio nel 1974 e approfondito negli anni da Porter nel 1993. Come detto precedentemente, il revisore tende a minimizzare l'importanza del suo ruolo nelle individuazioni della frode sottolineando il ruolo dei manager, ma uno studio sulle cause dei fallimenti aziendali ha mostrato che il ruolo dei revisori viene messo in

discussione con frequenza molto maggiore quando il fallimento è collegato a frodi commesse da dipendenti o dal management.

L'audit expectation gap riflette una netta divergenza di prospettive tra gli obblighi normativi della professione e le aspettative del mercato. La logica economico-giuridica che governa la revisione legale impone al professionista il raggiungimento di una ragionevole sicurezza circa l'assenza di errori significativi, escludendo il rilascio di una garanzia assoluta in merito all'inesistenza di frodi. Al contrario, l'opinione pubblica, gli investitori e gli stakeholder tendono a percepire la firma della relazione di audit come una certificazione totale di integrità aziendale. Tale scollamento genera un'asimmetria informativa penalizzante per la reputazione del settore, spingendo i regolatori a interventi normativi mirati a ridefinire il perimetro delle responsabilità del controllo esterno (Akther, 2020). Storicamente, gli interventi del legislatore si sono concentrati sulla maggior richiesta di scetticismo professionale e sull'ampliamento degli obblighi di documentazione in capo al team di verifica. Questo approccio reattivo non risolve il limite intrinseco delle metodologie tradizionali: un modello di controllo ex-post e basato su verifiche campionarie periodiche fatica a intercettare le frodi contabili più complesse.

I limiti dell'audit tradizionale non sono superabili solo attraverso campioni più ampi, procedure più accurate, scetticismo più rigido, ma richiedono un ripensamento più profondo delle metodologie e degli strumenti a disposizione del revisore. I progressi tecnologici non solo migliorano l'efficienza dell'audit interno, ma amplificano anche l'efficacia, specialmente nel contesto della rilevazione delle frodi. Le tecniche di audit analytics e data mining sono strumenti essenziali per allocare le risorse in modo efficace e ridurre il rischio di frode interna in un'azienda. Il continuous auditing porta numerosi benefici tra cui riduzione dei rischi, diminuzione dei tentativi di frode, consente un accesso tempestivo alle informazioni, supporta la revisione esterna, consente aggiustamenti tempestivi e modifica i compiti di routine dei revisori, permettendo loro di concentrarsi su responsabilità più importanti.

È in questo spazio che possono collocarsi i sistemi di intelligenza artificiale e continuous auditing che sono il tema principale dell’analisi successiva. Si tratta di strumenti che, se correttamente integrati nel processo di revisione, possono contribuire ad affrontare sistematicamente i limiti del campionamento attraverso l'analisi dell'intera popolazione di transazioni, a ridurre il ritardo nella rilevazione delle anomalie attraverso

il monitoraggio in tempo reale, e a supportare l'esercizio dello scetticismo professionale attraverso la produzione di segnali oggettivi e quantitativamente fondati.

1.6 L'intelligenza artificiale come risposta ai limiti dell'audit

Gli approcci incrementali al modello esistente, quali l'estensione a campioni più ampi, l'adozione di procedure più accurate o l'esercizio di uno scetticismo più rigido, si rivelano parziali nel colmare il divario tra le aspettative di controllo che la società ripone nella revisione e le capacità effettive dell'audit periodico e campionario. È in questo spazio che si inserisce il contributo dell'intelligenza artificiale.

Con il termine intelligenza artificiale, nel contesto della revisione contabile, si intende un insieme eterogeneo di tecnologie e metodologie computazionali che consentono ai sistemi informatici di apprendere da grandi volumi di dati, riconoscere pattern complessi e produrre previsioni o segnalazioni senza essere esplicitamente programmati per farlo. Questa definizione comprende strumenti tra loro distinti, come gli algoritmi di machine learning applicati all'analisi dei dati quantitativi di bilancio, i modelli di natural language processing orientati all'analisi testuale delle comunicazioni aziendali e i sistemi di continuous auditing basati sul monitoraggio in tempo reale delle transazioni. Tali strumenti condividono la capacità di elaborare informazioni su larga scala con una velocità inaccessibile al controllo umano tradizionale. Non si tratta di una tecnologia unitaria, ma di un ecosistema di soluzioni che la letteratura recente ha cominciato ad applicare sistematicamente alla revisione contabile proprio in risposta ai limiti descritti nel paragrafo precedente.

Il collegamento tra le criticità strutturali dell'audit tradizionale e le potenzialità dell'IA è un tema sempre in maggiore evoluzione. Laddove il campionamento periodico lascia non analizzata la grande maggioranza delle transazioni, i sistemi di continuous auditing consentono di monitorarle interamente e in tempo reale. Inoltre, se lo scetticismo professionale è soggetto a bias cognitivi e pressioni relazionali, gli algoritmi possono produrre segnalazioni oggettive e indipendenti dal giudizio del singolo professionista. Infine, poiché la frode si manifesta spesso attraverso anomalie sottili distribuite su grandi volumi di dati, il machine learning risulta progettato esattamente per intercettare tali configurazioni. Questa corrispondenza tra problemi e soluzioni non significa che l'intelligenza artificiale azzeri ogni limite dell'audit tradizionale; essa introduce a sua volta

rischi e limitazioni proprie, ma spiega perché l'interesse della ricerca e della pratica professionale verso questi strumenti sia cresciuto in modo così rapido negli ultimi anni.

La trattazione successiva si propone di approfondire queste dinamiche: il terzo capitolo analizzerà nel dettaglio ciascuno di questi strumenti, documentandone l'efficacia empirica nella rilevazione delle diverse tipologie di frode e discutendone i limiti applicativi, mentre il quarto capitolo si occuperà delle implicazioni che la loro adozione produce sul ruolo del revisore, sullo scetticismo professionale e sul quadro normativo internazionale.

II. Il metodo e il protocollo della rassegna della letteratura

2.1 Gli obiettivi della rassegna della letteratura

L'obiettivo del presente lavoro di ricerca consiste nel ricostruire e sintetizzare lo stato degli studi su un tema in forte evoluzione, ovvero l'applicazione dell'intelligenza artificiale e del continuous auditing alla rilevazione delle frodi contabili, al fine di trarne indicazioni utili sia per la prassi professionale che per la ricerca futura. Per questa ragione l'indagine si sviluppa attraverso una narrative review. Questo approccio si rivela idoneo a esplorare campi di studio caratterizzati da una rapida accelerazione tecnologica, in cui la produzione scientifica appare frammentata tra contributi accademici, documenti professionali e linee guida normative di natura eterogenea, e in cui l'adozione di criteri di inclusione ed esclusione eccessivamente rigidi rischierebbe di escludere i contributi più recenti e innovativi. La selezione delle fonti avviene comunque secondo criteri espliciti e documentati, illustrati nei paragrafi che seguono, in modo che ogni scelta sia tracciabile e giustificabile.

La narrative review si caratterizza per la facoltà attribuita al ricercatore di esercitare un alto grado di giudizio interpretativo nella selezione, organizzazione e sintesi concettuale delle fonti, privilegiando la costruzione di un'argomentazione coerente rispetto alla copertura necessariamente esaustiva della letteratura esistente. Tale approccio risponde a specifiche esigenze conoscitive, configurandosi come lo strumento d'elezione nel caso in cui il campo d'indagine si presenti frammentato tra domini scientifici differenti, la letteratura sia ancora in fase di consolidamento e l'obiettivo primario sia la strutturazione di un percorso logico capace di collegare filoni tra loro distanti (Snyder, 2019). A differenza della systematic literature review, che segue protocolli rigidi e non modificabili impostati a priori su quesiti fortemente circoscritti con l'obiettivo di mappare in modo esaustivo tutti i contributi disponibili, la narrative review permette di gestire l'intersezione tra ambiti disciplinari eterogenei senza produrre risultanze atomistiche o penalizzare la comprensione complessiva del fenomeno indagato (Torraco, 2016).

Nel presente elaborato il tema dell'intelligenza artificiale volta all'individuazione della frode contabile si colloca tra tre ambiti disciplinari distinti, ciascuno con le proprie riviste di riferimento, i propri standard metodologici e i propri tempi di pubblicazione: la letteratura economico-aziendale di accounting e auditing, la letteratura di data science e

machine learning, e l'ambito più recente giuridico-istituzionale dedicato alla regolamentazione e alla compliance dei sistemi automatizzati.
L'applicazione di un protocollo sistematico rigido, come la systematic review, a un campo così eterogeneo comporterebbe il rischio di produrre risultati frammentati o di restringere artificialmente il perimetro dell'indagine, escludendo contributi di rilievo provenienti da tradizioni di studio differenti. La narrative review permette invece di preservare l'eterogeneità di tali contributi, traducendoli in un quadro d'insieme volto a valutare criticamente l'impatto delle tecnologie sulla professione e sul quadro normativo.

A tali considerazioni si aggiunge un vincolo legato alla rapidità dell'evoluzione tecnologica in corso. Come evidenziato dall'analisi della distribuzione temporale degli articoli inclusi nella rassegna (Tabella 2.3), più della metà dei contributi rilevanti si concentra nell'ultimo biennio, con una parte significativa dei paper che si trova ancora in fase di prima diffusione al momento della redazione di questa tesi. La narrative review garantisce la necessaria flessibilità metodologica utile a incorporare le evidenze scientifiche più recenti man mano che si consolidano nei canali ufficiali, mantenendo il rigore di un impianto esplicito e tracciabile.

2.2 La selezione delle fonti e la raccolta dei dati

La fase di raccolta della letteratura scientifica si sviluppa attraverso la consultazione combinata di tre banche dati accademiche: Scopus, Google Scholar e Web of Science. Il motore di ricerca principale è stato Scopus, sul quale è stata applicata la stringa di estrazione. Gli altri due database hanno svolto una funzione integrativa e di controllo, la loro consultazione, successiva all'estrazione primaria, mira a intercettare eventuali contributi rilevanti, working paper o pubblicazioni minori non individuati da Scopus, con l'obiettivo di ridurre il rischio di publication bias e ampliare la completezza del corpus documentale.

Il punto di partenza è stata la costruzione di una stringa di ricerca in grado di catturare contemporaneamente i tre ambiti tematici della tesi: il processo di audit, le tecnologie applicate alla revisione e il fenomeno della frode contabile. Ciascuno dei tre raggruppamenti di parole chiave intercetta una tradizione dottrinale distinta, riconducibile rispettivamente ai filoni dell'auditing aziendale, della data science e, infine, agli studi più recenti in materia di criminologia economica e compliance organizzativa. La stringa di

ricerca combina queste matrici eterogenee, con l'obiettivo di strutturare un corpus documentale unitario, capace di far dialogare prospettive e metodologie disciplinari diverse; le parole chiave sono state organizzate in tre gruppi, combinati mediante gli operatori booleani OR e AND.

Tabella 2.1 – Keywords usate per la ricerca

Processo di audit	Ambito tecnologico	Frode
Audit	Artificial intelligence	Corporate fraud
External audit	IA / AI	Fraud
Internal audit	Continuous auditing	Accounting anomalies
Professional skepticism	Automation	Accounting fraud
Automation bias	Machine learning	Violation
Audit quality	Data analytics	Deviance
Auditor judgment	Digital Audit	Deviant
Auditor judgement		Irregularities
		Criminal

La stringa di ricerca completa utilizzata per la ricerca su Scopus è la seguente:

("Audit" OR "External Audit" OR "Internal Audit" OR "Professional Skepticism" OR "Automation Bias" OR "Audit Quality" OR "Auditor Judgment" OR "Auditor Judgement") AND ("Artificial Intelligence" OR "AI" OR "IA" OR "Continuous Auditing" OR "Automation" OR "Machine Learning" OR "Data Analytics" OR "Big Data") AND ("Corporate Fraud" OR "Fraud" OR "Accounting Anomalies" OR "Accounting Fraud" OR "Financial Statement Fraud" OR "Violation" OR "Deviance" OR "Crime")

L'applicazione di questa stringa ha prodotto inizialmente 711 risultati. A seguito di un primo filtro per aree disciplinari, con cui sono state escluse le aree prettamente tecniche come ingegneria dei sistemi, informatica applicata e scienze naturali, il numero di articoli è diminuito a 655, che costituiscono la popolazione di partenza dell'estrazione.
Della popolazione iniziale di 655 contributi, la selezione finale è avvenuta applicando cinque criteri di esclusione, definiti prima dell'avvio della classificazione sistematica del materiale e applicati in modo coerente a ciascun articolo: pertinenza tematica, finestra temporale, soglia minima di citazioni, qualità e natura della fonte, non sovrapposizione

con temi del capitolo 1.

Il primo criterio riguarda la pertinenza tematica. Sono stati esclusi gli articoli che, pur contenendo nel titolo o nell'abstract parole chiave pertinenti, trattavano il tema della frode o dell'intelligenza artificiale in contesti del tutto distanti da quello della revisione contabile. Rientrano in questa categoria, ad esempio, i paper sulla rilevazione delle frodi nelle reti elettriche, sulla sorveglianza dei sussidi governativi o sull'uso dell'AI nei sistemi di polizia predittiva, ambiti in cui i termini "audit" e "fraud" vengono utilizzati in accezioni radicalmente diverse da quelle proprie delle discipline economico-aziendali.

Sotto il profilo cronologico, la finestra temporale definita si concentra sulla letteratura pubblicata a partire dal 2023. Questa delimitazione rappresenta un punto di discontinuità significativo nella letteratura specialistica, coincidente con la diffusione su larga scala dei modelli linguistici di grandi dimensioni (LLM) e con l'accelerazione nell'adozione di strumenti di intelligenza artificiale nella prassi professionale. A questa regola fanno eccezione alcuni contributi antecedenti al 2023 considerati utili per l'evoluzione del settore, come lo studio di Vasarhelyi e Halper (1991) sul continuous auditing, il lavoro di Kim et al. (2021) sull'applicazione del Machine Learning per il rilevamento di errori nei bilanci, o i contributi di Rezaee e Wang (2019) sul fintech applicato alla revisione.

Successivamente sono stati considerati articoli con una soglia minima di citazioni, utilizzata come indicatore approssimativo della validazione scientifica da parte della comunità accademica. Per non penalizzare i contributi più recenti, la soglia è stata calibrata dinamicamente in funzione dell'anno di pubblicazione: almeno 20 citazioni per gli articoli del 2023, almeno 8 per il 2024, almeno 3 per il 2025, azzerando il requisito minimo per i paper del 2026 data la loro recentissima immissione.

Riguardo alla qualità e alla natura della fonte, è stata data preferenza ad articoli pubblicati su riviste peer-reviewed indicizzate. I conference paper e i book chapter sono stati ammessi esclusivamente laddove il contenuto risultasse direttamente pertinente, mentre i documenti classificati come "note" o "conference review" sono stati esclusi.

L'ultimo criterio ha infine risposto all'esigenza di non sovrapposizione con il quadro teorico del Capitolo 1. Di conseguenza, i paper incentrati esclusivamente su concetti tradizionali e tassonomie consolidate, come le definizioni generali di frode, le metriche ACFE o il triangolo di Cressey, sono stati scartati per evitare duplicazioni, a meno che non introducessero qualcosa di nuovo rispetto a quanto già trattato.

Il processo di classificazione si sviluppa attraverso l'analisi individuale di ciascun articolo estratto, registrando lo status di inclusione o esclusione e la relativa motivazione. La tabella seguente riassume l'esito del processo di scrematura:

Tabella 2.2 – Risultati del processo di selezione della letteratura

Fase del processo	**N. articoli**
Articoli estratti da Scopus (stringa completa)	711
Dopo filtro per aree disciplinari	655
Esclusi per filtro temporale (pre-2023)	233
Esclusi per soglia citazioni non raggiunta	214
Esclusi per rivista informatica/ingegneristica	97
Esclusi perché già trattati nel capitolo 1	40
Esclusi per tipo documento non ammesso	4
Esclusi per non pertinenza tematica	25
Articoli inclusi nella rassegna finale	**42**

Gli articoli inclusi nella rassegna presentano caratteristiche eterogenee in termini di anno di pubblicazione, tipo di documento e approccio metodologico adottato, varietà che riflette la natura multidisciplinare e in rapida evoluzione del campo di ricerca.
La tabella seguente illustra la distribuzione degli articoli inclusi per anno di pubblicazione.

Tabella 2.3 – Distribuzione degli articoli inclusi per anno di pubblicazione

Anno	**N. articoli inclusi**	**% sul totale**
Pre 2023 (inclusi come eccezioni)	5	~12%
2023	4	~10%
2024	9	~21%
2025	10	~24%
2026	14	~33%
Totale	**42**	**100%**

La concentrazione degli articoli negli anni 2025 e 2026 riflette l'accelerazione della produzione scientifica sul tema dell'intelligenza artificiale applicata all'audit, conseguente alla diffusione dei modelli linguistici di grandi dimensioni. Questa concentrazione impone una certa cautela interpretativa in quanto gli articoli più recenti non hanno ancora beneficiato del processo di validazione cumulativa che caratterizza i contributi con un numero elevato di citazioni. Il loro peso nella rassegna è stato ponderato di conseguenza.

2.3 L'analisi delle fonti selezionate

La classificazione cronologica e l'applicazione dei criteri di selezione non esauriscono l'esame critico del materiale documentale raccolto. Al fine di comprendere appieno la composizione della letteratura posta a fondamento del presente elaborato, gli articoli inclusi sono stati ulteriormente classificati secondo due dimensioni aggiuntive: la tipologia metodologica del contributo e, per gli studi empirici, il contesto geografico all'interno del quale si sviluppa la ricerca.

Per quanto riguarda la tipologia metodologica, ciascun articolo viene ricondotto a una di cinque categorie fondamentali, individuate per mappare l'eterogeneità delle fonti. La prima classe accoglie i contributi di natura empirico-quantitativa, caratterizzati dal testing di modelli predittivi o algoritmi di machine learning applicati a dataset contabili strutturati, spesso estratti da grandi database finanziari globali o archivi sanzionatori istituzionali. Ad essi si affiancano gli studi empirico-qualitativi, in cui l'evidenza sul campo si sviluppa tramite interviste strutturate, analisi di casi aziendali o mappature di processo all'interno delle società di revisione. Una terza categoria raccoglie le rassegne sistematiche della letteratura, volte a sintetizzare la produzione scientifica precedente secondo un protocollo esplicito e dichiarato. I contributi teorico-concettuali includono invece quegli articoli focalizzati sullo sviluppo di framework interpretativi, riflessioni metodologiche o posizioni dottrinali prive di una diretta componente empirica. Infine, l'analisi isola i report di matrice prettamente pratica e professionale, orientati alla operatività degli strumenti tecnologici piuttosto che alla ricerca accademica.

Tabella 2.4 – Distribuzione degli articoli inclusi per tipologia e capitolo di destinazione

Tipologia	Capitolo 3	Capitolo 4	Totale	% sul totale
Empirico Quantitativo	13	14	27	64,3%
Empirico Qualitativo	2	3	5	11,9%
Rassegna Sistematica	1	1	2	4,8%
Teorico-Concettuale	1	6	7	16,7%
Report/Pratico	1	0	1	2,4%
Totale	**18**	**24**	**42**	**100%**

Il dato più rilevante che emerge è la netta prevalenza dei contributi empirico-quantitativi, i quali rappresentano quasi due terzi dell'intera rassegna (64,3%). Questa concentrazione risponde alla natura della letteratura scientifica focalizzata su intelligenza artificiale e rilevazione delle frodi, sviluppata in larga misura attorno alla validazione sul campo di modelli predittivi e architetture algoritmiche applicati a flussi transazionali, evidenze documentali ed estrazioni di bilancio. Si delinea quindi un campo di ricerca giovane ma già fortemente orientato alla verifica quantitativa e alla misurazione empirica delle proprie ipotesi conoscitive, più che alla pura riflessione teorico-astratta. La distribuzione del materiale all'interno della tesi conferma questa lettura. Il terzo capitolo, dedicato agli strumenti tecnologici di rilevazione, si fonda quasi interamente su contributi empirici quantitativi (13 articoli su 18), in linea con l'obiettivo di documentare l'efficacia misurata degli algoritmi. Il quarto, incentrato sulle implicazioni professionali e normative, presenta invece una componente teorico-concettuale molto più sostanziale (6 articoli su 24, pari a un quarto del totale) accanto a quella empirica. Si tratta di un equilibrio coerente con la natura dei temi trattati, in cui questioni come l'automation bias e il quadro regolatorio richiedono sia evidenze sul campo sia un'elaborazione concettuale e normativa.

