PROFESSIONISTI

AI e responsabilità del professionista: i nuovi confini del rischio

di **Mauro Festa**

1. **La trasformazione in atto: dall'innovazione all'esposizione al rischio**

Per decenni i professionisti, avvocati, commercialisti, ingegneri, consulenti, hanno esercitato la propria attività con **strumenti prevalentemente analogici**, controllando in modo diretto ogni passaggio del proprio lavoro. **L'avvento dell'intelligenza artificiale**, specie nella forma generativa e predittiva, **ha cambiato radicalmente lo scenario.**

Oggi gli studi professionali utilizzano piattaforme di **analisi documentale automatizzata**, software di contabilità intelligente, sistemi di redazione contrattuale basati su AI, strumenti di diagnosi forense e consulenza predittiva. Il salto di produttività è enorme, ma altrettanto lo **è l'esposizione al rischio.**

2. **Il quadro regolatorio europeo**

La risposta dell'ordinamento europeo è arrivata con **l'AI Act (Regolamento (UE) 2024/1689),** entrato in vigore nell'agosto 2024, che introduce un modello di regolazione **fondato sul rischio** ("risk-based approach").

Non tutte le applicazioni di AI sono uguali: il Legislatore distingue fra rischio inaccettabile (vietato), alto, limitato e minimo. Ogni livello comporta diversi obblighi per chi sviluppa, fornisce o utilizza sistemi di intelligenza artificiale.

Per i professionisti, la parte più rilevante riguarda i sistemi ad alto rischio e rischio limitato, quali:

- **strumenti di scoring** per l'accesso al credito o all'assistenza legale;
- sistemi di **valutazione fiscale o previsionale**;
- algoritmi che automatizzano parte **dell'attività consulenziale o decisionale**.

In questi casi il professionista non può più considerarsi un semplice "utente finale": egli diventa parte integrante della **catena di responsabilità.**

Deve quindi garantire: **tracciabilità delle decisioni**, controllo umano ("human oversight"), conoscenza dei limiti del sistema, e soprattutto trasparenza verso il cliente.

3. **L'Italia e la Legge n. 132/2025**

Con la Legge n. 132/2025, l'Italia ha introdotto la **prima Legge nazionale in materia di intelligenza artificiale**, in coordinamento con l'AI Act europeo.

Si tratta di una Legge delega che affida al Governo il compito di definire decreti attuativi su: vigilanza, sanzioni, reati connessi all'uso illecito dell'AI, certificazioni e audit.

AgID (Agenzia per l'Italia digitale) e ACN (Agenzia per la cybersicurezza nazionale), sono individuate dall'**art. 20** quali autorità nazionale per l'intelligenza artificiale.

Per il mondo delle professioni, il segnale è duplice: da un lato, **stimolare l'adozione dell'AI** come leva di competitività; dall'altro, imporre un **regime di responsabilità consapevole**, fondato su regole etiche e tecniche.

Si segnala, tra l'altro, che questa Legge segna un passaggio storico: l'Italia diventa, fra gli Stati UE, il primo paese ad adottare un quadro normativo nazionale specifico sull'AI.

4. **Responsabilità e AI: verso un nuovo paradigma giuridico**

L'uso professionale dell'AI pone un problema essenziale: il **controllo effettivo sul risultato**.

Se un algoritmo redige un parere sbagliato, una valutazione di rischio finanziario distorta o una simulazione contabile errata, la **responsabilità può derivare da:**

- **negligenza** nell'affidarsi a strumenti non verificati o non adeguati allo scopo;
- **mancata vigilanza sul funzionamento** e sull'output del sistema;
- **violazione degli obblighi deontologici** di diligenza e competenza tecnica.

In base al diritto civile (**artt. 1176** e **1218, c.c.**), il professionista risponde per **colpa lieve o grave** a seconda della natura dell'incarico. L'introduzione di strumenti di AI **non attenua tale responsabilità**: anzi, ne amplia la portata, poiché introduce nuovi obblighi di controllo, documentazione e trasparenza.

