AI E DIGITALIZZAZIONE

L'intelligenza artificiale nello studio 4.0: come tutelare i dati e la privacy

di **Andrea Comencini**

L'uso dell'intelligenza artificiale (AI) si sta rapidamente diffondendo in tutti i settori e anche gli studi professionali, ormai, non ne possono più fare a meno. Siamo di fronte a un cambiamento epocale: l'AI ci aiuta nell'automazione delle registrazioni contabili, nella sincronizzazione degli archivi di studio con quelli dell'Agenzia delle Entrate, nella formulazione di testi, nel controllo delle fatture elettroniche e dei dichiarativi, nella ricerca normativa, solo per fare alcuni esempi.
L'adozione dell'AI offre sicuramente il vantaggio di consentire un efficientamento della gestione dei dati, ma occorre guardare al di là della semplice innovazione tecnologica. I dati che diamo "in pasto" a questi "robot" non sono nostri: sono dei nostri clienti, che ce li hanno affidati perché si fidano di noi. Lo studio professionale è obbligato a preservare l'integrità e la sicurezza di questi dati, di queste informazioni.
La riflessione che ogni professionista deve fare riguarda questioni che vanno oltre la semplice implementazione software: la tutela del dato, la governance operativa e la responsabilità deontologica. Nel presente contributo analizziamo questi 3 elementi fondamentali, anche grazie all'ausilio della "Guida operativa di intelligenza artificiale #3 – L'aiuto intelligente al Commercialista" pubblicata sul sito del CNDCEC il 24 ottobre 2025.

Bilanciare intelligenza artificiale e tutela della privacy

L'AI nasce, impara e si evolve solo se trova sempre nuove fonti di informazione e nuove banche dati da elaborare. L'addestramento e l'affinamento dei modelli AI per l'espletamento di compiti specialistici, come l'analisi di bilancio, la due diligence o l'analisi predittiva dei flussi di cassa, sono possibili solo grazie all'elaborazione e all'analisi di un'ingente quantità di informazioni.

Questa caratteristica, comune a tutti i servizi di AI, è in netta contrapposizione con il Regolamento Generale sulla Protezione dei Dati (GDPR), Regolamento UE 2016/679, che

impone severi limiti all'uso e alla conservazione dei dati personali e, ancor più, delle categorie particolari di dati. La recente approvazione della Legge n. 132/2025 in materia di intelligenza artificiale costituisce un ulteriore passo avanti verso un'adeguata regolamentazione dell'uso di tali tecnologie, anche nel campo delle professioni intellettuali.

La scelta di una piattaforma di intelligenza artificiale non deve essere effettuata solo alla luce della tecnologia offerta e delle prestazioni garantite; occorre analizzare bene come la stessa utilizza i dati e se lo fa in modo conforme e sicuro. Fondamentalmente i fornitori di servizi AI, che siano di ricerca, generativi o predittivi, offrono 2 categorie di profili: consumer e business/enterprise.

Il livello base, quello consumer, è utilizzabile a livello privato e, solitamente, non richiede alcun tipo di abbonamento. Ma sappiamo bene che dietro la gratuità si nasconde un prezzo occulto da pagare: non stiamo parlando di soldi ma di dati. Tutte le informazioni inserite (prompt, documenti, chat e quant'altro) sono utilizzate dai provider per l'addestramento e il miglioramento continuo dei loro sistemi di AI.

I dati immessi in rete escono, così, dal perimetro del nostro controllo, irrimediabilmente, rendendo sconsigliabile l'utilizzo di questa tipologia di servizi a livello professionale.

Negli studi professionali è, quindi, opportuno utilizzare i servizi offerti con abbonamenti business/enterprise, specificamente progettati per offrire prestazioni maggiori e, soprattutto, per garantire standard più elevati di sicurezza nella gestione dei dati. I fornitori di questi servizi offrono, infatti, la possibilità di opporsi all'utilizzo delle informazioni immesse in rete ai fini di addestramento e miglioramenti dei modelli AI. Un ulteriore passo in avanti in tema di sicurezza nella gestione dei dati è quella di adottare soluzioni integrate nel proprio gestionale che lavorino solo all'interno del proprio cloud, evitando di immettere dati nella rete aperta.