La classificazione geografica riguarda i soli contributi empirici: i restanti 10 articoli, trattandosi di rassegne sistematiche o studi teorico-concettuali, analizzano modelli astratti o sintetizzano la produzione scientifica globale, risultando privi di un focus territoriale specifico. Al contrario, i 32 articoli di matrice empirica si basano necessariamente su dati raccolti sul campo, come l'estrazione di bilanci da mercati

finanziari regolamentati o interviste a professionisti inseriti in determinati contesti nazionali. Questa analisi risulta particolarmente rilevante per il presente studio, poiché consente di verificare in che misura la letteratura empirica disponibile rispecchi contesti regolatori e di mercato comparabili a quello italiano ed europeo.

Tabella 2.5 – Contesto geografico degli studi empirici

Contesto	N. articoli	% sul totale studi empirici
Globale (multi-paese)	11	34,4%
USA	8	25,0%
Asia	7	21,9%
Europa	5	15,6%
Africa	1	3,1%
Totale	**32**	**100%**

I dati confermano un'asimmetria significativa: gli studi condotti specificamente in ambiti europei rappresentano meno di un sesto della letteratura empirica selezionata (15,6%), mentre le ricerche focalizzate su mercati statunitensi o asiatici, sommate, superano da sole quasi la metà del campione (46,9%). Nessuno degli articoli inclusi adotta un campione incentrato sulla realtà italiana. Questa sproporzione rispecchia una caratteristica strutturale della letteratura disponibile, riconducibile alla maggiore disponibilità di dataset pubblici, in particolare quelli della SEC statunitense, e alla maggiore maturità del mercato nordamericano nell'adozione di strumenti di intelligenza artificiale in ambito di revisione.

Questo squilibrio geografico ha una conseguenza diretta sull'impianto argomentativo dell'intero lavoro. La validità dei modelli di machine learning addestrati su dataset di società quotate statunitensi non può essere data per scontata in un contesto come quello italiano, caratterizzato da una netta prevalenza di piccole e medie imprese, da principi contabili nazionali (OIC) affiancati a quelli internazionali e da una struttura del mercato della revisione sostanzialmente diversa da quella americana. La scarsità di letteratura empirica europea, unita all'assenza pressoché totale di studi italiani, rappresenta quindi non solo un dato descrittivo della rassegna, ma un argomento centrale a sostegno della

cautela interpretativa che viene adottata nel valutare la trasferibilità dei risultati discussi al contesto nazionale.

Alcuni dei contributi inclusi giungono a conclusioni in apparente tensione tra loro. È il caso, ad esempio, dello studio di Seethamraju e Hecimovic (2023), che documenta una riduzione significativa dello scetticismo professionale tra i revisori che utilizzano l'intelligenza artificiale in modo intensivo, e di quello di Vitali e Giuliani (2024), che rileva invece una relazione positiva tra l'adozione dell'IA e lo scetticismo, seppur moderata dai tratti individuali del professionista. Anziché privilegiare a priori un singolo risultato, la rassegna sceglie di presentare entrambe le evidenze, trattandole come espressione della complessità del fenomeno piuttosto che come un conflitto da risolvere. L'impatto dell'innovazione tecnologica e dell'automation bias appare condizionato da variabili individuali e organizzative che la letteratura cerca ancora di isolare con precisione; l'analisi riflette pertanto tale incertezza, evitando di appiattirla su una conclusione univoca.

Vale la pena soffermarsi anche sulla natura editoriale delle fonti. Gli articoli inclusi vengono ripartiti in cinque macroaree: le riviste storiche di accounting e auditing, le riviste focalizzate sull'intelligenza artificiale e la tecnologia applicata alla finanza, i contributi dedicati all'etica e alla regolamentazione giuridica dell'IA, i report emessi da organismi professionali e, infine, le pubblicazioni di natura prevalentemente interdisciplinare. La quasi totalità di essi proviene da riviste accademiche peer-reviewed indicizzate in Scopus. La tabella seguente riporta le testate scientifiche più ricorrenti all'interno del corpus documentale:

Tabella 2.6 – Distribuzione degli articoli per area disciplinare della rivista

Area disciplinare	Riviste rappresentative	N. articoli
Accounting e auditing	Journal of Accounting Research, Journal of Accounting Literature, Auditing: A Journal of Practice & Theory, Contemporary Accounting Research	12
IA, data science e tecnologia applicata	Intelligent Systems in Accounting Finance and Management, International Journal of Accounting Information Systems, Journal of Risk and Financial Management	14

Area disciplinare	Riviste rappresentative	N. articoli
Etica, diritto e regolamentazione dell'IA	AI & Society, Scientific African, Audit Financiar	8
Report e fonti professionali	ISACA Journal, ACFE Report to the Nations	4
Altro (riviste interdisciplinari)	Varie	4
Totale		**42**

Oltre la metà dell'intero corpus documentale (26 articoli su 42) si concentra all'interno dei primi due macro-ambiti, confermando un forte legame tra la ricerca contabile tradizionale e la sua evoluzione in chiave tecnologica. La presenza di 8 contributi focalizzati sulla regolamentazione e sull'etica dell'IA testimonia la recente ma rapida espansione del dibattito normativo, elemento centrale per comprendere l'attuale contesto di compliance in cui si muove la professione del revisore. Questa composizione riflette proprio la natura multidisciplinare del campo e giustifica ulteriormente la scelta metodologica della narrative review rispetto a un protocollo più rigido vincolato a un numero ristretto di riviste.

Un'ulteriore distinzione rilevante riguarda la natura della fonte da cui ciascun contributo trae le proprie evidenze. Sotto questo profilo, gli articoli inclusi si dividono in due grandi macro-categorie: i contributi che sviluppano l'analisi a partire dalla letteratura precedente (mediante la rielaborazione teorica di modelli esistenti, l'estensione di framework già pubblicati o l'applicazione di metodologie consolidate a nuovi dataset) e gli studi che raccolgono evidenze originali direttamente sul campo, attingendo all'esperienza pratica dei professionisti attraverso interviste, questionari o l'esame di casi aziendali reali.

La maggioranza dei contributi inclusi rientra nella prima categoria. Si tratta in larga parte di studi che testano algoritmi di machine learning su dataset storici di bilancio, oppure di analisi volte a estendere modelli teorici preesistenti. È il caso, ad esempio, del lavoro di Bao et al. (2020), il quale innesta tecniche di ensemble learning su variabili contabili selezionate sulla base della letteratura precedente. Una quota minoritaria ma significativa

di contributi si basa invece su evidenze raccolte direttamente nel contesto professionale; questo approccio emerge nello studio di Kokina, Blanchette e Davenport (2025), fondato su interviste a professionisti delle Big Four, così come nelle ricerche di Seethamraju e Hecimovic (2023) e di Vitali e Giuliani (2024), entrambe basate su questionari somministrati e fatti compilare a campioni di revisori esterni. Questi ultimi contributi assumono un peso particolare all'interno del capitolo 4, poiché offrono un riscontro diretto, non mediato da modelli statistici su serie storiche, relativamente a come i professionisti percepiscano l'integrazione dell'intelligenza artificiale nel lavoro quotidiano.

2.4 L'organizzazione tematica della rassegna

Il materiale selezionato è stato organizzato in funzione della struttura argomentativa dell'elaborato, la quale si articola attorno a due macro-aree tematiche che riflettono i due principali filoni della ricerca.

La prima area raccoglie i contributi di matrice tecnologica, focalizzati sullo sviluppo e sull'efficacia predittiva degli algoritmi di machine learning, degli strumenti di natural language processing e dei sistemi di continuous auditing applicati all'identificazione delle anomalie contabili. Questi contributi costituiscono la base documentale del terzo capitolo. In fase di analisi, essi sono stati ulteriormente suddivisi in base allo strumento tecnologico prevalentemente discusso (ovvero machine learning, NLP o continuous auditing). Tale scelta permette di costruire un'argomentazione progressiva che ripercorre l'evoluzione tecnologica della revisione prima di affrontare, nel paragrafo conclusivo del capitolo, il confronto integrato tra i diversi strumenti rispetto alle tipologie di frode definite nel primo capitolo.

La seconda area raggruppa gli studi di natura professionale, comportamentale e normativa, incentrati sull'impatto delle nuove tecnologie sulla figura del revisore, sullo scetticismo professionale e sull'evoluzione del quadro regolatorio internazionale. Questi contributi alimentano l'analisi del quarto capitolo e seguono una progressione analoga: si esamina in primo luogo la trasformazione del ruolo professionale, si passa poi all'approfondimento dell'automation bias e dei bias algoritmici incorporati nei modelli, e si analizzano infine le risposte normative di IAASB, PCAOB e del legislatore europeo. La maggiore presenza di articoli destinati al quarto capitolo rispetto al terzo riflette il

diverso grado di maturità dei due filoni di ricerca. Il dibattito sulle implicazioni professionali e regolatorie genera nuovi contributi con maggiore frequenza rispetto alla ricerca sugli algoritmi, la quale appare ormai consolidata attorno a un numero ristretto di lavori fondamentali.

A integrazione della selezione effettuata attraverso l'estrazione sistematica su Scopus, la rassegna include alcune categorie di fonti che per loro natura non compaiono nei database accademici, ma che risultano indispensabili per ancorare l'analisi alla realtà normativa e operativa della revisione contabile. Si tratta dei principi di revisione internazionali emessi dallo IAASB (con particolare riferimento all'ISA Italia 240 e alla sua versione revisionata) e del Report to the Nations dell'ACFE. Completano questa selezione i documenti di indirizzo prodotti da organismi professionali quali il PCAOB e l'ISACA sull'integrazione delle tecnologie digitali nei processi di controllo, oltre al testo del Regolamento europeo sull'intelligenza artificiale (EU AI Act).

Va infine riconosciuto un limite metodologico intrinseco a qualsiasi rassegna condotta su un campo in rapida espansione; si rileva il rischio che alcuni contributi rilevanti, pubblicati nei mesi immediatamente precedenti la stesura dell'elaborato, non siano stati intercettati dall'estrazione, specialmente se ancora in fase di indicizzazione nei database consultati. Questo limite non inficia la validità delle conclusioni raggiunte, le quali si fondano su un corpus selezionato con criteri espliciti, documentati e coerentemente applicati lungo l'intero processo di ricerca.

III. L’impatto dell’intelligenza artificiale e del monitoraggio continuo

Questo capitolo analizza come gli strumenti tecnologici più avanzati, tra cui l'intelligenza artificiale, il machine learning e il continuous auditing, stiano modificando la capacità della revisione contabile di rilevare le frodi nei bilanci.

Il punto di partenza è l'evoluzione storica del rapporto tra tecnologia e revisione, in quanto capirne la trasformazione è necessario per valutarne correttamente la portata attuale. L'introduzione degli strumenti informatici nella pratica di audit è un processo iniziato decenni fa che ha attraversato fasi di continua evoluzione con la diffusione dell'intelligenza artificiale. Nel valutare questo impatto la letteratura suggerisce di superare sia l'entusiasmo acritico verso l'automazione sia lo scetticismo difensivo di chi vede la tecnologia come una minaccia alla professione. La trattazione si concentra sui tre strumenti principali che la letteratura identifica come più promettenti per la rilevazione delle frodi: il machine learning, con la sua capacità di analizzare grandi volumi di dati alla ricerca di pattern anomali, il Natural Language Processing, focalizzato sull'analisi semantica dell’informativa testuale, e il continuous auditing, con la sua logica di monitoraggio sistematico e in tempo reale che rappresenta una risposta diretta ai limiti della periodicità dell'audit tradizionale.

3.1 L'evoluzione tecnologica nella revisione contabile

Le radici del legame tra revisione e tecnologia risalgono agli anni Sessanta e Settanta del Novecento, quando i revisori iniziarono a interfacciarsi con la crescente informatizzazione dei processi aziendali, che rendeva i libri contabili cartacei sempre meno centrali e imponeva lo sviluppo di nuove metodologie capaci di operare su supporti digitali. In questa prima fase la tecnologia si configurava principalmente come una complessità da gestire piuttosto che come un'opportunità da sfruttare: il revisore doveva imparare a fare audit attraverso il computer, approccio che impone la verifica dei controlli informatici interni incorporati nei sistemi informativi aziendali invece di limitarsi ad analizzare soltanto gli output cartacei che ne derivavano (Alles, 2015). Questa distinzione, apparentemente tecnica, ha avuto implicazioni profonde sul modo in cui si è sviluppata la professione nei decenni successivi.

Un salto significativo si è verificato con la diffusione su larga scala dei sistemi ERP a partire dagli anni Novanta. I sistemi ERP (Enterprise Resource Planning) sono piattaforme software integrate di gestione che consentono alle aziende di automatizzare e

connettere in un unico database centrale tutte le principali attività operative, dai cicli attivi e passivi alla logistica, fino alla contabilità generale. La loro adozione massiva ha reso l'audit informatizzato una necessità, poiché la presenza di questi sistemi ha costretto i revisori a adottare l'approccio orientato ai sistemi informativi, accelerando lo sviluppo delle tecniche e degli strumenti di audit assistito da computer (CAATTs) che supportano i revisori nell'estrazione e nell'analisi dei dati, migliorando l'efficienza e l'efficacia della revisione. Gli strumenti CAATTs hanno rappresentato per diversi anni il principale punto di contatto tra la revisione e la tecnologia in quanto consentivano di interrogare grandi archivi di dati, di eseguire riconciliazioni automatiche e di identificare anomalie statistiche nelle distribuzioni delle transazioni. Questi strumenti hanno rappresentato un avanzamento significativo rispetto all'audit manuale, restando però vincolati a una logica reattiva e guidata dall'utente, il quale è tenuto a sapere in anticipo l'oggetto della ricerca per poter costruire la richiesta adatta, e l'analisi rimaneva circoscritta a insiemi di dati limitati e a tipologie di test predefinite.

La fase successiva nell'evoluzione tecnologica dell'audit è quella delle audit data analytics, consolidatasi nel corso degli anni 2000 e 2010 parallelamente alla crescita esponenziale della disponibilità di dati aziendali. Come documentano Appelbaum, Kogan e Vasarhelyi (2024), questa trasformazione ha progressivamente spostato il baricentro della revisione dal campionamento all'analisi di intere popolazioni di transazioni, aprendo la strada a forme di monitoraggio molto più sistematiche e continue rispetto a quelle consentite dai metodi tradizionali. Le audit analytics hanno introdotto nella pratica professionale strumenti come la visualizzazione dei dati, l'analisi delle distribuzioni statistiche, il rilevamento delle anomalie e i modelli predittivi applicati ai dati contabili, soluzioni che le principali società di revisione hanno progressivamente incorporato nelle proprie metodologie.

La crescita esponenziale dei volumi informatici ha aperto le porte all'integrazione dell'intelligenza artificiale anche all'interno dei processi di audit dal momento che il settore è particolarmente predisposto alla parziale automazione a causa della sua natura ad alta intensità di lavoro e dell'ampio spettro di strutture decisionali che lo caratterizza. La letteratura più recente conferma che il passaggio dall'analisi tradizionale all'IA è ormai avviato nella pratica professionale, anche se con gradi di adozione molto disomogenei tra contesti geografici e dimensionali diversi.

La trasformazione digitale della revisione richiede oggi una combinazione di competenze tradizionali di audit e di competenze tecnologiche, imponendo ai revisori di sviluppare capacità in data analytics, cybersecurity e sistemi informativi per rimanere rilevanti ed efficaci nel loro ruolo. Questo passaggio verso l'adozione dell'intelligenza artificiale sta modificando profondamente gli strumenti di lavoro, le competenze richieste al team di revisione, le modalità operative e le stesse responsabilità connesse all'uso dell'automazione.

Il passaggio dalle audit analytics tradizionali all'intelligenza artificiale rappresenta un salto quantitativo nella capacità di elaborare dati e un cambiamento qualitativo nel tipo di analisi che è possibile condurre. Gli strumenti basati sull'intelligenza artificiale consentono di analizzare interi dataset finanziari identificando comportamenti insoliti che sfuggirebbero ai test manuali, permettendo di effettuare valutazioni del rischio più precise e tempestive rispetto a quelle consentite dai metodi tradizionali. Un sistema di machine learning applicato ai dati contabili, oltre a cercare anomalie predefinite dall'utente, è in grado di apprendere autonomamente i modelli ordinari di comportamento di un'organizzazione e di segnalare le deviazioni da questi standard anche quando non corrispondono ad alcuna categoria di irregolarità precedentemente codificata. Questa capacità, che nella letteratura viene spesso definita anomaly detection, è particolarmente rilevante per la rilevazione delle frodi poiché molte si manifestano proprio come deviazioni sottili e sistematiche dai pattern attesi (Lim et al., 2025).

Le organizzazioni che adottano strumenti avanzati di analisi dei dati registrano miglioramenti significativi nella capacità di individuare irregolarità contabili e di produrre informazioni finanziarie più affidabili, come confermato dai riscontri pratici che testimoniano che i benefici di tali tecnologie si traducono in miglioramenti reali sul campo (Mardessi, 2023).

In passato, quando il revisore applicava una tecnica di campionamento statistico a una determinata popolazione di documenti contabili, esisteva generalmente un tasso di errore atteso. Avere accesso remoto a tutti i dati di un cliente ha consentito l'implementazione di nuove e migliorate procedure di data analytics capaci di verificare ogni singola transazione, riducendo drasticamente il rischio di campionamento e focalizzando l'attenzione sulle reali anomalie dei dati. La pandemia da Covid-19 ha ulteriormente accelerato questa transizione, rendendo l'accesso digitale ai dati del cliente

e il testing automatizzato una necessità operativa per molte delle società di revisione quando prima era solo una sperimentazione isolata (Butaka, 2022). I professionisti si trovano ora ad affrontare trasformazioni di grande portata in un arco di tempo relativamente breve. La sfida rimane capire come utilizzare gli strumenti disponibili per ottenere una ragionevole sicurezza che il bilancio non contenga errori significativi, e come farlo in modo che la tecnologia amplifichi le capacità del team di controllo senza sostituirne il giudizio critico. I paragrafi che seguono analizzano in dettaglio i principali strumenti oggi disponibili per la fraud detection: il machine learning, il natural language processing e il continuous auditing, esaminandone per ciascuno i risultati empirici documentati dalla letteratura e i limiti applicativi che ne condizionano l'adozione nella pratica professionale.

3.2 Il machine learning applicato alla fraud detection

Tra gli strumenti tecnologici che negli ultimi anni hanno attirato maggiormente l'attenzione nella letteratura di revisione contabile, il machine learning occupa una posizione centrale. La crescita esponenziale della capacità di elaborazione, la disponibilità sempre maggiore di dati finanziari strutturati e lo sviluppo di algoritmi sempre più sofisticati hanno trasformato il machine learning in una leva strategica fondamentale, soprattutto nei contesti più avanzati della pratica professionale. La comprensione delle logiche di funzionamento, delle potenzialità applicative e dei vincoli strutturali costituisce un prerequisito indispensabile per analizzare criticamente l'evoluzione della revisione contabile.

A differenza degli approcci tradizionali, un sistema di machine learning non viene programmato con regole esplicite per identificare le frodi, ma viene addestrato su un insieme di dati storici, come transazioni, voci di bilancio o indici finanziari, in modo da apprendere autonomamente i modelli comportamentali che distinguono le osservazioni normali da quelle anomale. Una volta addestrato, il modello può applicare quanto appreso a nuovi dati, assegnando a ciascuna osservazione una probabilità di essere fraudolenta o segnalando le deviazioni più significative rispetto alle tendenze attese. Questa capacità di generalizzare partendo dall'esperienza passata segna una netta discontinuità rispetto ai sistemi basati su regole fisse, l'apprendimento automatico si rivela molto efficace nel far emergere quegli illeciti progettati proprio per aggirare i controlli già noti.

La letteratura distingue tradizionalmente tra due grandi categorie di approcci algoritmici: il supervised learning e l'unsupervised learning, con un terzo filone emergente rappresentato da metodi che combinano i due.