Si segnala, a tal proposito, una recentissima vicenda che ha coinvolto una **nota società di consulenza**, in particolare la sua sede australiana.

L'azienda ha accettato di rimborsare parzialmente il compenso ricevuto per un rapporto commissionato dal Governo australiano, dopo aver ammesso che **alcune sezioni del documento erano state redatte con l'aiuto dell'intelligenza artificiale**. Il Dipartimento

dell'Occupazione e delle Relazioni sul Lavoro aveva incaricato la società, nel dicembre scorso, di condurre una revisione indipendente dal valore di circa 400.000 dollari australiani.

Il rapporto era stato pubblicato nei mesi successivi, ma alla fine di agosto il quotidiano Australian Financial Review aveva portato alla luce numerosi errori, tra cui **citazioni e riferimenti accademici inventati**. In seguito alle verifiche, la società aveva ammesso di aver utilizzato una **catena di strumenti basati sul modello linguistico generativo** Azure OpenAI GPT-4o.

Una nuova edizione, corretta, del rapporto è stata dunque diffusa sul sito ufficiale del dipartimento. La società ha dichiarato di aver rivisto i riferimenti, le citazioni e il riepilogo legale, precisando, tuttavia, che **le conclusioni e le raccomandazioni principali non sono cambiate.**

L'episodio alimenta ulteriori dubbi sull'impiego dell'intelligenza artificiale, evidenziando il **rischio di errori, distorsioni o "allucinazioni"** nei documenti ufficiali. Mentre le grandi società di revisione e consulenza continuano a investire in sistemi di automazione avanzata, le autorità contabili, come quella del Regno Unito, sottolineano che i **controlli di qualità restano ancora inadeguati**.

Questo caso rappresenta un monito importante sull'uso dell'intelligenza artificiale in **ambiti professionali delicati**. L'automazione può offrire efficienza e rapidità, ma l'assenza di un controllo umano rigoroso può generare **errori gravi e compromettere la credibilità** di istituzioni e aziende. La supervisione umana, dunque, rimane essenziale: solo un equilibrio tra tecnologia e responsabilità può garantire che **l'IA sia uno strumento di progresso**, e non una fonte di rischi o disinformazione.

5. **Implicazioni pratiche per i professionisti**

a) Governance e due diligence sugli strumenti di AI

È suggeribile che ogni professionista che utilizza un software o una piattaforma AI svolga una **due diligence tecnica e legale**: verificare il **fornitore, le licenze, i dataset**, i limiti di utilizzo, e soprattutto se il sistema rientra nelle categorie di rischio dell'AI Act.

In pratica, serve una "*checklist*" di *compliance*:

- **l'IA è trasparente e documentata**?
- **sono previsti *log* e *audit trail*** (ovvero, un registro cronologico e dettagliato che documenta tutte le attività e gli eventi significativi all'interno di un sistema informatico o di un processo aziendale, specificando chi ha eseguito cosa, quando, e come, per garantire trasparenza, sicurezza, integrità dei dati e conformità normativa)

delle operazioni?
- **l'utente può correggere o bloccare *l'output*?**
- i **dati usati rispettano il GDPR?**

b) Contratti, pareri e documenti generati con AI

Sempre più professionisti impiegano strumenti generativi (ChatGPT, Copilot, Harvey AI, ecc.) per redigere documenti. Qui il rischio è duplice:

- **rischio di contenuto** (errori, bias, plagi, violazioni di copyright);
- **rischio informativo** (trasmissione di dati riservati a sistemi esterni).

Il professionista deve, quindi, esplicitare nei contratti con i clienti **l'uso di sistemi di intelligenza artificiale**, indicando limiti, grado di intervento umano e responsabilità residuale.