Anonimizzazione e pseudonimizzazione

I termini "pseudonimizzazione" e "anonimizzazione" sono profondamente diversi l'uno dall'altro e conoscere le differenze tra i 2 è determinante per riuscire a gestire correttamente i dati utilizzati per alimentare i servizi di AI. I 2 termini, inoltre, nel contesto del GDPR non sono sinonimi ma, al contrario, descrivono 2 processi giuridicamente e tecnicamente distinti, con conseguenze radicalmente diverse per gli obblighi di conformità di uno studio professionale:

– pseudonimizzazione: è la tecnica mediante la quale i dati personali vengono trattati in modo tale da non poter essere attribuiti a un interessato specifico senza l'uso di informazioni aggiuntive (ad esempio, una chiave di cifratura o una tabella di corrispondenza che collega lo pseudonimo all'identità reale). Tali informazioni aggiuntive sono conservate separatamente e protette da adeguate misure di sicurezza tecniche e organizzative. È bene ricordare che, ai sensi del GDPR, il dato pseudonimizzato resta comunque un dato personale poiché

l'identificazione, sebbene non diretta, è ancora possibile; il suo trattamento, quindi, è soggetto a tutti i vincoli normativi (art. 4, par. 1, n. 5, Regolamento UE 2016/679);

– anonimizzazione: consiste in un processo di trattamento dei dati personali che impedisce, in modo irreversibile, l'identificazione dell'interessato. La mancata possibilità di invertire il processo fa sì che il risultato non sia più considerato un "dato personale" e, di conseguenza, non è obbligatorio applicare il GDPR all'uso di tali informazioni.

Nel caso in cui lo studio professionale intenda utilizzare i servizi di AI, non solo per la ricerca normativa o per i classici compiti di segreteria, ma voglia impiegare i dati dei propri clienti, ad esempio, per effettuare analisi gestionali o per effettuare controlli sui modelli dichiarativi, è necessario minimizzare i rischi di perdita degli stessi e tutelare le informazioni dei clienti tramite l'adozione della tecnica di anonimizzazione. Tale processo deve essere robusto e tecnicamente irreversibile per garantirne la piena conformità al GDPR, motivo per cui è consigliabile appoggiarsi a fornitori specializzati. Il mercato offre un'ampia gamma di strumenti per l'anonimizzazione dei documenti, utilizzabili sia in cloud che tramite installazione su proprio hardware. La scelta della soluzione più adatta dipende dalle capacità tecniche interne dello studio, dal volume e dalla tipologia dei dati da trattare, dai requisiti di conformità specifici e, fattore non trascurabile, dal budget a disposizione.

Nel caso in cui il professionista decida di anonimizzare i dati con procedure "fai da te", come la rimozione manuale delle informazioni da un documento è opportuno che segua questi brevi consigli:

– metodi da evitare assolutamente: è un errore grave e comune pensare di poter anonimizzare un documento digitale semplicemente cambiando il colore del testo in bianco o coprendo il testo con una forma nera utilizzando gli strumenti di commento di un editor di testo o PDF. Questi metodi si limitano ad aggiungere un livello grafico sopra il testo originale, che rimane presente nel file e può essere facilmente recuperato con un semplice copia-incolla o selezionando l'area. Allo stesso modo, la semplice cancellazione del testo in programmi di videoscrittura come Word è insufficiente, poiché i metadati del file possono conservare una cronologia delle revisioni, rendendo potenzialmente recuperabili le informazioni eliminate;

– metodi efficaci: l'unico approccio manuale sicuro consiste nel creare una versione completamente nuova e "pulita" del documento, copiando e incollando selettivamente solo le informazioni non sensibili. In alternativa, si possono utilizzare le funzionalità di "Redazione" professionale presenti in software come Adobe Acrobat Pro. Questi strumenti non si limitano a coprire il testo, ma lo rimuovono permanentemente dal documento sottostante e offrono opzioni per eliminare i metadati nascosti, garantendo che l'informazione sia irrecuperabile[1].