I modelli di supervised learning, come la regressione logistica, gli alberi decisionali e le support vector machine, si basano su dataset etichettati per apprendere le ricorrenze del comportamento fraudolento, raggiungendo alta accuratezza quando sono disponibili dati etichettati sufficienti. In pratica, questo significa addestrare il modello su un insieme di casi storici di cui si conosce già l'esito (ad esempio distinguendo tra aziende che hanno commesso illeciti e società del tutto regolari) lasciando che l'algoritmo identifichi quali variabili distinguono meglio i due gruppi.

La regressione logistica è stata per lungo tempo il metodo di riferimento nella letteratura di fraud detection in ambito contabile, principalmente per la sua interpretabilità. A differenza di molti algoritmi più sofisticati, produce coefficienti leggibili che consentono di capire quali variabili contribuiscono maggiormente alla previsione di frode, un requisito importante in un contesto professionale in cui il revisore deve essere in grado di giustificare le proprie conclusioni (Enget, 2015).

Gli alberi decisionali offrono un approccio altrettanto intuitivo segmentando la popolazione di bilanci attraverso una serie di regole logiche sequenziali "se-allora" basate su soglie quantitative (ad esempio, anomalie nel rapporto tra flussi di cassa operativi e utile netto). Questo approccio mappa visivamente il percorso decisionale dell'algoritmo, facilitando il compito del revisore nell'identificare i singoli fattori di rischio.

Una complessità matematica decisamente superiore caratterizza le support vector machine (SVM), le quali proiettano i dati finanziari in uno spazio multidimensionale tracciando un confine ottimale (iperpiano) di separazione tra le osservazioni regolari e quelle potenzialmente fraudolente. Pur garantendo un'elevatissima accuratezza predittiva anche in presenza di relazioni non lineari tra le voci contabili, i modelli SVM scontano una minore interpretabilità immediata, configurandosi spesso come modelli più opachi per l'operatore umano.

Nella letteratura contabile internazionale si nota come il superamento dei vecchi modelli statistici richieda l'integrazione tra la conoscenza economico-aziendale e le tecniche di ensemble learning. Il contributo più significativo in tale direzione è rappresentato dallo studio di Bao et al. (2020), il quale dimostra come l'addestramento

degli algoritmi su dati contabili grezzi, anziché sui classici quozienti di bilancio, permetta di intercettare segnali predittivi di frode altrimenti invisibili alle analisi classiche. Questo metodo, oltre a sostituire la regressione logistica con soluzioni aventi una maggiore capacità di calcolo, costituisce anche un supporto al giudizio critico del revisore. Il confronto tra i modelli di machine learning e i benchmark storici basati su singole variabili mostra incrementi significativi nell'accuratezza delle previsioni riducendo drasticamente i tassi di falsi allarmi contabili. L'efficacia delle procedure di tracciamento della frode è legata a quanto sia sofisticato l'algoritmo ma la differenza reale la fa la capacità di alimentare i modelli con variabili radicate nella teoria contabile, capaci di intercettare le asimmetrie nei flussi finanziari.

Su questa linea si colloca il contributo di Achakzai e Peng (2023) che introduce il Dynamic Ensemble Selection algorithm, uno studio che combina dinamicamente diversi classificatori individuali per produrre una previsione finale. Gli strumenti basati sul machine learning sono più efficaci nel rilevare anomalie e segnali di frode nei bilanci rispetto al tradizionale approccio campionario. L'applicazione di queste tecnologie consente una migliore elaborazione di volumi di dati maggiori, generando previsioni più accurate e riducendo i falsi positivi. In un contesto di revisione, un falso positivo è un’anomalia che inizialmente sembra valida ma in realtà è priva di fondamento dopo l'analisi del revisore. Un sistema che genera troppi falsi positivi rischia di trarre in inganno il professionista, che finisce per ignorare le segnalazioni o per ridurne il peso nel proprio giudizio complessivo. La capacità di ridurre i falsi allarmi mantenendo al contempo un'elevata sensibilità nella rilevazione delle frodi reali rappresenta una delle sfide tecniche più importanti nella progettazione dei modelli di apprendimento automatico per l’attività di audit.

Una prospettiva metodologica radicalmente diversa è quella espressa dai modelli di unsupervised learning. Questi algoritmi non richiedono dati etichettati e non vengono addestrati su casi di frode noti, bensì operano identificando strutture e raggruppamenti nei dati finanziari, segnalando come anomale le osservazioni che si discostano in modo significativo dal comportamento della maggioranza.

Attualmente, entrambi gli approcci, sia quelli supervisionati sia quelli non supervisionati, trovano spazio con successo nella prassi di audit per l'individuazione di irregolarità documentali. L'identificazione di anomalie nei dati del libro mastro generale evidenzia

come le tecniche tradizionali, quali il campionamento casuale o la verifica manuale, risultino progressivamente inefficienti a causa dei crescenti volumi di dati e dei pattern fraudolenti sconosciuti complessi da identificare senza l'ausilio di sistemi automatizzati.

L'isolation forest e gli autoencoder sono tra gli algoritmi unsupervised più utilizzati in questo contesto. L'Isolation Forest si basa sulla costruzione di alberi decisionali casuali per isolare i record sospetti; gli autoencoder invece sfruttano le reti neurali per apprendere una rappresentazione compressa dei dati normali e segnala come anomale le osservazioni che non riescono a essere ricostruite con sufficiente precisione. Questi approcci sono particolarmente utili quando si tratta di rilevare tipologie di frode mai osservate in precedenza, per cui non esistono esempi etichettati su cui addestrare un modello supervisionato.

La frontiera più avanzata in questo campo è rappresentata dal filone dei metodi ensemble. L'idea di fondo, invece di affidarsi a un singolo algoritmo, è di combinare le previsioni di più modelli, per sfruttare il fatto che ogni sistema tende a commettere errori diversi e che la loro combinazione produce risultati più robusti e precisi. Il random forest, il gradient boosting e più recentemente il XGBoost sono tra gli algoritmi ensemble più studiati. Questi algoritmi ensemble basati su strutture decisionali ad albero mostrano le capacità predittive più elevate nella classificazione degli illeciti, mentre l'analisi discriminante lineare si è distinta come il principale algoritmo lineare per i task predittivi che coinvolgono dati contabili.

Il contributo di Gkegkas e Pazarskis (2025) offre una rassegna sistematica di 43 studi pubblicati tra il 2010 e il 2024 sull'uso della data analytics nella fraud detection e prevention. Gli studi analizzati provengono prevalentemente da contesti nordamericani e asiatici, un dato che conferma il gap geografico. I risultati indicano che i modelli ensemble ottengono in media un'accuratezza dell'87-92% nella classificazione dei bilanci fraudolenti, a fronte del 71-78% registrato dalla regressione logistica tradizionale; viene confermata la superiorità degli approcci ensemble rispetto ai metodi statistici tradizionali, ma evidenziano anche un elemento che tende a essere sottovalutato nel dibattito, il fatto che la qualità e la rappresentatività dei dati di addestramento è una variabile critica tanto quanto la sofisticazione dell'algoritmo. Un modello addestrato su dataset non bilanciati, in cui i casi di frode reale sono una minoranza rispetto ai casi normali, tende a sovrastimare la categoria maggioritaria producendo un'elevata accuratezza generale ma

una bassa sensibilità proprio sui casi di frode, che sono esattamente quelli che il modello dovrebbe rilevare. Questa asimmetria nei database, noto come class imbalance, rappresenta una delle principali sfide tecniche nell'applicazione del machine learning all'auditing e ha generato un filone di ricerca dedicato allo sviluppo di tecniche di bilanciamento dei dataset di partenza.

L'efficacia applicativa degli strumenti di machine learning è legata alla capacità del revisore di interpretare correttamente gli output. La tecnologia non elimina la necessità del giudizio professionale ma ne cambia la natura spostando l'attenzione dall'esecuzione delle procedure alla valutazione critica dei segnali prodotti dagli algoritmi.

Una questione molto affrontata riguarda la spiegabilità dei modelli. Molti degli algoritmi più potenti producono previsioni accurate ma non forniscono una spiegazione comprensibile del processo decisionale che le ha generate. In un contesto professionale come quello della revisione contabile, in cui il revisore deve riuscire a motivare le proprie conclusioni e comunicarle al management, ai responsabili della governance e alle autorità di vigilanza, un modello non interpretabile crea problemi significativi.

La scelta tra accuratezza predittiva e interpretabilità del modello è uno dei focus nella progettazione dei sistemi di machine learning per l'audit e la sua risoluzione implica delle scelte riguardanti la responsabilità e l'etica professionale. Il filone della explainable AI (XAI), che si propone di sviluppare algoritmi in grado di fornire spiegazioni comprensibili per le proprie previsioni, rappresenta uno degli sviluppi più promettenti per l'adozione del machine learning nella pratica di revisione (Tragouda et al., 2024)

Un ultimo aspetto riguarda la necessità di integrare i sistemi di machine learning con la conoscenza profonda del dominio contabile. I modelli che combinano variabili selezionate sulla base delle teorie contabili esistenti con algoritmi di machine learning avanzati producono risultati superiori rispetto a quelli che si affidano esclusivamente alle capacità di apprendimento automatico dell'algoritmo. Questo significa che il machine learning non va usato come uno strumento che il revisore può semplicemente "accendere" e lasciare lavorare autonomamente ma richiede delle competenze ibride in cui la comprensione dei meccanismi contabili e dei pattern tipici della frode è tanto importante quanto la padronanza degli strumenti tecnici. È questa forma ibrida tra competenza di dominio e competenza tecnologica che definisce il profilo del revisore del futuro.

3.3 Il natural language processing e l'analisi documentale

Una delle presunzioni principali che ha guidato per decenni la ricerca sulla rilevazione delle frodi è che queste si nascondano principalmente nei numeri, nelle voci di bilancio alterate, nei ricavi fittizi, nelle passività occultate; in realtà le manipolazioni di bilancio emergono anche nel modo in cui chi le commette ne argomenta i risultati, in altri termini nel linguaggio che il management adotta nelle relazioni sulla gestione, nelle note al bilancio o nelle comunicazioni agli stakeholder. Quando qualcosa non va il linguaggio utilizzato dal management cambia in modo spesso impercettibile ma in qualche modo rilevabile. È su questa intuizione che si fonda l'applicazione del natural language processing (NLP) per la ricerca delle frodi, un filone di ricerca relativamente giovane ma in rapida crescita che, soprattutto dopo la diffusione dei modelli linguistici di grandi dimensioni, sta attirando un'attenzione crescente nell'ambito della revisione contabile.

Il punto di partenza teorico di questo filone risiede nella particolare condizione psicologica in cui si trovano i redattori di bilanci fraudolenti, i quali hanno necessità di comunicare risultati che sanno essere falsi cercando allo stesso tempo di risultare credibili nei confronti dei destinatari del documento che lo leggeranno e non dovranno sospettare di niente. Questa tensione, che caratterizza chi scrive il documento nel tentativo di occultare le irregolarità, si riflette nel linguaggio in modi misurabili. La ricerca ha documentato che i bilanci fraudolenti tendono a contenere una maggiore frequenza di termini vaghi e ambigui, un minore uso di riferimenti quantitativi precisi, una riduzione delle espressioni di incertezza e un aumento dell'uso di linguaggio positivo e rassicurante in prossimità delle sezioni più delicate del documento. Paradossalmente, chi mente tende a sembrare più sicuro di sé.

Il NLP ha trovato una conferma fondamentale attraverso l'introduzione di dizionari testuali creati appositamente per il settore economico-aziendale. L'uso di questi modelli permette di superare i limiti dei normali dizionari linguistici, nei quali i termini prettamente contabili rischiano di essere scambiati per parole negative o ambigue quando in realtà non lo sono. L'evidenza empirica dimostra che la presenza di anomalie nel tono del testo non è dovuta a una generica incertezza, ma è collegata in modo significativo a problemi aziendali molto precisi, come l'emersione di debolezze nei controlli interni, una forte volatilità dei rendimenti sul mercato e una maggiore probabilità di subire o

commettere frodi. Le evoluzioni di questo filone di ricerca hanno dimostrato come le sfumature del linguaggio societario possano funzionare come veri e propri indicatori anticipatori delle irregolarità nei bilanci. Le alterazioni nella frequenza di parole chiave legate al rischio, all'ambiguità o a un'esagerata enfasi positiva tendono a manifestarsi spesso insieme alle manovre di gestione opportunistica degli utili. Il sistema NLP offre al revisore un segnale d'allarme precoce e molto utile per intercettare la potenziale manipolazione delle informazioni e la pianificazione di irregolarità future (Loughran e McDonald, 2016).

La sezione dei report annuali che ha ricevuto maggiore attenzione è la cosiddetta MD&A (Management Discussion and Analysis) ovvero la relazione sulla gestione in cui il management descrive i risultati dell'esercizio, i rischi principali e le prospettive future. Si tratta di una sezione narrativa in cui la voce del management è particolarmente presente e in cui le scelte linguistiche riflettono in modo più diretto la disposizione cognitiva ed emotiva di chi scrive.

In uno studio vengono applicati i modelli BERT pre-addestrati su testi finanziari alle sezioni MD&A di circa 3.400 aziende quotate statunitensi nel periodo 2000-2019, identificando anomalie nel tono linguistico come segnali predittivi di frode. Il modello finale supera il benchmark testuale del 15% e quello quantitativo del 12%, identificando cinque volte più casi fraudolenti rispetto ai metodi testuali tradizionali a parità di aziende analizzate. Il risultato ottenuto è particolarmente significativo in quanto dimostra che le informazioni contenute nel testo narrativo aggiungono, rispetto alle informazioni contenute nei dati quantitativi di bilancio, un contributo informativo autonomo che migliora significativamente la capacità predittiva dei modelli di fraud detection (Bhattacharya, 2024).

Un ulteriore e recente avanzamento nell'applicazione del Natural Language Processing all'audit è rappresentato nello studio di Ergun (2025), il quale introduce un modello predittivo denominato DeepFraud. L'elemento di forte originalità di questo approccio risiede nel superamento delle analisi statiche, ottenuto attraverso l'impiego di vettori linguistici avanzati (i cosiddetti embedding) capaci di tracciare l'evoluzione del significato delle parole nel tempo. Invece di limitarsi a scansionare un singolo bilancio in modo isolato, questo sistema converte i testi dei report finanziari in coordinate matematiche che riflettono il contesto storico e settoriale in cui sono stati scritti,

catturando anche le minime variazioni nel tono e nello stile della narrativa aziendale. Per elaborare questa serie storica di informazioni, il modello si appoggia alle reti neurali ricorrenti di tipo LSTM (Long Short-Term Memory), una tecnologia particolarmente adatta alla revisione contabile poiché è progettata per elaborare sequenze di dati ricordando le informazioni passate. Nella pratica, un algoritmo LSTM effettua una comparazione con la "memoria storicizzata" dei documenti relativi agli anni precedenti, evitando di analizzare la relazione sulla gestione dell'anno corrente come un evento a sé stante. Questa architettura adotta un metodo longitudinale su un arco temporale di trent'anni (dal 1995 al 2024), dimostrando una spiccata capacità di allerta precoce.
Tale impostazione si sposa perfettamente con le dinamiche del rischio di revisione. Il fenomeno della frode contabile ha una natura intrinsecamente incrementale e tende a persistere per diversi esercizi prima di essere scoperto. Un sistema capace di monitorare le traiettorie linguistiche del management lungo più anni, anziché basarsi su modelli che analizzano un unico istante temporale, consente al revisore di intercettare tempestivamente quel progressivo irrigidimento del linguaggio che spesso anticipa l'emersione di condotte fraudolente.

Per il NLP risulta molto importante la scelta degli strumenti linguistici da utilizzare per le analisi. Nella prima fase di sviluppo la ricerca si è affidata soprattutto ad approcci basati su dizionari chiusi. Questi sistemi utilizzavano liste di parole classificate in categorie come positive, negative, incerte o conflittuali per calcolare la frequenza dei termini nelle sezioni chiave del bilancio e usarla come variabile per prevedere le irregolarità. Il limite di questo metodo risiede nel fatto che un elenco fisso di vocaboli non permette di cogliere il contesto in cui le parole vengono effettivamente inserite, non distingue l'uso letterale da sfumature più particolari e non riesce a intercettare strutture sintattiche complesse. I modelli linguistici di grandi dimensioni (Large Language Models) riescono a superare gli approcci tradizionali proprio nei compiti che richiedono una comprensione linguistica più profonda. Tuttavia, anche questi strumenti avanzati devono affrontare sfide complesse come la necessità di adattarsi al dominio specifico della contabilità, la difficoltà nel garantire l'interpretabilità dei risultati e la presenza di potenziali distorsioni (bias) nei dati di partenza. In questo scenario, il modello FinBERT, sviluppato da Huang et al. nel 2022, rappresenta oggi il punto di riferimento per l'analisi dei testi finanziari. Essendo stato pre-addestrato su un enorme database di documenti

societari e di borsa, questo algoritmo è in grado di cogliere i significati precisi del linguaggio aziendale che i modelli generici spesso fraintendono. Un esempio emblematico è la gestione del termine "liability": mentre un software comune tende a interpretarlo nel suo significato generico di passività o svantaggio, FinBERT ne riconosce immediatamente il valore tecnico e contabile all'interno del bilancio, offrendo al revisore un livello di precisione nettamente superiore nelle attività di controllo.

Una direzione più originale nell'ambito del Natural Language Processing è quella esplorata dallo studio di Luo et al. (2025), il quale analizza l'utilità dei report di sanzione emessi dalle autorità di vigilanza cinesi come fonte testuale complementare per intercettare le frodi nei bilanci delle società quotate. Esaminando un campione di oltre 41.000 aziende e più di 11.000 provvedimenti sanzionatori tra il 2007 e il 2021, i report di sanzione vengono convertiti in vettori testuali attraverso modelli di embedding specializzati, poi integrati con gli indicatori finanziari tradizionali in un framework multimodale. L'integrazione delle fonti testuali esterne produce incrementi compresi tra il 7% e il 12% nella sensibilità del modello, ovvero nella capacità di identificare correttamente le aziende fraudolente senza aumentare il tasso di falsi allarmi. In particolare, lo studio evidenzia incrementi nei principali indicatori di efficacia algoritmica, come la sensibilità, la specificità e l'area sotto la curva ROC (indicatore che misura la capacità complessiva del modello di distinguere correttamente tra bilanci manipolati e bilanci conformi). Questo risultato suggerisce che il perimetro informativo utile per l'individuazione della frode non deve limitarsi ai soli documenti prodotti dall'azienda stessa, come la relazione sulla gestione o le note del bilancio, l'efficacia del controllo aumenta considerevolmente se si estende l'analisi all'intero ecosistema di comunicazioni scritte che circonda l'emittente includendo i verbali delle autorità di vigilanza, le dichiarazioni formali delle controparti e i report degli analisti finanziari. L'espansione del database testuale verso fonti esterne e indipendenti rappresenta una frontiera in cui il NLP si dimostra uno strumento unico, capace di estrarre e incrociare informazioni qualitative non strutturate che i tradizionali indicatori quantitativi di bilancio non potrebbero mai intercettare.

Le applicazioni più recenti del Natural Language Processing stanno estendendo il proprio raggio d'azione oltre l'analisi dei bilanci, orientandosi verso l'ottimizzazione del processo decisionale che conduce alla formulazione del giudizio professionale. Un esempio

significativo in questo senso è rappresentato dallo sviluppo di architetture a doppio modello basate su agenti LLM (Large Language Models), utilizzate per prevedere l'orientamento della relazione di revisione, per anticipare se l'esito della verifica condurrà a un giudizio senza rilievi, con rilievi o a un'impossibilità di esprimere un giudizio, attraverso l'esame congiunto dei flussi quantitativi e della narrativa aziendale.
Questa evoluzione risulta particolarmente rilevante per la pratica professionale, poiché identifica le singole anomalie isolate nei registri contabili e simula la sintesi complessiva che il team di revisione è chiamato a compiere al termine della fase di final. L'opportunità di stimare in anticipo la tipologia di opinione di audit offre spunti di riflessione critici sulla gestione del rischio di revisione. Nella realtà operativa, la definizione del giudizio finale non è una mera operazione matematica, ma il risultato di un processo negoziale e valutativo complesso tra il revisore e la governance societaria, spesso condizionato da scadenze temporali per l'approvazione del bilancio. Poter contare su uno strumento algoritmico che riesce a processare la totalità delle informazioni disponibili, sia numeriche sia testuali, permette al team di revisione di disporre di un benchmark indipendente fin dalle prime fasi dell'incarico. Questo supporto non deve essere inteso come un tentativo di automatizzare il giudizio del professionista, il cui scetticismo e la cui sensibilità al contesto rimangono insostituibili. L'analisi predittiva della opinion agisce come un presidio di qualità che consente di identificare tempestivamente le aree con maggiore rischio o le incertezze sulla continuità aziendale, ottimizzando l'allocazione delle risorse sui rischi a maggiore valore aggiunto e riducendo la probabilità di rilievi tardivi o inattesi.