Ciò è stato, tra l'altro, **puntualizzato nel testo della Legge italiana sull'IA**, la quale all'**art. 13** prevede quanto segue:

«1. *L'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è finalizzato al solo esercizio delle attività strumentali e di supporto all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera.*

2. Per assicurare il rapporto fiduciario tra professionista e cliente, le informazioni relative ai sistemi di intelligenza artificiale utilizzati dal professionista sono comunicate al soggetto destinatario della prestazione intellettuale con linguaggio chiaro, semplice ed esaustivo.»

La trasparenza è un principio cardine non solo normativo, ma anche un dovere deontologico: il cliente ha diritto di sapere se un parere o una relazione è stata generata, in tutto o in parte, da un sistema automatizzato.

c) Audit, tracciabilità e formazione

Le strutture professionali dovranno dotarsi di **policy interne di gestione del rischio AI**, prevedendo audit periodici, registri delle applicazioni usate, protocolli di sicurezza informatica e percorsi di formazione obbligatoria.

L'AI act, all'art. 4, parla espressamente di "**AI literacy":** alfabetizzazione digitale e conoscenza dei rischi.

Non è più accettabile, giuridicamente e deontologicamente, **usare strumenti intelligenti "alla cieca**".

6. **Rischi penali e disciplinari: la nuova frontiera**

L'uso dell'IA può dar luogo anche a **responsabilità penali o disciplinari**.

Si pensi all'impiego di deepfake in **attività promozionali**, alla diffusione non autorizzata di dati sensibili, o all'uso di sistemi predittivi in **violazione della privacy.**

Le norme esistenti possono già applicarsi per analogia:

- **frode informatica** (**art. 640-*ter*, c.p.**),
- **trattamento illecito di dati** (**art. 167, Codice della privacy**),
- **responsabilità degli enti** *ex* D.Lgs. n. 231/2001, se l'uso dell'IA avviene in assenza di adeguati modelli di controllo.

Non solo, la Legge n. 134/2025 introduce, anche, **modifiche al Codice penale**, e in particolare:

1. aggravante comune (**art. 61, n. 11-*decies*, c.p.**): viene introdotta un'aggravante comune per chi **commette il fatto mediante l'impiego di sistemi di IA**, quando questi abbiano costituito un mezzo insidioso, ostacolato la pubblica o privata difesa, o aggravato le conseguenze del reato;
2. aggravante specifica (**art. 294, c.p.**): la pena è della reclusione da 2 a 6 anni se l'inganno è posto in essere mediante l'impiego di sistemi di intelligenza artificiale;
3. nuovo reato (**art. 612-*quater*, c.p.**): viene inserito il reato di illecita **diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale**, punendo chiunque cagioni un danno ingiusto a una persona diffondendo tali contenuti.

Per gli ordini professionali, il tema si sposta anche sul piano disciplinare: la **mancata vigilanza sull'uso dell'IA** o la presentazione al cliente di un **elaborato generato senza verifica** può integrare **violazione del dovere di competenza e diligenza.**

7. **L'equilibrio tra trasparenza e segretezza**

Un ulteriore punto di tensione è la contrapposizione tra **l'obbligo di trasparenza e il diritto alla segretezza** professionale.

Molti modelli di AI sono proprietari e **non consentono di accedere ai codici o ai dataset**, rendendo difficile garantire la piena auditabilità.

Per gli avvocati e i consulenti, che fondano il proprio lavoro sulla fiducia e sulla riservatezza, ciò implica la necessità di **scegliere piattaforme che garantiscano localizzazione dei dati**, clausole di non retention e opzioni di controllo interno.

Nel futuro, si prevede che le regole europee imporranno **forme di "*disclosure* controllata**": accesso agli algoritmi solo per autorità competenti o organismi di audit certificati, bilanciando tutela del **segreto industriale e diritto di difesa.**

8. **Diritto, etica e deontologia**

L'AI costringe i professionisti a un **salto di mentalità**. Non si tratta solo di aggiornare strumenti, ma di ridefinire il proprio ruolo: da **mero esecutore tecnico a garante di legalità** e responsabilità nell'uso dell'intelligenza artificiale.