Rimane aperta una questione centrale che la letteratura non ha ancora risolto in modo soddisfacente, la spiegabilità del processo decisionale. Come già evidenziato per le architetture di machine learning, anche nel campo del NLP i sistemi più evoluti e in particolare i Large Language Models tendono a garantire un'elevata accuratezza predittiva a scapito della trasparenza del processo decisionale. Un algoritmo che segnala come sospetta la relazione sulla gestione di un bilancio, senza essere in grado di indicare quali specifici passaggi linguistici abbiano attivato l'allerta, risulta di difficile utilizzo pratico per il professionista. Il revisore, infatti, ha il dovere deontologico e professionale di motivare le proprie conclusioni in modo oggettivo e documentabile. La ricerca sulla spiegabilità applicata all'analisi testuale per l'audit è ancora nelle sue fasi iniziali, e

l'opacità di tali strumenti rappresenta oggi uno dei principali ostacoli alla loro adozione su larga scala nella pratica professionale.

3.4 Il continuous auditing

Il continuous auditing, inteso come metodo di monitoraggio in tempo reale delle transazioni e dei controlli aziendali, mette in discussione uno dei fondamenti più consolidati della revisione tradizionale che è l'idea che l'audit sia un processo periodico, concentrato in specifiche scadenze di fine esercizio o infra-annuali e finalizzato a produrre un giudizio su eventi passati. La comprensione della portata di questa transizione verso un modello di monitoraggio continuo richiede, prima di tutto, una definizione precisa di cosa si intende per continuous auditing e di come esso si distingue da pratiche affini ma concettualmente diverse.

La definizione più usata è quella elaborata da Vasarhelyi e Halper (1991), che per la prima volta hanno introdotto il concetto di continuous audit of online systems descrivendo le condizioni che lo rendono possibile. Da quel contributo, scritto quando i sistemi informativi aziendali erano ancora agli albori, la letteratura ha progressivamente affinato e articolato il concetto in linea con l'evoluzione dei sistemi informativi. I moderni sistemi informatici consentono di misurare e monitorare i processi aziendali con un livello di dettaglio senza precedenti in tempo reale o quasi, portando i revisori a dipendere sempre di più dalla tecnologia e dagli strumenti software. Il continuous auditing viene oggi definito come un insieme di metodologie e strumenti che consentono al revisore, che sia esso interno o esterno, di raccogliere evidenze di revisione e valutare i controlli in modo continuativo attraverso l'analisi automatizzata delle transazioni nel momento stesso in cui vengono registrate nei sistemi aziendali, senza la necessità di attendere la chiusura del periodo contabile.

È importante distinguere il continuous auditing da due concetti affini con cui viene spesso confuso. Il primo è il continuous monitoring, un'attività prevalentemente gestionale attraverso cui il management monitora in tempo reale i processi operativi dell'azienda per rilevare anomalie, garantire la conformità e ottimizzare le performance. Il continuous auditing, invece, è un'attività di assurance indipendente, condotta dal revisore che utilizza strumenti automatizzati per valutare in modo continuativo se i controlli funzionano e se le transazioni sono conformi alle norme e ai principi contabili

applicabili. Il secondo concetto da distinguere è quello di automated auditing che indica semplicemente l'uso di software per automatizzare procedure di revisione tradizionalmente manuali, senza necessariamente modificare la frequenza o la logica temporale dei test di audit. Il continuous auditing è una trasformazione per il tempo della revisione, che passa da una logica ex-post a una logica in tempo reale.

Sotto il profilo strutturale, l'implementazione del continuous auditing richiede un'infrastruttura informatica di alto livello capace di garantire l'accesso ai flussi transazionali in tempi rapidi. C'è quindi la necessità di appoggiarsi a sistemi di gestione dei dati robusti, in grado di catturare e archiviare grandi volumi di informazioni provenienti da fonti diverse all'interno dell'organizzazione, integrandoli direttamente con database, piattaforme ERP e altri software finanziari o operativi.
L'architettura di un sistema di monitoraggio continuo si articola su tre livelli principali.
Il primo è il livello di acquisizione dei dati, che prevede il collegamento diretto con i sistemi ERP aziendali (come SAP, Oracle o Microsoft Dynamics) al fine di estrarre le transazioni nel momento stesso in cui vengono registrate a sistema, azzerando i tempi di latenza informatica. Il secondo livello si concentra sulle fasi di elaborazione e analisi, all'interno delle quali operano gli algoritmi di rilevazione; le regole di business e i modelli predittivi che esaminano in automatico ogni singola operazione in ingresso, confrontandola con i pattern attesi e segnalando le deviazioni che superano determinate soglie di rischio preventivamente calcolate. Il terzo e ultimo livello riguarda il reporting e l'alerting, la generazione automatica di segnalazioni, dashboard e report grafici. Questo modulo ha il compito di portare le anomalie rilevate all'attenzione del revisore o del management in modo tempestivo, consentendo un intervento rapido e mirato prima che l'errore o l'irregolarità si propaghi nei periodi contabili successivi (Appelbaum et al., 2024).

Il passaggio dalla teoria all'applicazione sul campo trova il suo caso di studio fondamentale nella realizzazione di un sistema pilota di monitoraggio continuo dei controlli interni presso una realtà multinazionale complessa come Siemens (Alles et al., 2006). Il sistema pilota fu implementato su un sottoinsieme di processi del ciclo acquisti, monitorando in tempo reale le transazioni generate dal sistema SAP dell'azienda. I controlli automatizzati erano programmati per verificare la coerenza tra ordini di acquisto, bolle di consegna e fatture, e per segnalare immediatamente i casi in cui l'importo fatturato

superasse quello autorizzato o in cui il fornitore non figurasse nell'anagrafica approvata. Il sistema produceva segnalazioni in tempo reale che venivano classificate per livello di rischio e trasmesse al team di audit interno entro pochi minuti dalla registrazione dell'anomalia. Questo progetto ha segnato una svolta metodologica spostando il dibattito dalle architetture concettuali alla scomposizione dei problemi operativi legati a un'implementazione reale. Le lezioni apprese da questa esperienza pilota hanno delineato alcuni fattori critici di successo, tra cui la necessità di un'integrazione nativa e profonda con le infrastrutture IT dell'organizzazione, unita a un forte coinvolgimento del management per superare le resistenze organizzative. Sotto il profilo strettamente contabile la sfida più complessa è risultata la formalizzazione dei controlli sui processi aziendali; tradurre procedure di verifica tradizionali in regole algoritmiche rigide sufficientemente precise da consentire un monitoraggio automatizzato senza generare anomalie fittizie, richiede uno sforzo di mappatura notevole. Ne consegue che il successo del continuous auditing non dipende solo dall'architettura del software, ma richiede che il revisore abbia competenze informatiche avanzate, capace di fare da ponte tra i flussi transazionali dell'ERP e i requisiti di assurance della revisione.

Il vantaggio del continuous auditing, rispetto al modello periodico tradizionale, è legato in modo diretto alla dimensione temporale del fenomeno della frode. L'esecuzione di un controllo costante all'interno dei sistemi gestionali permette di valutare i flussi transazionali in tempo reale, offrendo la possibilità di identificare i profili di rischio nel giro di poche ore anziché di settimane. Un riscontro pratico di questa efficacia emerge dall'analisi di un caso studio del 2023 relativo a un grande gruppo europeo della grande distribuzione organizzata (GDO), dove l'adozione di un'architettura algoritmica ha permesso di ridurre il ciclo di verifica da 45 giorni a meno di una settimana, intercettando le anomalie nei registri contabili e le aggregazioni sospette di spesa nel momento stesso in cui venivano immesse a sistema. In questo caso il sistema era integrato con l'ERP aziendale e configurato per monitorare in automatico oltre 200 regole di business, dalle soglie di approvazione degli ordini alla frequenza anomala di pagamenti a singoli fornitori. Le segnalazioni venivano classificate in tre livelli di urgenza (basso, medio, alto) e trasmesse al team di revisione attraverso una dashboard aggiornata ogni quattro ore. Questa contrazione dei tempi si traduce in una maggiore efficienza operativa per il team di revisione e soprattutto determina una drastica riduzione della finestra di

esposizione al rischio. Se si considera, come rilevato dai report internazionali, che la perdita mediana per una frode intercettata entro i primi sei mesi si attesta intorno ai 30.000 dollari, mentre la stessa voce sale a 250.000 dollari se la scoperta avviene dopo due o tre anni (ACFE, 2024), la capacità di bloccare le anomalie sul nascere assume una valenza economica immediata. Anticipare l'emersione dell'illecito porta quindi a limitare l'effetto cumulativo del danno patrimoniale prima che le manipolazioni compromettano l'integrità del bilancio d'esercizio.

Un'ulteriore conferma della validità di questo approccio emerge dalle analisi sulle metodologie di implementazione pratica del continuous auditing e del risk monitoring all'interno delle realtà aziendali più strutturate. Le esperienze più efficaci dimostrano che il monitoraggio costante non deve limitarsi all'esame delle singole transazioni prese in isolamento. L'analisi transazionale esprime il suo massimo potenziale quando viene integrata con il tracciamento dei Key Risk Indicators (KRI), ovvero indicatori compositi capaci di fotografare il livello di rischio complessivo di un determinato processo o di un'intera area aziendale, restituendo una visione dinamica e costantemente aggiornata del profilo di rischio societario (Cai, 2024). Questa stretta interconnessione tra il controllo dei singoli record e il monitoraggio degli indicatori aggregati risulta molto importante proprio in ottica di individuazione della frode. Alcune tipologie di illecito particolarmente complesse, come i fenomeni corruttivi o gli schemi di kickback, sono strutturate in modo tale da non lasciare tracce evidenti o anomalie nella singola operazione contabile. Tuttavia, queste condotte tendono a generare scostamenti statistici significativi a livello di trend cumulativi; una distorsione sistematica che un sistema di controllo continuo, basato su indicatori di rischio evoluti, è perfettamente in grado di intercettare e segnalare tempestivamente. Rilevare queste anomalie su base aggregata attraverso i metodi tradizionali risulterebbe estremamente complesso, se non del tutto impossibile, per un revisore umano, il quale si troverebbe a dover elaborare manualmente flussi informativi massivi in tempi compatibili con le esigenze di assurance.

Nonostante i riscontri positivi in termini di efficacia, il continuous auditing presenta limiti strutturali e sfide implementative. Sebbene il management e i revisori percepiscano chiaramente i benefici possibili di questo approccio, il tasso di adozione concreta all'interno dei contesti aziendali rimane ancora sorprendentemente contenuto a causa di barriere che ne frenano l'introduzione e la diffusione. La prima criticità riguarda

l'infrastruttura tecnologica: l'integrazione con i sistemi ERP preesistenti si rivela spesso complessa e onerosa, in particolare all'interno di organizzazioni che operano con sistemi informatici datati o caratterizzate da un'architettura IT frammentata tra diverse unità di business. Un secondo ostacolo, di carattere prettamente organizzativo, è legato al profondo cambiamento culturale e professionale richiesto dal passaggio da una logica periodica a una costante, tale transizione impone una revisione radicale dei processi e delle competenze coinvolgendo, oltre al team incaricato della revisione, l'intera struttura aziendale del cliente che dovrebbe adattarsi alla novità. A queste problematiche si aggiunge infine un limite di natura metodologica: la definizione rigorosa delle regole operative e delle soglie di allerta che governano i sistemi automatizzati costituisce un'operazione tecnica complessa, che richiede una conoscenza approfondita sia dei processi di business sia delle tecniche di audit. Una calibrazione imprecisa di queste variabili rischia di generare un volume insostenibile di falsi positivi, con la conseguenza di sovraccaricare l'attenzione del revisore e di rendere vana l'efficacia stessa dell'aiuto fornito dalla tecnologia.

In questo scenario, un aspetto che merita una riflessione specifica riguarda la relazione tra l'audit continuo e l'attività di revisione esterna. Storicamente il continuous auditing è stato associato principalmente all'audit interno, il quale, operando dall'interno dell'organizzazione, dispone di pieno accesso ai sistemi informativi della società. Per i professionisti esterni la transizione verso un monitoraggio costante appare più complessa in quanto frenata dai limiti oggettivi di condivisione dei database e dai limiti di tempo che governano il mandato professionale e le connesse responsabilità legali. Negli ultimi anni la diffusione di audit analytics basate su infrastrutture cloud e l'evoluzione dei modelli contrattuali stanno progressivamente riducendo queste distanze. I principali network internazionali hanno infatti sviluppato piattaforme proprietarie avanzate progettate per analizzare in modo ricorrente e sistematico i flussi transazionali del cliente lungo l'intero arco dell'esercizio. Questo progresso tecnologico permette di agganciare dinamiche di controllo costante all'interno del tradizionale audit annuale, avvicinando progressivamente la revisione esterna a un modello di verifica dinamico e distribuito nel tempo, capace di attenuare la forte concentrazione dei controlli nella fase di final.

Guardando al futuro della professione, l'unione tra le attività di controllo interno dell'azienda e il lavoro di revisione esterna rappresenta una delle direzioni più promettenti

per i prossimi anni (Appelbaum et al., 2024). In questo modo i dati raccolti dal monitoraggio continuo aziendale non servono solo al management, ma diventano una base di partenza utile anche per il revisore esterno. Questo scambio di informazioni evita la duplicazione delle procedure di verifica, risparmiando tempo e migliorando la qualità del lavoro finale di verifica.

Anche se nella realtà operativa questa collaborazione non è ancora applicata ovunque, indica chiaramente come si muoverà il settore per arrivare a un significativo miglioramento in termini di tempo e di efficacia. Per arrivare a questo risultato il team di revisione esterno deve verificare preventivamente l'affidabilità del sistema informatico del cliente, solo se i controlli preliminari sui software dell'azienda danno esito positivo il revisore potrà fidarsi dei dati generati in automatico, trasformando l'audit continuo in uno strumento di lavoro efficiente.

3.5 L'efficacia nella rilevazione delle diverse tipologie di frode

I paragrafi precedenti hanno analizzato i tre principali strumenti tecnologici oggi disponibili per la rilevazione della frode nell'ambito della revisione contabile: il machine learning, il natural language processing e il continuous auditing. Ciascuno di essi è stato esaminato nella sua struttura, nei suoi fondamenti e nei risultati pratici documentati dalla letteratura. Resta però da chiarire quale sia lo strumento più efficace per le varie tipologie di frode. Il collegamento tra queste tecnologie e la classificazione delle frodi elaborata dall'ACFE, discussa nel primo capitolo, è un tema rilevante; questo paragrafo ragiona in modo integrato su come machine learning, NLP e continuous auditing si posizionino rispetto alle tre macrocategorie di frode (appropriazione indebita, corruzione e falsificazione del bilancio) e su cosa ciascuno di essi possa realmente apportare nella pratica professionale.

Non esiste uno strumento in assoluto superiore agli altri per tutte le tipologie di illecito; c’è una tendenza verso l'utilizzo di dati reali e verso approcci ibridi, che combinano metodi diversi, riconoscendo che ciascun tipo di frode presenta sfide specifiche. Questo significa che un sistema di controllo efficace unisce gli algoritmi diversi in modo coerente con la natura del rischio che si vuole monitorare. È proprio questa integrazione, e non la superiorità tecnica di un solo strumento, a rappresentare il vero valore aggiunto che la tecnologia può offrire oggi alla revisione contabile.

La falsificazione del bilancio è la tipologia di frode in cui il machine learning ha dimostrato la maggiore efficacia, dovuto a motivi molto pratici. Questo genere di illecito si basa su manipolazioni sistematiche dei numeri, come ricavi alterati o passività nascoste, che modificano i normali equilibri economico-finanziari, di conseguenza l'anomalia lascia una traccia numerica evidente nei dati quantitativi, sotto forma di variazioni e distribuzioni insolite che un software può intercettare molto meglio e più rapidamente di un controllo visivo. L'applicazione di queste tecniche ha aiutato il mondo della revisione soprattutto grazie a modelli capaci di incrociare indicatori finanziari con dati non finanziari.

Lo studio di Bao et al. (2020) rappresenta il riferimento pratico più solido su questo punto. Il dataset utilizzato comprende circa 40.000 osservazioni aziendali relative a società quotate statunitensi nel periodo 1991-2008, estratte dagli Accounting and Auditing Enforcement Releases (AAER) della SEC, i quali documentano le irregolarità contabili accertate dall'autorità di vigilanza. Il modello, basato su un algoritmo di ensemble learning addestrato su dati contabili grezzi, anziché sui tradizionali indici di bilancio, supera il benchmark della regressione logistica di circa 8 punti percentuali in termini di accuratezza predittiva, mostrando una capacità di anticipare la frode fino a due anni prima della sua emersione pubblica. Per il revisore si tratta di un vantaggio enorme, se un software segnala un forte rischio di manipolazione con così tanto anticipo, il team di controllo può concentrare subito i test sulle aree pericolose prima che il danno diventi irreparabile e senza stare a concentrarsi su aree in cui il rischio è molto minore. Il machine learning si trasforma così in uno strumento preventivo, che permette al professionista di muoversi in anticipo anziché rincorrere l'emergenza.

A conferma di questo, la ricerca di Achakzai e Peng (2023) introduce un elemento ancora più preciso attraverso l'algoritmo di Dynamic Ensemble Selection. Il modello viene testato su un campione di 533 aziende cinesi quotate nel periodo 2010-2020, caratterizzato da un rapporto di circa 1 a 10 tra casi fraudolenti e conformi. Il Dynamic Ensemble Selection seleziona dinamicamente, per ogni nuova osservazione, il classificatore più appropriato tra quelli disponibili nella libreria algoritmica, ottenendo una riduzione dei falsi positivi del 23% rispetto ai modelli ensemble statici e un'area sotto la curva ROC, indicatore della capacità di discriminazione del modello, superiore al 90%. Nella pratica, questo sistema utilizza un insieme di algoritmi eterogenei e, a seconda del

tipo di azienda o del bilancio che si trova davanti, seleziona quello più adatto per la specifica situazione. Questo metodo riduce drasticamente i falsi positivi, evitando di segnalare errori dove non ci sono, ma mantiene una sensibilità altissima nel trovare le vere e proprie falsificazioni nei bilanci o nei rendiconti finanziari.

Per la stessa tipologia di illecito, il Natural Language Processing offre un contributo complementare e non sostitutivo rispetto all'approccio del machine learning. I bilanci manipolati presentano caratteristiche linguistiche particolari e ricorrenti come un tono eccessivamente ottimista, un ricorso ridotto a espressioni di incertezza e restano molto vaghi nelle descrizioni delle aree di rischio. Questi segnali non possono essere intercettati analizzando soltanto i numeri di bilancio e il loro valore informativo si somma a quello fornito dai dati quantitativi. L'uso di modelli avanzati per l'analisi delle relazioni sulla gestione consente di individuare molte più anomalie rispetto ai sistemi testuali tradizionali superando l'efficacia dei soli modelli numerici di circa il 12% (Mickovic et al., 2024). Questo dimostra che il revisore che unisce l'analisi testuale della relazione sulla gestione con il controllo informatico dei dati quantitativi ottiene un quadro della situazione molto più completo rispetto a chi si affida a uno solo dei due strumenti. Bisogna tuttavia evidenziare che il NLP applicato alle frodi di bilancio funziona al meglio dove la narrativa aziendale è ricca e strutturata, come accade nelle società quotate che sono soggette a obblighi informativi molto stringenti. Lo strumento, al contrario, si rivela meno efficace nei contesti in cui i testi sono limitati o fortemente standardizzati. Per le piccole e medie imprese, che costituiscono la parte principale del tessuto economico italiano ed europeo, la presenza di relazioni sulla gestione scritte in modo approfondito è spesso ridotta. Questo limite strutturale restringe l'uso pratico del NLP soprattutto al segmento delle grandi aziende quotate, lasciando scoperti i mercati della revisione meno strutturati e con meno obblighi informativi.

L'appropriazione indebita è la tipologia di illecito più diffusa a livello aziendale e si manifesta attraverso azioni che colpiscono i flussi ordinari delle transazioni, come pagamenti non autorizzati, deviazioni di incassi, fatture per fornitori fittizi o rimborsi spese gonfiati. Queste condotte lasciano una traccia nei registri contabili, ma si tratta spesso di anomalie frammentate e di importo unitario ridotto. Per questo motivo i campionamenti tradizionali fatti a fine anno hanno pochissime probabilità di intercettarle. È proprio in questo ambito che il continuous auditing esprime il suo vantaggio più diretto

rispetto al modello di controllo periodico.

Un sistema di controllo continuo permette una verifica precisa e in tempo reale dei processi di approvvigionamento e della supply chain, aiutando a bloccare sul nascere errori e inefficienze operative. Nel caso delle giacenze di magazzino, ad esempio, il sistema permette di monitorare anomalie come la capitalizzazione impropria dei costi o il mantenimento di scorte obsolete. Essendo integrato direttamente con l'ERP aziendale, il software esamina ogni singola operazione nel momento stesso in cui viene registrata, la confronta con le soglie di approvazione previste, verifica la coerenza tra la richiesta di pagamento e i documenti di supporto (come l'ordine o il documento di trasporto) e segnala subito le irregolarità. Esempi tipici sono un pagamento inviato a un fornitore non presente tra quelli autorizzati, una fattura con un importo posizionato appena sotto la soglia in cui scatta l'approvazione obbligatoria, o un rimborso spese privo di giustificativi allegati. Queste segnalazioni, generate in tempo reale, permettono al team di revisione di intervenire tempestivamente con procedure di approfondimento, impedendo che l'illecito si ripeta.

La corruzione si configura come la tipologia di illecito più complessa da intercettare attraverso le ordinarie registrazioni contabili. Spesso le transazioni legate a una tangente o a un accordo illecito sono formalmente perfette per cui la fattura esiste, l'importo è autorizzato e la registrazione rispetta i principi contabili. Per scoprire la corruzione l'analisi dei singoli numeri non basta, è necessario esaminare i legami e i pattern relazionali all'interno dell'organizzazione. In questo contesto uno degli strumenti più promettenti è la graph analytics (o network analysis), che rappresenta l'analisi delle reti di relazione, tecnologia che permette di visualizzare graficamente i collegamenti nascosti tra fornitori, dipendenti e terze parti. Invece di guardare la singola operazione, il software mappa l'intero comportamento del sistema, evidenzia, ad esempio, quale dipendente approva con frequenza insolita i pagamenti a un determinato fornitore, o se ci sono anomalie nelle tempistiche o nelle modalità di assegnazione delle commesse. Qualora un dipendente dell'ufficio acquisti approvi sistematicamente pagamenti urgenti a un fornitore creato da meno di sei mesi, con fatture emesse sempre il venerdì pomeriggio e importi appena sotto la soglia che richiede una doppia firma, l’azione congiunta del continuous auditing e della network analysis individua questo schema relazionale e temporale come anomalo anche se ogni singola transazione, presa isolatamente, appare formalmente

corretta. È esattamente questo tipo di pattern, invisibile al campionamento tradizionale ma evidente nell'analisi di rete, che caratterizza molti schemi corruttivi reali. L'incrocio tra il continuous auditing, che monitora i flussi finanziari, e la network analysis, che mappa le relazioni umane e societarie, rappresenta l'unico modo reale per far emergere condotte fraudolente che altrimenti rimarrebbero invisibili al revisore.

L'analisi sull'efficacia delle nuove tecnologie richiede anche una riflessione sui loro limiti oggettivi. I sistemi informatici sono eccezionali nell'identificare anomalie nei dati, ma non possono in alcun modo sostituire il giudizio professionale del revisore nella valutazione del significato di quelle anomalie. Ciascuna tipologia di illecito societario presenta caratteristiche e pattern specifici che richiedono approcci su misura. Un algoritmo può segnalare che una determinata voce di bilancio si discosta in modo statisticamente significativo dall'andamento atteso, ma non può stabilire da solo se quella deviazione rappresenti una frode, un semplice errore contabile, un cambio nelle politiche aziendali o una variazione legittima nelle condizioni di mercato. Comprendere questa distinzione richiede conoscenza del settore, capacità di confrontarsi con il management e valutazione critica delle risposte ricevute; in altre parole, richiede lo scetticismo professionale che resta una prerogativa esclusiva del revisore umano.

Va aggiunto che l'efficacia di questi strumenti dipende interamente dalla qualità e dalla completezza dei database su cui operano. Un sistema di continuous auditing può monitorare in tempo reale solo le operazioni che transitano nei sistemi aziendali. Le frodi che avvengono senza la necessità di alcuna registrazione, come accordi verbali, scambi di favori o manipolazioni precedenti alla registrazione, rimangono strutturalmente invisibili anche al software più sofisticato. Allo stesso modo, un modello di machine learning addestrato su dati storici farà fatica a rilevare tipologie di frode del tutto nuove o schemi che non hanno precedenti nel passato. La tecnologia è potente ma non onnisciente, e i suoi limiti vanno compresi chiaramente per evitare che una fiducia eccessiva nell'automazione crei l'effetto opposto, riducendo l'attenzione del team di controllo.

Il quadro finale mostra un contesto in cui strumenti diversi si completano a vicenda a seconda del tipo di rischio e del contesto aziendale. Il machine learning si conferma lo strumento principale per scoprire le falsificazioni nei bilanci delle società più grandi, dove i dati quantitativi sono ricchi. Il NLP aggiunge un livello informativo in più attraverso

l'analisi della parte narrativa delle relazioni. Il continuous auditing è la soluzione migliore per sorvegliare giorno per giorno le transazioni operative, bloccando sul nascere l'appropriazione indebita e la corruzione negli approvvigionamenti. Nessuno di questi strumenti è sufficiente da solo e nessuno può fare a meno dell'occhio del revisore. È proprio questa complementarità tra tecnologia e giudizio umano a definire il modello di revisione verso cui il settore si sta muovendo.

IV. Il revisore nell'era dell'intelligenza artificiale

Il consolidamento delle tecnologie di intelligenza artificiale e continuous auditing nel processo di revisione sposta inevitabilmente il focus del dibattito scientifico dal piano puramente tecnologico a quello metodologico e deontologico. L'efficacia computazionale di tali strumenti solleva infatti un interrogativo sulla ridefinizione del ruolo del revisore e delle modalità di espressione del suo giudizio professionale quando l'algoritmo diventa parte integrante della routine di lavoro. Risulta essenziale valutare se l'automazione potenzi l'attitudine critica del team di audit o se rischi di attenuarne lo scetticismo.

Il presente capitolo analizza i possibili rischi e l'impatto organizzativo della transizione digitale dell'audit. Viene esaminata prima la trasformazione del ruolo del revisore, il cui profilo evolve da esecutore di procedure standardizzate a supervisore critico dei report algoritmici. Successivamente, l'attenzione si concentra sul fenomeno dell'automation bias, inteso come la tendenza psicologica a fare affidamento sui risultati del software e sulle implicazioni derivanti dai bias euristici intrinseci ai modelli statistici. Vengono infine esaminate le risposte regolamentari dei principali standard setter internazionali e le prospettive di evoluzione verso un modello di audit ibrido, fondato sulla complementarità sinergica tra l'algoritmo e il giudizio umano indipendente.

4.1 Il revisore da controllore periodico a supervisore del sistema

Per comprendere come cambia il ruolo del revisore con l'introduzione dell'intelligenza artificiale, è necessario analizzare come si struttura il lavoro di un team di revisione nella pratica quotidiana. Gran parte del tempo di un incarico tradizionale è assorbito da attività che hanno un forte carattere esecutivo e un basso contenuto di giudizio: il controllo e l'estrazione dei dati, la riconciliazione delle scritture contabili, i test di dettaglio sulle transazioni e la verifica dei documenti a supporto dei saldi di bilancio. Tuttavia, tali procedure sono indispensabili per garantire la correttezza dei conti e richiedono principalmente precisione e rigore procedurale, lasciando poco spazio a un ragionamento critico approfondito. L'inserimento dei sistemi di intelligenza artificiale e degli strumenti di analisi dei dati interviene direttamente su queste mansioni, automatizzando le fasi più meccaniche e ripetitive del processo. Il professionista viene sollevato dalle mansioni di routine di campionamento e controllo documentale, potendo così dedicare più tempo e capacità analitica ad attività complesse che richiedono un reale giudizio professionale, come la valutazione delle stime di bilancio e l'analisi dei rischi

aziendali più delicati.

Tale evoluzione costituisce una realtà consolidata all'interno dei principali network di revisione internazionali, i quali hanno già iniziato a integrare sistemi di intelligenza artificiale nelle proprie metodologie operative (Kokina et al., 2025). Rimane aperto il dibattito su come l'adozione di questi strumenti influenzi concretamente la qualità delle verifiche e lo scetticismo professionale del revisore. Emerge una legittima preoccupazione riguardo al rischio che l'automazione possa condizionare il giudizio critico del professionista. Lo scenario introduce una tensione centrale nel dibattito attuale: l'innovazione tecnologica incrementa l'efficienza dei controlli ma non è scontato che si traduca automaticamente in un miglioramento della qualità del giudizio finale.

Il concetto che meglio descrive questa trasformazione è quello di “human-in-the-loop”. Tale espressione indica un modello in cui l'essere umano rimane parte integrante del processo decisionale, implicando che il revisore deputato a validare le conclusioni prodotte dalla tecnologia mantenga un approccio critico verso gli output generati dal sistema. Un riscontro diretto emerge anche sul piano regolamentare, in particolare all'interno del nuovo regolamento europeo sull'intelligenza artificiale (AI Act), il quale ribadisce che la responsabilità finale delle decisioni automatizzate deve restare in capo all'uomo. Per il revisore contabile, l'implicazione è immediata: occorre che il professionista possieda le competenze necessarie per valutare i risultati dell’algoritmo in modo consapevole, assumendosi la piena responsabilità delle conclusioni espresse nella relazione di bilancio. Nel concreto, questo cambiamento si manifesta in primo luogo sul piano delle abilità richieste. Il revisore che si avvale di strumenti di intelligenza artificiale non può limitarsi a verificare la correttezza di un saldo contabile, ma deve comprendere la logica dell'algoritmo che ha segnalato un'eventuale anomalia. Ciò significa saper valutare quali variabili il sistema ha considerato o ignorato e in quale misura l'output sia affidabile nello specifico contesto aziendale. Il revisore deve avere conoscenza dei sistemi di analisi dati e delle applicazioni del machine learning, insieme a una chiara consapevolezza dei limiti tecnici dello strumento. Questo profilo ibrido, capace di unire la solida preparazione contabile alle nuove conoscenze tecnologiche, si differenzia nettamente dalla figura del revisore tradizionale, in quanto deve affrontare programmi di formazione professionale continui.

L’evoluzione delle competenze ridefinisce anche l'attenzione professionale durante l'incarico. Se nell'approccio tradizionale l'attività del team si concentra sulla verifica di un campione di transazioni selezionate, l'introduzione dell'intelligenza artificiale si concentra maggiormente sulla valutazione delle anomalie segnalate dai modelli predittivi. Il revisore è chiamato a interpretare gli output del sistema distinguendo le segnalazioni che richiedono un effettivo approfondimento da quelle che trovano una giustificazione ordinaria nelle dinamiche aziendali.

Tale passaggio potrebbe aumentare la complessità dell’audit. Il professionista si trova a dover gestire un flusso informativo molto più denso rispetto al passato, affrontando il problema dei cosiddetti falsi positivi, ovvero operazioni lecite che l'algoritmo classifica come sospette a causa di anomalie puramente statistiche. Uno studio empirico condotto da Kokina, Blanchette e Davenport (2025) attraverso interviste ai professionisti delle Big Four conferma questa dinamica. Lo studio si basa su 22 interviste semi-strutturate condotte con professionisti di audit delle principali società di revisione internazionale, con un'esperienza media nel settore superiore ai dodici anni. I partecipanti descrivono una ridefinizione concreta delle attività quotidiane: laddove in precedenza il 60-70% del tempo era assorbito da procedure di estrazione e controllo manuale dei dati, l'adozione di sistemi di analisi automatizzata ha spostato il baricentro del lavoro verso la valutazione critica degli output algoritmici e la gestione delle eccezioni segnalate dal sistema. I revisori che utilizzano regolarmente strumenti di intelligenza artificiale riferiscono infatti una netta contrazione dei tempi dedicati all'esecuzione materiale delle procedure, a favore di una maggiore focalizzazione sulla valutazione critica dei risultati. Gli stessi autori evidenziano come tale attività richieda una sensibilità professionale e un'attitudine allo scetticismo che non tutti i membri del team di audit hanno ancora sviluppato in modo omogeneo.

Un'ultima dimensione del cambiamento riguarda il profilo della responsabilità professionale. Il nodo centrale riguarda l'attribuzione della responsabilità legale nei casi in cui un modello algoritmico non riesca a intercettare una frode contabile: la domanda principale è se la colpa sia da imputare al revisore che ha guidato l'analisi, al fornitore esterno che ha sviluppato il software o al network di revisione che ha validato la tecnologia, quesito che non trova ancora una risposta univoca nella prassi giuridica.

Gli attuali standard internazionali, pur iniziando ad affrontare i temi della validazione

degli strumenti informatici e dei relativi requisiti di documentazione, si trovano ancora in una fase di sviluppo. Questa parziale lacuna normativa genera una sorta di zona grigia che crea incertezza tra i professionisti, i clienti e le stesse autorità di vigilanza. Di conseguenza, la definizione di linee guida chiare sul perimetro di responsabilità dell'auditor umano rappresenta uno dei passaggi più importanti per garantire un'integrazione sicura e trasparente dell'intelligenza artificiale nella pratica professionale.

È opportuno evidenziare che questa ridefinizione del ruolo non debba essere interpretata necessariamente come una minaccia per la stabilità della professione. L'evoluzione storica dimostra che ogni grande innovazione tecnologica introdotta nel campo dell'audit, dall'adozione dei primi sistemi informatici negli anni Sessanta fino alla diffusione degli strumenti CAATTs negli anni Novanta, ha finito per valorizzare il profilo dell'auditor, spostando l'attenzione verso attività di giudizio a più alto valore aggiunto. I dati emersi dall'ISACA 2025 AI Pulse Poll confermano quanto detto; indicano che il 70% dei professionisti operanti nei settori dell'audit e dell'assurance ritiene indispensabile incrementare le proprie competenze in materia di intelligenza artificiale entro l'anno successivo per far avanzare la propria carriera e per rispondere ai nuovi standard richiesti dal mercato. Questa percentuale riflette una diffusa consapevolezza all'interno del settore che la transizione digitale è un cambiamento in atto che richiede una risposta formativa e un costante aggiornamento da parte di ciascun professionista.

Il rischio effettivo non risiede nella sostituzione del professionista da parte della tecnologia, bensì nella possibilità che l'automazione lo induca a esercitare il proprio ruolo in modo meno critico, portandolo ad accettare gli output dell'algoritmo senza un adeguato approfondimento. Serve quindi un'analisi approfondita che richiede la comprensione del meccanismo psicologico alla base di tale comportamento, noto in letteratura come automation bias.

4.2 L'automation bias

Il rischio principale con l'adozione dell'intelligenza artificiale nei processi di audit risiede nella possibilità che l'affidamento costante agli output algoritmici possa, nel tempo, indebolire involontariamente la capacità critica del professionista. La letteratura economico-comportamentale e gli studi più recenti in materia di revisione contabile identificano questa tendenza psicologica come automation bias, descrivendola come una

vulnerabilità operativa concreta. L'introduzione di sistemi automatizzati complessi può generare una sorta di dipendenza cognitiva nel team di verifica, condizionando l'efficacia dello scetticismo professionale proprio nei contesti in cui l'errore o la frode risultano più difficili da intercettare.

L'automation bias si manifesta come la propensione psicologica degli operatori a riporre una fiducia sproporzionata nei risultati forniti dalla tecnologia, che porta a ridurre l'attività di verifica indipendente anche in presenza di indicatori contrari o informazioni contraddittorie. Questa dinamica attenua il ragionamento attivo, indebolendo sia l'autenticità del giudizio critico sia l'autonomia decisionale del professionista. Nei diversi ambiti in cui l'effetto è stato studiato, come l'aviazione civile, la diagnostica medica e i mercati finanziari, il modello comportamentale riscontrato si presenta identico: di fronte a una raccomandazione o a una segnalazione prodotta da un software, l'utente tende ad accettarla senza uno scrutinio adeguato. Questa inclinazione, inoltre, tende a rafforzarsi progressivamente con il tempo e con l'aumentare della familiarità nei confronti dello strumento tecnologico utilizzato (Tümmler et al., 2026).

Nel contesto della revisione legale, l'automation bias assume una configurazione specifica direttamente legata ai presidi sullo scetticismo professionale. Il principio ISA Italia 240 impone all'auditor di mantenere un atteggiamento critico e attivo per tutta la durata dell'incarico, valutando costantemente la validità degli elementi probativi raccolti e superando la naturale tendenza ad accettare le dichiarazioni della direzione senza un adeguato riscontro. L'inserimento dei sistemi di intelligenza artificiale determina una nuova forma di condizionamento: alla tradizionale pressione relazionale esercitata dal management si affianca una sollecitazione di natura cognitiva proveniente dallo strumento stesso. Qualora l'algoritmo non rilevi alcuna anomalia nei flussi contabili, il professionista può essere indotto a presumere l'assenza di irregolarità, attenuando il livello di attenzione anche nei casi in cui l'esperienza e la conoscenza del settore suggerirebbero un esame più approfondito delle poste di bilancio.

Il riscontro più significativo a supporto di tale dinamica proviene dallo studio di Seethamraju e Hecimovic (2023), incentrato sull'analisi comportamentale dei professionisti esposti a un uso intensivo delle nuove tecnologie. La ricerca si basa su un'indagine empirica condotta su un campione di 120 auditor interni ed esterni operanti in Australia, attraverso questionari strutturati e interviste di approfondimento. I

partecipanti sono stati segmentati in base all'intensità d'uso degli strumenti algoritmici: il gruppo ad alto utilizzo, definito come chi impiega sistemi automatizzati per oltre il 60% delle procedure di audit, mostra una contrazione del 35% nei livelli di scetticismo misurati attraverso scale psicometriche validate, mentre il gruppo a basso utilizzo non manifesta variazioni statisticamente significative. Una riduzione di questa portata rappresenta una vulnerabilità rilevante, capace di compromettere l'intercettazione di manovre fraudolente o errori di particolare rilevanza. I dati evidenziano come il cambiamento della visione critica tende a stabilizzarsi come una condotta ordinaria indotta dalla routine tecnologica. Questo scenario impone la definizione di nuovi standard di controllo della qualità orientati a verificare i protocolli di interazione e cooperazione tra l'operatore umano e la macchina, superando la tendenza dei network di revisione a misurare esclusivamente i vantaggi legati alla contrazione dei tempi e all'efficienza dei costi.

Il comportamento esaminato si lega a un secondo meccanismo noto come assuefazione tecnologica. L'esposizione ripetuta ai sistemi di intelligenza artificiale porta il team di revisione a sviluppare un livello di confidenza che aumenta la probabilità di accettare le raccomandazioni del software senza un esame rigoroso. Nelle fasi iniziali di introduzione di un nuovo strumento di analisi automatizzata, il revisore tende a controllare con estrema attenzione ogni singola segnalazione prodotta dall'algoritmo, manifestando una naturale diffidenza verso una tecnologia non ancora consolidata nella pratica quotidiana. Con il tempo la costante accuratezza dei report e la progressiva riduzione dei falsi positivi spingono l'operatore a riporre nello strumento la stessa fiducia che riserverebbe a un collega esperto (International AI Safety Report, 2026). Questo affidamento rischia di tradursi in una riduzione graduale e impercettibile dell'intensità delle verifiche indipendenti, creando la vulnerabilità descrittiva dell'automation bias.

Il condizionamento psicologico, oltre ai casi in cui l’algoritmo segnala un’anomalia, si estende soprattutto alle circostanze in cui il sistema non rileva alcuna criticità. Tale dinamica viene definita omission bias e si traduce nella tendenza a non approfondire le aree di bilancio che il software ha classificato come prive di rischio, anche in presenza di segnali di contesto, di settore o relazionali che suggerirebbero una verifica. In linea con quanto detto nella behavioral mindset theory, l'affidamento incondizionato verso sistemi automatizzati imperfetti può spingere i membri del team a formulare decisioni premature (Romeo et al., 2026). Nel campo della rilevazione delle frodi si

configura un rischio: una manipolazione contabile architettata per eludere gli indicatori di allerta dell'algoritmo rischia di passare del tutto inosservata, persino davanti a un professionista tecnicamente preparato, qualora quest'ultimo abbia sviluppato una dipendenza acritica nei confronti della tecnologia.