Gli ordini professionali **dovranno aggiornare i propri codici deontologici**, introducendo principi di uso corretto e consapevole dell'AI, sul modello già adottato da alcune bar associations anglosassoni.

Le varie categorie professionali stanno procedendo in modo non coordinato. I **giornalisti hanno già aggiornato il loro codice deontologico a giugno 2025**, recependo il nuovo obbligo. Avvocati e notai sono al lavoro per modificare i rispettivi regolamenti, così da includere esplicitamente le **nuove disposizioni**. I commercialisti, il cui codice è stato rivisto nel 2024, considerano, invece, che le **regole già previste in tema di informazione al cliente e gestione degli incarichi siano sufficienti** a garantire un uso corretto dell'intelligenza artificiale. L'obbligo riguarda anche le **professioni non organizzate in ordini** (disciplinate dalla Legge n. 4/2013), per le quali il COLAP (Coordinamento delle libere associazioni professionali) sta elaborando specifiche linee guida.

Anche la **formazione continua dovrà comprendere moduli obbligatori su AI**, cybersecurity, data governance e rischi legali.

9. **Conclusione: verso una cultura della responsabilità aumentata**

L'AI apre orizzonti di efficienza, ma **anche di fragilità.**

Nel futuro prossimo, la **vera differenza tra un professionista e una macchina sarà la capacità di assumersi la responsabilità delle decisioni.**

Chi saprà integrare la tecnologia con etica, controllo e trasparenza potrà trarne vantaggio competitivo; chi la userà come scorciatoia rischia di smarrire la fiducia del mercato e del cliente.

L'intelligenza artificiale **non elimina il rischio professionale**: lo trasforma, spostandolo dal gesto umano all'algoritmo, ma senza attenuarne la portata.

Il diritto e i professionisti che lo incarnano dovranno imparare a **convivere con questo nuovo confine**. Un confine che segna non tanto il limite della responsabilità, quanto la soglia della consapevolezza.

Cinque raccomandazioni operative per i professionisti che usano l'AI:

1. Conoscere il sistema e il fornitore

Prima di utilizzare un software basato su intelligenza artificiale, **verifica sempre chi lo sviluppa,** dove risiedono i dati e quali garanzie di sicurezza e conformità offre, leggi attentamente i Terms&Conditions. Prediligi soluzioni certificate o con documentazione tecnica trasparente. La "fiducia cieca" nella tecnologia può tradursi in responsabilità diretta.

2. Mantenere il controllo umano ("*human-in-the-loop*")

L'AI può assistere, ma **non sostituire la decisione professionale**. Ogni risultato prodotto da un algoritmo, parere, simulazione, calcolo, valutazione, deve essere verificato e validato dal professionista. In caso di errore, sarà lui a rispondere, non il software.

3. Informare il cliente in modo chiaro e preventivo

Inserisci nei contratti o nei mandati professionali una **clausola di trasparenza sull'uso dell'AI**: specifica se e come viene impiegata, con quali limiti e quali cautele. Il cliente ha diritto di sapere se un documento o una consulenza è stata generata con il supporto di strumenti automatizzati.

4. Proteggere dati e segreti professionali

Non immettere mai nei sistemi di AI dati riservati, sensibili o coperti da segreto professionale, a meno che la piattaforma garantisca pieno controllo locale e non condivisione con terzi. L'uso disinvolto di chatbot pubblici o API esterne può comportare violazioni gravi di privacy e deontologia.

5. Creare una cultura interna di "AI compliance"

Ogni studio o società professionale dovrebbe **dotarsi di policy interne**, audit periodici, e percorsi di formazione continua sull'uso sicuro dell'intelligenza artificiale. La responsabilità oggi non è solo individuale, ma anche organizzativa: la prevenzione è la miglior difesa.