Una prospettiva che arricchisce l'analisi emerge dall'indagine condotta da Vitali e Giuliani (2024). Analizzando un campione di 107 revisori esterni, la ricerca ha individuato una relazione positiva tra l'impiego dei sistemi di intelligenza artificiale e l'esercizio dello scetticismo professionale. Il campione è composto da revisori esterni francesi con almeno tre anni di esperienza professionale, raggruppati per livello di utilizzo degli strumenti di IA e per punteggio di scetticismo individuale misurato con la scala Hurtt (2010). La relazione positiva tra uso dell'IA e scetticismo risulta significativa solo nel sottogruppo con punteggi di scetticismo individuale superiori alla mediana, mentre nei revisori con propensione allo scetticismo inferiore alla mediana il segno della relazione si inverte, confermando l'effetto moderatore del tratto personale. Questa evidenza suggerisce che l'impatto dell'automation bias non si manifesti in modo uniforme all'interno dell'organizzazione aziendale, le sue conseguenze dipendono sensibilmente dalle caratteristiche personali del revisore, un fattore che impone alle società di revisione di ripensare i criteri di formazione, la composizione dei team di lavoro e le modalità di supervisione dei profili junior.

Un ulteriore profilo di rischio riguarda l'interazione tra l'automation bias e il fenomeno del management over ride, quale criticità centrale individuata dal principio ISA Italia 240. Qualora la direzione aziendale conosca le logiche di funzionamento e i parametri del software in uso, l'eccessivo affidamento del revisore nei confronti dei report automatici genera una vulnerabilità strutturale profonda. Il management potrebbe orientare le proprie politiche di bilancio e le registrazioni contabili in modo da aggirare le soglie di allerta del sistema, con la consapevolezza che un team di audit condizionato dall'assuefazione tecnologica difficilmente estenderà le verifiche oltre i risultati generati dall'algoritmo. Questo scenario trova riscontro in un filone di ricerca in forte espansione, incentrato sulla cosiddetta adversarial manipulation dei modelli di machine learning, ovvero la capacità di introdurre nei database dati alterati che appaiono del tutto ordinari ai controlli automatizzati ma che di fatto occultano gravi irregolarità. La necessità di

contrastare queste manipolazioni mirate rappresenta una delle sfide metodologiche più complesse che la professione della revisione si trova oggi ad affrontare.

La letteratura scientifica punta su alcune indicazioni per mitigare gli effetti dell'automation bias. Un primo intervento essenziale è rappresentato dalla formazione specifica sul fenomeno, sviluppare nei revisori la consapevolezza del condizionamento psicologico aumenta la loro capacità di mantenere un approccio critico. Risulta essenziale ricordare costantemente che ogni output algoritmico costituisce un elemento probativo complementare e non una conclusione definitiva, senza dover diffidare però a priori della tecnologia. Appare necessaria la strutturazione di protocolli di audit che prevedano verifiche indipendenti obbligatorie, slegate dai risultati del software, in particolare nelle aree di bilancio a più alto rischio di errore. Oltre alla formazione un ruolo decisivo è coperto dal design degli strumenti informatici. Sistemi progettati secondo i principi della Explainable AI (IA spiegabile), capaci di esplicitare le logiche e le motivazioni alla base di una segnalazione, favoriscono un coinvolgimento attivo dell'auditor, a differenza dei modelli tradizionali di tipo black-box che generano output privi di giustificazione trasparente.

Sono state identificate cinque fonti primarie che alimentano le distorsioni tecniche e umane nell'audit automatizzato: le carenze qualitative dei dati, l'omogeneità demografica dei campioni, le correlazioni spurie, i comparatori impropri e i bias cognitivi individuali (Murikah et al., 2024). Vengono analizzati 83 studi pubblicati tra il 2018 e il 2023, selezionati da banche dati accademiche internazionali. Tra le evidenze più rilevanti emerge che il 67% degli studi inclusi documenta almeno un caso di bias legato alla qualità dei dati di addestramento, mentre il 41% segnala distorsioni attribuibili a comparatori inadeguati, ovvero benchmark di riferimento costruiti su campioni non rappresentativi della popolazione aziendale oggetto di revisione. Per neutralizzare tali vulnerabilità, la dottrina suggerisce l'adozione della modellazione causale, un approccio che consente ai revisori di comprendere i nessi logici di fondo e scoprire anomalie algoritmiche altrimenti invisibili.

Si può dunque affermare che l'automation bias non costituisce un limite all'adozione dell'intelligenza artificiale nella revisione legale, ma rappresenta una forte motivazione per guidare questa transizione con consapevolezza. Risulta fondamentale progettare i flussi di lavoro e i percorsi formativi affinché l'innovazione tecnologica amplifichi il

giudizio professionale del revisore evitando che possa sostituirlo senza che se ne renda conto. Chiarite le modalità con cui l'operatore umano interagisce con la macchina, sono da affrontare le distorsioni che risultano direttamente incorporate all'interno degli algoritmi di verifica.

4.3 I bias algoritmici e limiti tecnici dei modelli di IA applicati all'audit

Nell'ipotesi in cui il revisore eserciti il proprio giudizio professionale in modo impeccabile, la qualità finale dell'audit risulta inevitabilmente compromessa qualora gli strumenti tecnologici di supporto producano output distorti o inaffidabili. Comprendere le determinanti tecniche degli errori algoritmici è un prerequisito essenziale per un utilizzo consapevole e responsabile dei sistemi di intelligenza artificiale nella pratica professionale.

Il principale limite tecnologico è rappresentato dall'opacità dei modelli predittivi, comunemente definita con l'espressione black-box. Le soluzioni più avanzate applicate alla fraud detection, come le reti neurali profonde, i modelli di ensemble e i Large Language Models, garantiscono elevati livelli di accuratezza statistica, operando però attraverso processi decisionali interni che non risultano direttamente decifrabili dall'utente. Tali sistemi sono in grado di classificare una determinata voce di bilancio come anomala, senza però chiarire in modo comprensibile le motivazioni sottostanti, le combinazioni di variabili considerate o l’impatto che ciascun fattore ha esercitato sul risultato finale. Più questi sistemi sono complessi, più diventa difficile capire come arrivino a una conclusione. La mancanza di trasparenza pone barriere significative all'attività di verifica, ponendosi in netto contrasto con il principio di spiegabilità sancito dalla normativa europea (AI Act), che considera l'interpretabilità dei modelli un requisito imprescindibile per garantire la fiducia, la governance e la responsabilità legale delle decisioni derivanti da IA.

Per il revisore, tale limitazione si traduce in una problematicità operativa estremamente concreta. I principi di revisione internazionali, con particolare riferimento all'ISA Italia 240, impongono al professionista l'obbligo di documentare le motivazioni alla base delle conclusioni espresse, consentendogli di sostenerle nel confronto con il management, con i responsabili delle attività di governance e, nell'eventualità di contestazioni, dinanzi alle autorità di vigilanza.

Qualora l'opinione del team si fondi sull'output di un algoritmo non decifrabile, la posizione del revisore diventa professionalmente indifendibile; non è ammissibile l'inserimento nelle carte di lavoro di una mera presa d'atto della segnalazione automatica, priva di argomentazione critica che ne chiarisca i presupposti economico-aziendali. L'interpretabilità dei sistemi di intelligenza artificiale cessa di essere un semplice requisito tecnico, configurandosi come una condizione essenziale per un'adozione professionale che sia coerente con l'impianto normativo della revisione.

Per superare questo limite la ricerca scientifica sta dedicando una crescente attenzione al filone della Explainable AI (XAI). L'introduzione di strumenti metodologici come LIME (Local Interpretable Model-agnostic Explanations) e SHAP (SHapley Additive exPlanations) risponde proprio all'esigenza di rendere decifrabili le previsioni delle architetture black-box, fornendo al professionista una scomposizione locale dei fattori che hanno determinato la classificazione di una specifica anomalia. Il modello LIME, introdotto originariamente da Ribeiro, Singh e Guestrin (2016), opera modificando leggermente i dati di input di un singolo caso e osservando come cambiano le previsioni del software; ciò permette di costruire un modello lineare semplice facilmente interpretabile attorno a quella specifica decisione per spiegarne il risultato.

L'approccio SHAP, sviluppato da Lundberg e Lee (2017), si fonda sui principi matematici della teoria dei giochi cooperativi e sui valori di Shapley. Esso calcola l'apporto individuale e il peso relativo di ciascuna variabile aziendale nel determinare l'output finale garantendo una ripartizione equa e matematicamente rigorosa dell'importanza dei diversi fattori contabili esaminati dall'algoritmo. In un contesto di revisione pratico, SHAP potrebbe scomporre una segnalazione di rischio elevato su una specifica voce di bilancio in questo modo: il 42% del peso predittivo è attribuibile a un'anomalia nel rapporto tra ricavi e flussi di cassa operativi, il 31% a variazioni insolite nelle poste di credito verso clienti correlati, e il restante 27% a un pattern atipico nei tempi di incasso. Il revisore dispone così di un punto di partenza analitico concreto per orientare le proprie procedure di verifica sulle aree di bilancio a più alta incidenza di rischio, anziché distribuire uniformemente le risorse su un campione statistico privo di questa stratificazione per fattore.

Come evidenziato nello studio condotto da Murikah et al. (2024) in merito ai profili etici dei sistemi di intelligenza artificiale applicati all'audit, le risposte fornite da tali applicativi

rappresentano approssimazioni statistiche del processo decisionale effettivo del modello e non una trasparenza assoluta. Sussiste quindi il rischio operativo che il revisore interpreti i risultati di LIME o SHAP come una descrizione matematica esatta del percorso logico seguito dall'algoritmo, anziché come un'indicazione probabilistica di massima. Un simile fraintendimento conoscitivo può portare fuori strada, inducendo il team di revisione ad accettare la spiegazione tecnologica senza un adeguato riscontro sul piano contabile.

Altro limite tecnologico fondamentale risiede nella stretta dipendenza dalla qualità e dalla rappresentatività dei dati di addestramento. Poiché i modelli di machine learning estraggono le proprie regole predittive da database storici, l'eventuale presenza di informazioni distorte, incomplete o non omogenee determina l'automatica incorporazione di tali anomalie all'interno dei risultati finali. Nel contesto della fraud detection contabile questa vulnerabilità si manifesta attraverso tre dinamiche distinte.

Si rileva inizialmente un evidente effetto di selection bias nei dataset utilizzati per l'addestramento; le basi dati più diffuse nella letteratura scientifica includono esclusivamente gli illeciti che sono stati effettivamente scoperti e perseguiti dalle autorità. Le frodi rimaste latenti restano invisibili all'algoritmo, il quale finisce per specializzarsi nel riconoscimento delle sole irregolarità storicamente intercettate, riducendo l'efficacia predittiva di fronte a nuovi schemi manipolativi. A questa criticità si aggiunge il fenomeno del temporal drift, legato all'obsolescenza temporale dei dati. Le tecniche di manipolazione dei bilanci e le dinamiche operative aziendali evolvono rapidamente, un sistema addestrato su serie storiche non aggiornate rischia di avere una scarsa capacità di lettura di fronte a flussi contabili che sono condizionati da elementi più recenti.

Un'ulteriore barriera tecnica è rappresentata dal class imbalance (squilibrio di dati). Nei database usati per la revisione, i casi di frode sono pochissimi rispetto alla totalità delle transazioni regolari. Se il sistema non viene calibrato con precisione, rischia di ottimizzare l'accuratezza generale semplicemente classificando ogni operazione come corretta. Nei dataset tipici di fraud detection contabile il rapporto tra casi fraudolenti e conformi si colloca spesso tra 1 a 50 e 1 a 200. Un modello non calibrato che classifichi sistematicamente tutte le osservazioni come conformi ottiene un'accuratezza apparente del 98-99%, rivelandosi privo di utilità operativa in quanto privo della sensibilità necessaria per identificare proprio quelle rare anomalie che indicano un possibile illecito.

Le tecniche di oversampling come SMOTE (Synthetic Minority Over-sampling Technique) e di undersampling controllato sono oggi le soluzioni più diffuse per riequilibrare i dataset prima dell'addestramento, ma richiedono competenze specifiche che non tutti i team di revisione possiedono internamente.

Un terzo limite, di forte rilevanza per la professione del revisore, riguarda la possibilità di trasferire gli stessi modelli di intelligenza artificiale in contesti economici differenti. La maggior parte degli studi sono stati condotti utilizzando database di società quotate statunitensi, caratterizzate da assetti strutturali, in termini di trasparenza informativa, obblighi di disclosure e cultura contabile, distanti da quelli che qualificano il tessuto imprenditoriale europeo e, nello specifico, italiano. Un software addestrato sui dati della SEC statunitense possiede una validità circoscritta a quell'assetto regolamentare. La sua trasferibilità all'interno dello scenario nazionale, contraddistinto da una netta maggioranza di piccole e medie imprese (PMI), dall'applicazione dei principi contabili nazionali (OIC) accanto ai criteri internazionali (IAS/IFRS) e da prassi di verifica con specificità proprie, presenta forti elementi di incertezza. Senza un lavoro di adattamento alle caratteristiche e alle dimensioni delle nostre imprese, lo strumento tecnologico rischia di commettere molti errori segnalando finti problemi o non vedendo le anomalie tipiche del nostro mercato.

Le società di revisione devono quindi integrare l'intelligenza artificiale utilizzandola come uno strumento flessibile, da riparametrare sulla base delle reali dinamiche amministrative e dimensionali del mercato in cui operano. Solo attraverso questo sforzo di adattamento normativo e operativo è possibile garantire che i sistemi automatizzati rappresentino un reale supporto all'attività di vigilanza, minimizzando i rischi di distorsione del modello.

Le criticità legate all'inserimento di dati storici parziali o non perfettamente trasferibili si collegano direttamente al rischio di manipolazione mirata (adversarial manipulation) da parte del management della società. Sebbene l'alterazione intenzionale dei flussi contabili per aggirare i filtri tecnologici rappresenti una minaccia complessa, la sua progressiva transizione da ipotesi teorica a vulnerabilità concreta impone una profonda riflessione sulle metodologie di audit. Emerge la necessità di ripensare il livello di trasparenza da garantire alle imprese sottoposte a revisione in merito ai criteri di funzionamento dei software di controllo. Per evitare che la conoscenza dettagliata delle

soglie di allerta e dei parametri algoritmici si traduca in una guida per occultare eventuali irregolarità, i network di revisione dovranno adottare rigidi protocolli di riservatezza tecnologica. Mantenere l'opacità protettiva sulle logiche di estrazione e sui modelli predittivi aziendali diventa un presidio metodologico fondamentale per preservare l'effetto sorpresa e l'efficacia dello scetticismo professionale sul campo.

Infine, emerge un limite di natura etica e giuridica che viene analizzato con crescente urgenza, legato all'attribuzione delle responsabilità operative. Qualora un sistema di intelligenza artificiale generi una segnalazione di frode che si riveli successivamente infondata, le ripercussioni per l'impresa e per i soggetti coinvolti possono risultare particolarmente gravose, traducendosi in danni reputazionali, costi per investigazioni interne e forti tensioni relazionali con l'organo amministrativo e di controllo. In uno scenario simile, l'individuazione del soggetto chiamato a rispondere di tali esiti rimane complessa: ci si interroga se l'onere sia da imputare al singolo revisore che ha guidato l'analisi, al network che ha validato la tecnologia o al fornitore esterno che ha sviluppato l'algoritmo. L'assenza di un orientamento normativo e giurisprudenziale consolidato evidenzia come l'adozione di questi strumenti non azzeri la responsabilità professionale del revisore, ma la complichi, introducendo nuovi livelli di incertezza sulla titolarità delle conclusioni che derivano dall'interazione tra l'uomo e la macchina.

Alla luce di queste considerazioni, si può affermare che la tecnologia costituisce un supporto potente ma non infallibile, i cui vincoli devono essere compresi, documentati e gestiti con estrema trasparenza. Un professionista che utilizzi tali applicativi senza conoscerne i presupposti statistici, i potenziali condizionamenti e i limiti di trasferibilità geografica e dimensionale non esercita un giudizio informato, rischia di delegare passivamente le proprie valutazioni all'algoritmo, assecondando e rendendo sistematico proprio quell'effetto di automation bias che rappresenta la principale minaccia per l'efficacia della revisione contabile.

4.4 Il quadro regolatorio che risponde all’uso di IA nell’audit

L'analisi dei rischi cognitivi e dei limiti tecnici presenti nei modelli di machine learning evidenzia una delle critiche più frequenti mosse dalla dottrina alla risposta istituzionale, incentrata sul ritardo rispetto alla velocità con cui la tecnologia si è diffusa nella pratica operativa. I principali network di revisione hanno iniziato a incorporare

strumenti di intelligenza artificiale all'interno delle proprie metodologie prima che i regolatori e gli standard setter producessero indicazioni specifiche su come gestire tali soluzioni in modo responsabile. Lo sfasamento temporale tra l'innovazione tecnologica e l'adeguamento normativo ha generato una zona grigia in cui i professionisti si sono trovati a operare senza un quadro di riferimento consolidato, dovendo delineare autonomamente risposte a quesiti metodologici nuovi per l'intero settore.

Negli ultimi anni le autorità di regolamentazione internazionale hanno avviato un percorso volto a colmare questo divario, anche se ognuno a modo suo e con tempi diversi. L'assetto che sta emergendo, per quanto non ancora del tutto organico o definitivo, riflette una crescente consapevolezza verso la transizione digitale dell'audit che non può essere delegata interamente all'iniziativa dei singoli operatori, ma necessita di regole chiare per preservare la pubblica fiducia e l'affidabilità delle relazioni di bilancio.

L'International Auditing and Assurance Standards Board (IAASB), l'organismo deputato all'emanazione dei principi di revisione internazionali recepiti anche nell'ordinamento italiano, ha inserito l'innovazione tecnologica tra le proprie priorità strategiche per il quadriennio 2024-2027. Già a partire dall'ottobre 2024, con la pubblicazione della propria Technology Position, il board ha avviato un'analisi continuativa per valutare se le regole vigenti siano in grado di coprire i progressi tecnologici, inclusa l'intelligenza artificiale. In questo perimetro, nel giugno 2025 è stata lanciata la Technology Quality Management Initiative, un progetto finalizzato a esplorare l'impatto dei sistemi emergenti sulla gestione della qualità degli incarichi. I tavoli di lavoro globali condotti nel corso del 2025 hanno coinvolto oltre 240 stakeholder a livello internazionale, focalizzando l'attenzione sulle sfide di governance, sul controllo dei rischi e sui presidi necessari a preservare l'affidabilità delle verifiche (IAASB, 2025). Tra i temi emersi con maggiore frequenza nelle consultazioni figura la necessità di definire standard specifici per la documentazione dell'uso degli strumenti algoritmici nelle carte di lavoro: quando e come il revisore deve registrare che una determinata conclusione deriva dall'output di un modello predittivo, quali verifiche indipendenti devono essere effettuate prima di fare affidamento su quella segnalazione, e come deve essere documentata la valutazione critica del professionista sull'affidabilità dello strumento nel contesto specifico dell'incarico. La linea d'azione privilegiata dallo IAASB non prevede lo sviluppo di un principio di revisione autonomo e specificamente dedicato all'intelligenza

artificiale in quanto una simile scelta richiederebbe tempi di approvazione estremamente dilatati, con il rischio di produrre un impianto normativo già obsoleto al momento della sua emanazione. L'orientamento attuale si focalizza sull'integrazione delle considerazioni tecnologiche all'interno degli standard già esistenti e nei progetti di revisione in corso.
Questo approccio garantisce flessibilità e tempestività, ma introduce il rischio che le indicazioni rimangano troppo generali per essere operative nella pratica quotidiana. Gli orientamenti rischiano di non offrire ai professionisti quel grado di specificità tecnica necessario a gestire casistiche concrete, come la rendicontazione e la documentazione dell'utilizzo di un modello di machine learning all'interno delle carte di lavoro. I riscontri emersi dalle consultazioni del 2025 hanno confermato questa parziale distanza; pur riconoscendo che le attuali regole sulla gestione della qualità costituiscono una solida base di partenza, gli operatori del settore segnalano l'urgenza di emanare linee guida pratiche e materiali di supporto che calino i principi generali nella realtà quotidiana dell'audit automatizzato.

Il Public Company Accounting Oversight Board (PCAOB), l'organismo di vigilanza sui revisori delle società quotate negli Stati Uniti, ha delineato un percorso in parte differente e contraddistinto da un approccio orientato alla pratica nel rispondere all'evoluzione tecnologica. Nel corso del 2025 il PCAOB ha formalizzato proposte incentrate sull'utilizzo dei sistemi tecnologici e sull'applicazione avanzata della data analytics nelle procedure di audit, muovendosi in parallelo rispetto ai progetti di ricognizione avviati dallo IAASB. Il percorso dell'autorità americana verso la definizione di linee guida sull'intelligenza artificiale ha trovato un impulso decisivo nella costituzione, avvenuta nel 2022, del Technology Innovation Alliance Working Group (TIA). Questo comitato composto da esperti esterni con competenze specialistiche nelle tecnologie emergenti ha ricevuto il mandato di elaborare raccomandazioni strategiche su come adattare i programmi di vigilanza all'impiego dei dati strutturati e dei modelli di intelligenza artificiale, sia nella redazione dei bilanci da parte delle imprese sia nell'esecuzione delle verifiche da parte dei revisori. Le conclusioni del gruppo di lavoro, rese pubbliche nel 2024, hanno dato inizio a una nuova fase nel dibattito regolatorio evidenziando la disponibilità del PCAOB a emendare i propri standard professionali per recepire l'impiego dei nuovi strumenti tecnologici (PCAOB, 2024).
La postura del PCAOB su questo tema risente delle complessità intrinseche al contesto

istituzionale statunitense, condizionato nel 2025 da significativi accadimenti nella governance interna dell'organismo. La dialettica tra l'obiettivo di promuovere l'innovazione tecnologica nell'audit e la necessità di garantire presidi di qualità estremamente rigorosi costituisce uno dei nodi centrali del dibattito attuale. La risoluzione di tale equilibrio produce implicazioni profonde, oltre che per il mercato finanziario americano, anche per le prassi operative internazionali, considerato il peso specifico che gli standard del PCAOB esercitano sulle metodologie globali dei principali network di revisione.

Sul versante europeo, la risposta più strutturata e ambiziosa alle sfide poste dall'innovazione tecnologica proviene dal quadro normativo generale sulla digitalizzazione: il Regolamento europeo sull'intelligenza artificiale, noto come EU AI Act. Entrato in vigore il 1° agosto 2024, il testo prevede un'introduzione progressiva delle sue diverse disposizioni, con la cruciale scadenza del 2 agosto 2026 per l'applicazione delle regole relative ai sistemi classificati ad alto rischio. L'impianto normativo si fonda su pilastri rigorosi, quali la proporzionalità basata sul rischio, la trasparenza, la non discriminazione, la tutela dei dati personali e la necessità di una costante supervisione umana (Regolamento UE 2024/1689). Il regolamento adotta un approccio piramidale incentrato sul rischio, catalogando le applicazioni tecnologiche in quattro macrocategorie (rischio inaccettabile, alto rischio, rischio limitato e rischio minimo) e prevedendo adempimenti crescenti al crescere della potenziale pericolosità del sistema. Per la revisione legale è importante stabilire l'esatta collocazione dei software impiegati nelle procedure di audit. Sebbene la classificazione non sia ancora definita in modo univoco nella prassi interpretativa, i sistemi utilizzati in contesti che producono valutazioni con effetti significativi su terzi, come i modelli predittivi per l'identificazione delle frodi o per lo screening dei rischi di bilancio, presentano forti presupposti per essere qualificati come sistemi ad alto rischio, scontando di conseguenza stringenti obblighi di documentazione e trasparenza.

Il principio dello human in the loop emerge come una delle condizioni cardine per l'utilizzo dei sistemi ad alto rischio. La normativa europea impone l'implementazione di presidi che consentano l'intervento e il controllo umano lungo l'intero processo decisionale, determinando una perfetta convergenza con le responsabilità dell'auditor delineate dall'ISA Italia 240: lo strumento algoritmico può supportare e ottimizzare

l'attività di campionamento o di analisi dei flussi contabili, ma la responsabilità giuridica e professionale del giudizio finale rimane in capo alla persona fisica designata a firmare la relazione di revisione.

Nel contesto europeo, le organizzazioni professionali sono tenute a censire e classificare i software integrati nelle proprie metodologie di verifica, produrre una rendicontazione tecnica dettagliata sulle logiche di funzionamento dei modelli adottati, formalizzare i protocolli di supervisione umana e sottoporsi a verifiche periodiche di conformità. Si tratta di un onere amministrativo e operativo di notevole entità che risulta sostenibile per le strutture multinazionali delle Big Four ma rischia di penalizzare le società di revisione più piccole, prive di risorse dedicate alla gestione di processi di compliance così articolati. Una società di revisione di medie dimensioni che utilizzi un sistema proprietario di ML per l'anomaly detection sui dati contabili dei propri clienti dovrà, entro agosto 2026, produrre documentazione tecnica sul funzionamento del modello, implementare un sistema di monitoraggio continuo delle sue prestazioni, designare un responsabile della supervisione umana degli output e predisporre procedure di gestione degli incidenti nel caso in cui il sistema produca segnalazioni errate con conseguenze rilevanti per il cliente. Requisiti analoghi a quelli già in vigore nel settore bancario e assicurativo sotto la normativa DORA.

Il quadro regolatorio internazionale è in profonda transizione. Le autorità di vigilanza e gli standard setter riconoscono l'urgenza di governare la trasformazione tecnologica dell'audit ma le risposte attualmente formulate mantengono un carattere prevalentemente generale, spesso non vincolante, evidenziando un marcato ritardo rispetto alla rapidità con cui i sistemi di intelligenza artificiale si sono consolidati nella pratica quotidiana. L'emanazione di regole professionali specificamente dedicate alla validazione dei modelli algoritmici, alla standardizzazione dei requisiti di documentazione e ai protocolli operativi a tutela dello scetticismo si trova ancora in una fase di sviluppo. Questa parziale frammentazione normativa trasferisce un rilevante onere di autoregolamentazione in capo ai professionisti e ai network di revisione, chiamati a delineare internamente le proprie policy e le procedure di controllo in assenza di un orientamento regolatorio consolidato. Si tratta di una responsabilità complessa, che impone il possesso di elevate competenze tecniche e di capacità di interpretare i principi etici che devono governare l'applicazione di tali strumenti.

4.5 Le prospettive future verso un modello di revisione ibrido

Le evidenze esaminate nei precedenti paragrafi delineano un quadro metodologico complesso e apparentemente divergente. Gli strumenti di intelligenza artificiale offrono capacità di analisi senza precedenti, in grado di superare i limiti strutturali presenti nell'audit tradizionale da decenni, ma l'introduzione di queste tecnologie genera profili di rischio da considerare attentamente; l'automation bias, l'opacità dei processi decisionali delle macchine e le incertezze sull'attribuzione della responsabilità professionale rischiano, se non gestiti, di produrre l'effetto opposto a quello desiderato, indebolendo la funzione di tutela dell'informazione finanziaria. La dottrina contabile supera questo problema orientandosi verso una soluzione strategica: la transizione digitale, invece di imporre un'alternativa tra l'operatore umano e l'algoritmo, deve guidare alla progettazione di un modello di integrazione tra i due soggetti.

La combinazione delle due componenti, definita modello ibrido, si caratterizza per una divisione del lavoro che deriva da una scelta esplicita in merito alle attività da delegare all'automazione e alle prerogative da riservare al giudizio professionale. La letteratura conferma in modo coerente il potenziale dei sistemi avanzati nel migliorare l'efficienza e l'intercettazione degli illeciti, emergono però dei lati negativi evidenti tra i guadagni di produttività e i pericoli derivanti da un eccessivo affidamento tecnologico senza verifiche indipendenti. Diventa essenziale che i revisori adottino schemi operativi in cui il supporto della tecnologia sia costantemente subordinato al controllo critico del professionista, mentre le autorità di vigilanza sono chiamate a emanare linee guida flessibili in tema di trasparenza e accountability.

Per comprendere nella pratica tale integrazione, è utile osservare come l'attività professionale stia già distinguendo i diversi gradi di autonomia della tecnologia. Attualmente, le soluzioni di intelligenza artificiale generativa operano principalmente in una logica di assistenza; i team di audit ricorrono ad essa per redigere bozze documentali, condurre ricerche preliminari o effettuare screening di base, mantenendo l'obbligo di rivedere e validare ogni output. L'evoluzione successiva è rappresentata dai flussi di lavoro in cui i software manifestano la capacità di completare interi processi in autonomia, richiedendo l'intervento dell'operatore solo in presenza di eccezioni o anomalie complesse. La maggior parte dei network di revisione preferisce attestarsi sulla

fase assistenziale, consolidando la familiarità con i report generati dall'algoritmo prima di valutare l'automazione di intere procedure (Sundarasen et al., 2026).

Nel campo della fraud detection, questa distinzione assume un rilievo centrale. All'interno delle metodologie di machine learning e di continuous auditing, l'approccio assistenziale rimane quello prevalente: l'algoritmo identifica le anomalie e calcola le probabilità di rischio, ma la decisione strategica su come procedere, se estendere i campionamenti, coinvolgere la governance o considerare l'anomalia rilevante ai fini del giudizio finale, resta una prerogativa esclusiva del revisore. Un esempio concreto di questo modello in azione può essere che il sistema segnala un'anomalia statisticamente significativa nel saldo dei crediti verso clienti di una società manifatturiera, con una probabilità di irregolarità stimata al 78%. Il revisore non si limita ad accettare o scartare la segnalazione, ma è chiamato ad analizzare le variabili di contesto, valutando se l'entità abbia recentemente acquisito una nuova linea di business, se i termini di pagamento settoriali abbiano subito variazioni o se lo scostamento sia riconducibile a fattori operativi legittimi. Solo dopo questa valutazione decide se approfondire con procedure specifiche o documentare la propria valutazione critica a giustificazione del mancato follow-up. Un'evoluzione verso configurazioni in cui il sistema, oltre a segnalare, agisce autonomamente (ad esempio inviando richieste automatiche di chiarimenti al management o attivando procedure di approfondimento standardizzate), è tecnicamente percorribile. Nonostante ciò, questa soluzione viene vista ancora con estrema cautela a causa delle delicate implicazioni in termini di responsabilità giuridica e di tenuta dello scetticismo professionale.

L'evoluzione storica della tecnologia applicata alla revisione contabile dimostra che l'innovazione si è sempre tradotta in un percorso di avanzamento e implementazione rispetto a prima e quasi mai come una sostituzione del professionista umano. L'introduzione dei sistemi ERP aziendali ha automatizzato la registrazione delle transazioni e la reportistica di base, ma tale mutamento non ha eroso le competenze contabili, ha trasformato i revisori in esperti di processi di business e in advisor strategici. L'intelligenza artificiale non elimina la necessità di revisori qualificati ma rimuove l'esigenza di impiegarli in mansioni ripetitive e a basso valore aggiunto. Ogni volta che l'innovazione ha automatizzato una fase del processo di audit, il tempo liberato è stato

reinvestito in attività a più alto contenuto professionale, spostando verso l'alto il baricentro delle competenze richieste.

L'attuale fase di transizione non si presenta automatica né priva di costi. Il settore sta attraversando una profonda crisi della forza lavoro, contrassegnata da una significativa contrazione nel numero di candidati agli esami di abilitazione e dall'uscita di numerosi professionisti dal comparto. In questo scenario, in cui l'avvento dell'assurance continua e della valutazione perpetua del rischio sta sostituendo le tradizionali verifiche di fine periodo, gli strumenti tecnologici smettono di essere una mera opportunità di efficienza sui costi. L'intelligenza artificiale diventa una necessità strutturale per consentire alle società di revisione di compensare la carenza di personale e garantire la continuità e la qualità del servizio di vigilanza.

Le competenze del revisore del futuro rappresentano il punto di convergenza dell'intera analisi. Accanto ai requisiti tradizionali, assume un ruolo centrale la familiarità con la data analytics, la cybersecurity e il funzionamento degli algoritmi. Il professionista deve essere in grado di interpretare la logica interna dei modelli, validarne i risultati e valutarne i rischi intrinseci. Al contempo, le doti relazionali e il pensiero strategico acquisiscono un'importanza crescente; saper tradurre le anomalie quantitative in chiare narrazioni di rischio aziendale diventa un fattore discriminante. Il profilo emergente non coincide né con quello di un tecnico puro né con quello di un contabile tradizionale estraneo all'innovazione, ma si sostanzia in una figura ibrida in grado di trasformare un output algoritmico in un giudizio professionale motivato e, specularmente, di tradurre un dubbio di audit in una richiesta dettagliata per la macchina (Jones et al., 2026).

Il legame tra innovazione tecnologica e lotta alle frodi, oltre ad essere una questione di efficienza o di software più veloci, tocca da vicino il valore stesso della revisione contabile. L'errore più grande che si potrebbe commettere nei prossimi anni è pensare che un algoritmo possa sostituire la responsabilità dell’uomo. Se una macchina dovesse segnalare un'anomalia in modo matematicamente perfetto, spetterà comunque sempre al revisore capire il contesto, parlare con il management, interpretare le sfumature e, infine, assumersi il rischio di firmare la relazione finale. La tecnologia è e rimarrà un mezzo straordinariamente utile, ma la risposta finale non sarà mai tecnologica, sarà sempre professionale, etica e umana.

Conclusioni

Il presente lavoro di ricerca prende spunto da una constatazione che i dati empirici confermano con regolarità: le frodi contabili continuano a non essere rilevate tempestivamente attraverso i canali ordinari della revisione esterna, e i limiti strutturali che ne sono alla base (il campionamento periodico, l'approccio ex-post, la vulnerabilità cognitiva dello scetticismo professionale) non sono superabili attraverso semplici aggiustamenti incrementali del modello esistente. L'obiettivo del lavoro è valutare se e in che misura gli strumenti tecnologici oggi disponibili, quali machine learning, natural language processing e continuous auditing, siano in grado di rispondere a questi limiti, e quali rischi e implicazioni accompagnino la loro adozione nella pratica professionale quotidiana all'interno dei team di verifica. Il metodo adottato, basato sulla narrative review di 42 articoli selezionati attraverso un'estrazione su Scopus, ha permesso di costruire un'analisi che tiene insieme tre filoni di letteratura distinti: quello empirico-quantitativo sugli algoritmi di fraud detection, quello comportamentale sull'impatto dell'automazione sullo scetticismo professionale, e quello normativo sull'evoluzione del quadro regolatorio internazionale.

Dal punto di vista tecnologico, la letteratura documenta evidenze empiriche molto solide. Il machine learning applicato ai dati contabili grezzi supera nettamente i metodi statistici tradizionali nella rilevazione delle false comunicazioni sociali. Modelli avanzati, addestrati su serie storiche e ampi database sanzionatori istituzionali, dimostrano la capacità di anticipare l'allerta precoce sulla frode fino a due anni prima della sua emersione pubblica, garantendo incrementi significativi nell'accuratezza predittiva rispetto alla regressione logistica benchmark. Il natural language processing aggiunge un contributo informativo autonomo e complementare, poiché l'analisi del tono linguistico e delle alterazioni semantiche nelle sezioni narrative delle relazioni sulla gestione e delle MD&A societarie migliora sensibilmente la capacità predittiva rispetto ai soli dati quantitativi, identificando tempestivamente le manovre di gestione opportunistica degli utili. Inoltre, il continuous auditing risponde al limite temporale più critico dell'audit periodico, ossia la finestra di esposizione alla frode, trasformando la logica del controllo da ex-post a monitoraggio in tempo reale. L'implementazione di queste architetture algoritmiche integrate direttamente con i sistemi ERP aziendali permette di abbattere drasticamente i cicli di verifica transazionale da diverse settimane a meno di sei giorni,

veicolando flussi transazionali costantemente aggiornati e classificando le segnalazioni per livelli di urgenza all'interno delle dashboard a disposizione dei revisori.

Sul piano professionale e operativo la stessa letteratura documenta rischi di forte rilievo metodologico che non possono essere ignorati. L'automation bias si configura come la vulnerabilità più rilevante e spesso sottovalutata nella pratica degli studi professionali, traducendosi in una contrazione del 35% nei livelli di scetticismo professionale tra i revisori esposti a un uso intensivo e acritico degli strumenti algoritmici, con la tendenza a stabilizzarsi come comportamento ordinario indotto dalla routine tecnologica. L'impatto dell'automazione sullo scetticismo appare condizionato in modo significativo dal tratto individuale e dall'esperienza del professionista sul campo: i profili con una spiccata propensione allo scetticismo utilizzano l'intelligenza artificiale come un potente amplificatore delle proprie capacità d'indagine, mentre i profili con minore attitudine critica o più junior rischiano di utilizzarla come un passivo sostituto del proprio giudizio. A ciò si aggiungono i bias algoritmici intrinseci, quali il selection bias nei dataset di addestramento, il temporal drift dovuto all'obsolescenza dei dati storici e il profondo class imbalance nei dataset di fraud detection, che rischiano di produrre modelli con un'accuratezza apparente molto elevata ma privi della sensibilità necessaria per identificare proprio quelle rare anomalie transazionali che indicano un possibile illecito. Sotto questo profilo, la quasi totale assenza di studi empirici su contesti europei e l'assenza totale di casistiche italiane confermano che i modelli addestrati su dataset esteri non sono direttamente trasferibili al tessuto delle piccole e medie imprese nazionali, caratterizzato dalla prevalenza di principi contabili OIC, da una governance concentrata e da prassi di verifica con specificità proprie. Le implicazioni teoriche e di policy che emergono da questo quadro evidenziano un divario geografico nella letteratura, dominata da mercati anglosassoni o asiatici, che limita la generalizzabilità delle conclusioni e segnala un'area di ricerca prioritaria per i prossimi anni.

Per quanto riguarda il piano normativo, le autorità di regolamentazione internazionale e il legislatore europeo stanno rispondendo alla trasformazione tecnologica con approcci diversi e con tempistiche che faticano a stare al passo con la velocità di diffusione degli strumenti nella pratica professionale quotidiana. Lo IAASB, pur avendo avviato iniziative strategiche sulla gestione della qualità coinvolgendo numerosi stakeholder globali, ha optato per l'integrazione delle considerazioni tecnologiche

all'interno dei principi esistenti (come l'ISA Italia 240) anziché sviluppare un principio autonomo, lasciando talvolta una parziale distanza rispetto alle esigenze di rendicontazione pratica nelle carte di lavoro. Sul versante europeo, l'EU AI Act impone obblighi di trasparenza e supervisione umana estremamente rigorosi entro la scadenza del 2 agosto 2026 per i sistemi classificati ad alto rischio, delineando requisiti di compliance analoghi alla normativa DORA nel settore finanziario. Tali oneri amministrativi e operativi, pur risultando sostenibili per le strutture multinazionali delle Big Four, rischiano di penalizzare fortemente le società di revisione di medie e piccole dimensioni, prive di risorse dedicate alla gestione di processi di compliance così articolati.

Le indicazioni operative per la gestione quotidiana dell'attività di audit si articolano lungo tre direttrici essenziali, richiedendo un ripensamento strutturale che riguarda in primo luogo la formazione del team di verifica, il quale deve sviluppare una chiara consapevolezza dei rischi di automation bias e dei meccanismi di funzionamento degli algoritmi, mantenendo costanti protocolli di verifica indipendente e campionamenti obbligatori slegati dalle segnalazioni della macchina nelle aree a più alto rischio o di potenziale management override. Questa attenzione allo sviluppo delle competenze si riflette direttamente sul design e sulla trasparenza degli strumenti adottati, ambito in cui i sistemi di Explainable AI (come LIME e SHAP) cessano di essere opzioni accessorie per configurarsi come presupposti metodologici necessari; solo la scomposizione dei fattori predittivi consente al revisore di motivare e documentare le proprie conclusioni nelle carte di lavoro, superando l'opacità dei modelli black-box. Ne consegue che l'intera strategia di integrazione debba convergere verso il modello ibrido (human-in-the-loop) come unico approccio capace di garantire l'efficacia computazionale della fraud detection e la contemporanea tenuta dello scetticismo professionale, sottomettendo costantemente l'indizio algoritmico al giudizio critico del revisore umano.

Le risultanze e le analisi risentono inevitabilmente della fisiologica delimitazione del perimetro metodologico adottato, a partire dalla scelta della narrative review che, per quanto ottimale nel governare l'intersezione tra ambiti disciplinari eterogenei e in rapida accelerazione, predilige una sintesi concettuale e interpretativa rispetto alla mappatura puramente meccanica o cumulativa delle fonti. La marcata concentrazione geografica della letteratura disponibile rende i modelli discussi strutturalmente più rispondenti ai contesti regolamentati statunitensi rispetto alle specificità del mercato della revisione

nazionale. Queste stesse evidenze delineano le traiettorie d'elezione per gli sviluppi della ricerca scientifica futura, evidenziando l'urgenza di avviare studi empirici condotti su campioni interamente europei e italiani, atti a testare l'efficacia del machine learning su database di bilancio redatti secondo i principi contabili OIC e all'interno di strutture aziendali tipicamente non quotate o a controllo concentrato. Parallelamente, emerge la necessità di progettare e validare sul campo protocolli operativi strutturati per mitigare l'assuefazione tecnologica nei profili più junior, verificando se e in che misura le interfacce basate sulla spiegabilità algoritmica preservino l'attitudine critica del revisore. Sul piano istituzionale, infine, la reazione concreta della professione e degli studi professionali davanti ai vincoli amministrativi e tecnici imposti dall'imminente applicazione dell'EU AI Act si configura come un campo d'indagine aperto e cruciale, il cui esito andrà a ridefinire gli assetti strutturali e gli equilibri competitivi del settore dell'auditing per i prossimi decenni.

In definitiva, le evidenze analizzate suggeriscono che l'intelligenza artificiale non rappresenti una semplice innovazione tecnologica applicata alla revisione, bensì un cambiamento strutturale nel modo in cui il rischio di frode viene identificato, monitorato e gestito. Le tecnologie esaminate dimostrano di poter superare alcuni dei principali limiti dell'audit tradizionale, ampliando la capacità di analisi e migliorando la tempestività nell'individuazione delle anomalie. Allo stesso tempo, la letteratura evidenzia come il valore della revisione continui a dipendere dalla capacità del professionista di interpretare criticamente le evidenze disponibili, contestualizzarle e trasformarle in un giudizio motivato. Il futuro della professione non sembra quindi orientato verso la sostituzione del revisore da parte dell'algoritmo, ma verso l'affermazione di un modello di collaborazione in cui la potenza computazionale dell'intelligenza artificiale e il giudizio professionale umano operano in modo complementare, rafforzandosi reciprocamente nel perseguimento di una più efficace prevenzione e individuazione delle frodi.

Bibliografia

Abdo-Salloum A.M., Chehade S., 2026, "The Role of Artificial Intelligence in Transforming Accounting and Auditing Practices: A Systematic Review", SAGE Open. https://doi.org/10.1177/21582440251403296

Achakzai M.A.K., Peng J., 2023, "Detecting financial statement fraud using dynamic ensemble machine learning", International Review of Financial Analysis, Vol. 89, 102827. https://doi.org/10.1016/j.irfa.2023.102827

Akther T., Xu F., 2020, "Existence of the Audit Expectation Gap and Its Impact on Stakeholders' Confidence: The Moderating Role of the Financial Reporting Council", International Journal of Financial Studies, Vol. 8, n. 4.

Alles M., 2015, "Drivers of the Use and Facilitators and Obstacles of the Evolution of Big Data by the Audit Profession", Accounting Horizons, Vol. 29, n. 2, pp. 439-449. https://doi.org/10.2308/acch-51067

Alles M., Brennan G., Kogan A., Vasarhelyi M.A., 2006, "Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens", International Journal of Accounting Information Systems, Vol. 7, n. 2, pp. 137-161. https://doi.org/10.1016/j.accinf.2005.10.004

Association of Certified Fraud Examiners (ACFE), 2022, Occupational Fraud 2022: A Report to the Nations, Austin, TX.

Association of Certified Fraud Examiners (ACFE), 2024, Occupational Fraud 2024: A Report to the Nations, Austin, TX. Risorsa web reperibile all'indirizzo: https://www.acfe.com/report-to-the-nations/2024/ (consultato 5 marzo 2026).

Association of Certified Fraud Examiners (ACFE), 2026, Occupational Fraud 2026: A Report to the Nations, Austin, TX.

Bao Y., Ke B., Li B., Yu Y.J., Zhang J., 2020, "Detecting Accounting Fraud in Publicly Traded U.S. Firms Using a Machine Learning Approach", Journal of Accounting Research, Vol. 58, n. 1, pp. 199-235. https://doi.org/10.1111/1475-679X.12292

Barr-Pulliam D., Calvin C.G., Eulerich M., Maghakyan A., 2024, "Audit evidence, technology, and judgement: A review of the literature in response to ED-500", Journal of International Financial Management & Accounting, Vol. 35, pp. 36-67.

Bhattacharya M., Mickovic A., 2024, "Accounting fraud detection using contextual language learning", Journal of Accounting and Public Policy. https://doi.org/10.1016/j.jaccpubpol.2024.107184

Bonrath A., Eulerich M., 2024, "Internal auditing's role in preventing and detecting fraud: An empirical analysis", International Journal of Auditing, Vol. 28, n. 4, pp. 615-631.

Brickey K.F., 2003, "From Enron to WorldCom and Beyond: Life and Crime after Sarbanes-Oxley", Washington University Law Quarterly, Vol. 81, n. 2, pp. 357-402.

Burlacu G., Robu I.-B., Anghel I., Rogoz M.E., Munteanu I., 2025, "The Use of the Fraud Pentagon Model in Assessing the Risk of Fraudulent Financial Reporting", Risks, Vol. 13, 102.

Cai T., 2024, "Continuous Auditing and Risk Monitoring", ISACA Journal, Vol. 5.

Cambaza E.M., 2024, "The Parmalat Scandal: An Analysis of Financial Deception and Its Implications for Global Business", REVES - Revista Relações Sociais.

Campa D., Quagli A., Ramassa P., 2025, "The roles and interplay of enforcers and auditors in the context of accounting fraud: a review of the accounting literature", Journal of Accounting Literature, Vol. 47, n. 5, pp. 151-183. https://doi.org/10.1108/JAL-07-2023-0134

Chimonaki C., Papadakis S., Lemonakis C., 2023, "Perspectives in fraud theories - A systematic review approach", Corporate Governance and Organizational Behavior Review.
CNDCEC / Consob / MEF, 2020, Principio di Revisione Internazionale (ISA Italia) n. 240: "Le responsabilità del revisore relativamente alle frodi nella revisione contabile del bilancio".
Colbert J.L., 2000, "International and US standards: error and fraud", Managerial Auditing Journal, Vol. 15, n. 3, pp. 97-107.
Cressey D.R., 1953, Other People's Money: A Study in the Social Psychology of Embezzlement, Free Press, Glencoe (IL).
Decreto Legislativo 27 gennaio 2010, n. 39, Attuazione della direttiva 2006/43/CE relativa alla revisione legale dei conti annuali, Gazzetta Ufficiale n. 42 del 19 febbraio 2010.
Deliu D., 2024, "Professional Judgment and Skepticism Amidst the Interaction of Artificial Intelligence and Human Intelligence", Audit Financiar, Vol. 22, n. 176, pp. 724-741.
Dorminey J., Fleming A.S., Kranacher M.-J., Riley R.A., 2012, "The Evolution of Fraud Theory", Issues in Accounting Education, Vol. 27, n. 2, pp. 555-579.
Enget K.A., 2015, Indicators of fraud detection proficiency and their impact on auditor judgments in fraud risk assessments and audit plan modifications, Doctoral dissertation, Virginia Polytechnic Institute and State University.
Epstein B., 2019, The Development of the "Cressey Fraud Risk Triangle" Model and Its Variants.
Ergun M., 2025, "Financial Statement Fraud Detection via Large Language Models", Intelligent Systems in Accounting, Finance and Management. https://doi.org/10.1002/isaf.70021
Gkegkas M., Pazarskis M., 2025, "Using Data Analytics in Financial Statement Fraud Detection and Prevention: A Systematic Review", Journal of Risk and Financial Management, Vol. 18, n. 11, 598.
Hammersley J.S., 2011, "A Review and Model of Auditor Judgments in Fraud-Related Planning Tasks", Auditing: A Journal of Practice & Theory, Vol. 30, n. 4, pp. 101-128.
Hassink H.F.D., Bollen L.H., Meuwissen R.H.G., de Vries M.J., 2009, "Corporate fraud and the audit expectations gap: A study among business managers", Journal of International Accounting, Auditing and Taxation, Vol. 18, n. 2.
Hogan C.E., Rezaee Z., Riley R.A., Velury U.K., 2008, "Financial Statement Fraud: Insights from the Academic Literature", Auditing: A Journal of Practice & Theory, Vol. 27, n. 2, pp. 231-252.
Homer E.M., 2020, "Testing the fraud triangle: a systematic review", Journal of Financial Crime, Vol. 27, n. 1, pp. 172-187.
Huang A.H., Wang H., Yang Y., 2022, "FinBERT: A Large Language Model for Extracting Information from Financial Text", Contemporary Accounting Research.
Huang S.Y., Lin C.C., Chiu A.A. et al., 2017, "Fraud detection using fraud triangle risk factors", Information Systems Frontiers, Vol. 19, pp. 1343-1356.
IAASB, 2009, ISA 240 (Redrafted) - The Auditor's Responsibility to Consider Fraud in an Audit of Financial Statements, International Auditing and Assurance Standards Board.

IAASB, 2025, Technology Quality Management Initiative. Risorsa web reperibile all'indirizzo: https://www.iaasb.org/focus-areas/technology (consultato marzo 2026).
ICAEW, 2020, Fraudulent Financial Reporting: Fresh Thinking, Institute of Chartered Accountants in England and Wales.
International AI Safety Report, 2026. Risorsa web reperibile all'indirizzo: https://arxiv.org/pdf/2602.21012 (consultato aprile 2026).
ISACA, 2025, No Looking Back: Transforming Audit with Artificial Intelligence. Risorsa web reperibile all'indirizzo: https://www.isaca.org (consultato marzo 2026).
Issa H., Sun T., Vasarhelyi M.A., 2016, "Research Ideas for Artificial Intelligence in Auditing: The Formalization of Audit and Workforce Supplementation", Journal of Emerging Technologies in Accounting, Vol. 13, n. 2, pp. 1-20. https://doi.org/10.2308/jeta-10511
Jones S., Free C., 2026, "What accountants need to know about artificial intelligence and machine learning: a review and call for future research", Journal of Accounting Literature, Vol. 48, n. 5, pp. 133-158. https://doi.org/10.1108/JAL-12-2025-0693
Kokina J., Blanchette S., Davenport T.H., 2025, "Challenges and Opportunities for Artificial Intelligence in Auditing: Evidence from the Field", International Journal of Accounting Information Systems, Vol. 56, 100734.
Lim W.M. et al., 2025, "The role of artificial intelligence in auditing and fraud detection in accounting information systems", International Journal of Organizational Analysis, Vol. 38.
Loughran T., McDonald B., 2011, "When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks", Journal of Finance, Vol. 66, n. 1, pp. 35-65. https://doi.org/10.1111/j.1540-6261.2010.01625.x
Loughran T., McDonald B., 2016, "Textual Analysis in Accounting and Finance: A Survey", Journal of Accounting Research, Vol. 54, n. 4, pp. 1187-1230.
Lu Y., Hao J., Tang X., 2025, "Dual-model synergy for audit opinion prediction: A collaborative LLM agent framework approach", International Review of Economics & Finance, 104642.
Luo Y. et al., 2025, "Financial Statement Fraud Detection by Integrating Supervisory Punishment Reports Into Machine Learning Methods: Evidence From China", Accounting & Finance. https://doi.org/10.1111/acfi.70097
Lundberg S.M., Lee S.I., 2017, "A Unified Approach to Interpreting Model Predictions", Advances in Neural Information Processing Systems (NeurIPS 2017).
Mardessi S., 2023, "Big Data analytics and financial reporting quality: qualitative evidence from Canada", Journal of Financial Reporting and Accounting.
Marks J.T., 2012, The Mind of a Fraudster, Crowe Horwath LLP.
Minkkinen M., Laine J., Mäntymäki M., 2022, "Continuous Auditing of Artificial Intelligence: a Conceptualization and Assessment of Tools and Frameworks", Digital Society, Vol. 1, 21. https://doi.org/10.1007/s44206-022-00022-2
Mökander J., Axente M., Casolari F., Floridi L., 2021, "Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation", Minds and Machines, Vol. 32, pp. 733-748.
Murikah W., Nthenge J.K., Musyoka F.M., 2024, "Bias and Ethics of AI Systems Applied in Auditing: A Systematic Review", Scientific African, Vol. 25, e02281. https://doi.org/10.1016/j.sciaf.2024.e02281

Munter P., 2022, The auditor's responsibility for fraud detection, US Securities and Exchange Commission. Risorsa web reperibile all'indirizzo: https://www.sec.gov/newsroom/speeches-statements/munter-statement-fraud-detection-101122 (consultato 27 ottobre 2024).

Pavlidis G., 2023, "Can AI be Auditable?", arXiv. Risorsa web reperibile all'indirizzo: https://arxiv.org/pdf/2509.00575 (consultato 2026).

PCAOB, 2010, AS 2401 - Consideration of Fraud in a Financial Statement Audit, Public Company Accounting Oversight Board.

PCAOB, 2024, Technology Innovation Alliance Working Group - Future State Deliverable. Risorsa web reperibile all'indirizzo: https://pcaobus.org (consultato marzo 2026).

Perols J., 2011, "Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms", Auditing: A Journal of Practice & Theory, Vol. 30, n. 2, pp. 19-50.

Peta M., 2021, La responsabilità del Revisore alle frodi nella revisione di bilancio. Risorsa web reperibile all'indirizzo: https://www.fiscoetasse.com/approfondimenti/14314-la-responsabilita-del-revisore-alle-frodi-nella-revisione-di-bilancio.html (consultato 15 marzo 2025).

Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act), Gazzetta Ufficiale dell'Unione Europea, 12 luglio 2024.

Ribeiro M.T., Singh S., Guestrin C., 2016, "Why Should I Trust You?: Explaining the Predictions of Any Classifier", Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD 2016), pp. 1135-1144.

Roffia P., Poffo M., 2025, "Revisiting the Fraud Triangle in Corporate Frauds: Towards a Polygon of Elements", Journal of Risk and Financial Management, Vol. 18, 156.

Romeo G., Conti D., 2026, "Exploring Automation Bias in Human-AI Collaboration: A Review and Implications for Explainable AI", AI & Society, pp. 259-278.

Ruankaew T., 2016, "Beyond the fraud diamond", International Journal of Business Management and Economic Research, Vol. 7, n. 1, pp. 474-476.

Seethamraju R., Hecimovic A., 2023, "Adoption of Artificial Intelligence in Auditing", Australian Accounting Review, Vol. 33, n. 2, pp. 130-145. https://doi.org/10.1111/auar.12388

Soneji P.T., 2022, "The fraud theories: Triangle, diamond, pentagon", International Journal of Accounting, Auditing and Performance Evaluation, Vol. 18, n. 1, pp. 49-60.

Sundarasen S., Kamaludin K., Nakiran D., 2026, "From Adoption to Audit Quality: Mapping the Intellectual Structure of Artificial Intelligence-Enabled Auditing", Journal of Risk and Financial Management, Vol. 19, n. 3, 209.

Tahiri H., 2025, "Artificial Intelligence in Accounting and Auditing: Automation Bias, Internal Control Redesign, and EU AI Act Compliance", Journal of Risk and Financial Management.

Thomson Reuters Institute, 2026, The AI evolution changing the audit profession. Risorsa web reperibile all'indirizzo: https://tax.thomsonreuters.com/blog/the-ai-evolution-changing-the-audit-profession/ (consultato aprile 2026).

Thomson Reuters Institute, 2026, Audit challenges and changes in 2026. Risorsa web reperibile all'indirizzo: https://tax.thomsonreuters.com/blog/challenges-and-changes-within-the-audit-industry/ (consultato aprile 2026).

Thomson Reuters Institute, 2026, The state of AI in audit in 2026. Risorsa web reperibile all'indirizzo: https://tax.thomsonreuters.com/blog/state-of-ai-in-audit/ (consultato aprile 2026).

Tragouda V., Doumpos M., Zopounidis C., 2024, "Identification of fraudulent financial statements through a multi-label classification approach", Intelligent Systems in Accounting, Finance and Management.

Tümmler M., Quick R., 2026, "How to detect fraud in an audit: a systematic review of experimental literature", Management Review Quarterly, Vol. 76, pp. 287-332. https://doi.org/10.1007/s11301-024-00480-7

Vasarhelyi M.A., Halper F.B., 1991, "The continuous audit of online systems", Auditing: A Journal of Practice & Theory, Vol. 10, n. 1, pp. 110-125.

Veno J., 2024, "Preventing and Detecting Occupational Fraud", Galasso Learning Solutions. Risorsa web reperibile all'indirizzo: https://www.njcpa.org/article/2024/09/20/preventing-and-detecting-occupational-fraud (consultato 5 marzo 2026).

Vitali S., Giuliani M., 2024, "Man & Machine: Artificial Intelligence's Role in Shaping Auditor's Professional Scepticism", Journal of Modern Accounting and Auditing, Vol. 20, n. 4, pp. 171-181.

Vousinas G.L., 2019, "Advancing theory of fraud: the S.C.E.S. Fraud Hexagon model", Journal of Financial Crime, Vol. 26, n. 1, pp. 372-403.

Wolfe D.T., Hermanson D.R., 2004, "The fraud diamond: Considering the four elements of fraud", The CPA Journal, Vol. 74, n. 12, pp. 38-42.

Ringraziamenti

Il completamento di questo percorso segna il traguardo di un cammino intenso e impegnativo, risultato di un percorso di crescita personale reso possibile, e soprattutto migliore, grazie al sostegno di molte persone.

Ringrazio in primo luogo la mia relatrice, la Professoressa Paola Ramassa, che con la sua costante disponibilità e i suoi consigli mi ha permesso di portare a termine questa tesi.

Ringrazio immensamente la mia famiglia che ha sempre creduto in me sostenendomi in ogni momento. In particolare, a Mamma e Papà che mi hanno permesso di fare tutto questo e mi hanno sempre insegnato tutto rendendomi quello che sono, spero siate sempre fieri di me, e a mia sorella che in qualche modo spero di poterle essere da esempio. Un ringraziamento particolare ai nonni che in ogni momento sono sempre presenti e pronti a darmi consigli essenziali. Questo risultato va sicuramente anche ai nonni che non sono più qui, con la speranza di renderli sempre fieri di me.

Ringrazio Alessia, la mia fidanzata, con cui ho condiviso tutto questo percorso, colei che non si sa come è riuscita a sopportarmi, con cui sono felice di aver vissuto tutto questo, con cui ho condiviso molto e con cui spero di condividere ancora molto altro.

Un ringraziamento speciale va poi a tutti coloro che, in un modo o nell'altro, questi anni sono stati con me. Grazie a Dadu che ogni giorno, da quando siamo nati, è pronto ad ascoltare ogni mia lamentela, a tutti i miei compagni di università con cui ho condiviso un fantastico percorso giorno dopo giorno pronti a sostenerci e senza i quali sarebbe stato tutto molto più difficile e meno divertente, a Chisto che è sempre pronto nel caso ce ne fosse bisogno con i suoi consigli filosofici che non finiscono mai, a Faso, Edo, Fede, Nicolas e Mark sempre pronti a farmi innervosire con la loro disorganizzazione ma comunque sempre presenti, a tutti quelli che sono nel mio gruppo di amici sin da quando eravamo ragazzini e che so che nel momento del bisogno potrò sempre andare da Sacco e trovarli lì pronti ad accogliermi. Un grazie va anche ai colleghi incontrati durante l'esperienza di stage che mi hanno accolto e fatto crescere nel mondo del lavoro.

Davvero grazie a tutti coloro che in questi anni sono stati presenti, ma soprattutto il ringraziamento più importante lo devo dedicare a me stesso sempre determinato e costante nel raggiungere gli obiettivi prefissati nonostante i sacrifici necessari.