Il principio dello zero data retention

Nella selezione dei fornitori e delle piattaforme di servizi AI è necessario comprendere bene come e per quanto tempo vengono utilizzati i dati che immettiamo in rete. Alcuni provider offrono una clausola di garanzia che assicura che i dati siano cancellati immediatamente dopo il loro utilizzo. In questo caso gli stessi non vengono conservati, nemmeno per un determinato periodo, ma sono mantenuti solo per il tempo strettamente necessario a raggiungere gli scopi per cui sono raccolti. Questo è il principio conosciuto come zero data retention e garantisce che i dati non vengano memorizzati e utilizzati per l'addestramento e il miglioramento dei modelli di AI. Purtroppo, spesso, tale clausola è nascosta nei meandri dei menù dei portali ed è consigliabile andarla a cercare e attivare prima di iniziare a utilizzare lo strumento scelto.

Governare l'AI nello studio professionale

L'integrazione dell'AI nello studio professionale non è un'iniziativa delegabile solo al reparto IT. Il professionista deve, infatti, garantire l'accuratezza della contabilità, dei calcoli fiscali, delle rispose ai quesiti, anche se generati automaticamente. Non sottovalutiamo poi la riservatezza dei dati, soprattutto di quelli sensibili, nel momento in cui sono processati da algoritmi esterni.

Per trasformare la sfida dell'AI in opportunità competitiva serve, prima di tutto, la "consapevolezza". Il professionista, e di conseguenza tutti gli operatori di studio, non possono essere solo dei semplici utilizzatori di queste nuove tecnologie, ma devono elevare le proprie competenze tecniche e la loro comprensione del ciclo di vita di ogni dato, con una più profonda conoscenza della normativa sulla privacy. Gli studi professionali devono sviluppare al loro interno, in maniera trasversale, le competenze di supervisione e controllo di questi nuovi strumenti AI, apportando tutti i cambiamenti organizzativi necessari, considerando che tra pochi anni gli operatori "contabili" scompariranno e si evolveranno necessariamente in controller.

Per gli studi di medie e piccole dimensioni l'approccio vincente non è lo sviluppo interno di soluzioni, che richiederebbe un'elevata preparazione tecnica e il sostenimento di costi elevati, ma l'adozione di soluzioni AI, integrate o meno nel proprio gestionale, e già disponibili sul mercato.

Il primo passo da compiere per governare l'uso dell'AI in studio e decidere qual è la soluzione più corretta da utilizzare consiste nel mappare e valutare, ai sensi del GDPR e dell'AI Act, tutti gli strumenti adottati considerando alcuni parametri:

– classificazione del rischio (AI Act);

– finalità/uso;

– base giuridica (GDPR);

– rischi;

– misure di mitigazione del rischio.

Le principali procedure di valutazione sono 2:

– DPIA (Data Protection Impact Assessment): valutazione prevista dal GDPR per stimare i rischi privacy, verificare la proporzionalità del trattamento dei dati e identificare le misure di mitigazione necessarie;

– FRIA (Fundamental Rights Impact Assessment): valutazione introdotta dall'AI Act per analizzare l'impatto sui diritti fondamentali, come non discriminazione, libertà di espressione, equo processo, accesso a un rimedio effettivo[2].

La sfida per lo studio professionale consiste nel riuscire a combinare gli adempimenti richiesti dall'AI Act (Regolamento Europeo sull'Intelligenza Artificiale 2024/1689) e dal GDPR con l'uso innovativo e sicuro di queste nuove tecnologie. Utilizzare i servizi di AI è, all'apparenza, abbastanza semplice da quando è stato reso possibile l'uso del linguaggio naturale per interagire con tali strumenti. Gli elementi di difficoltà consistono nel capire come riuscire a formulare correttamente i quesiti (obiettivo, contesto, tono, lunghezza della risposta, ecc.) e, caratteristica fondamentale nell'uso degli stessi per la nostra professione, nel riuscire a ottenere i risultati voluti senza intaccare la sicurezza e la privacy dei dati dei nostri clienti.

Occorre, poi, impostare una procedura di monitoraggio periodico degli strumenti e dei rischi connessi al loro utilizzo, avendo cura di ricordare che l'evoluzione tecnologica è arrivata, ormai, a livelli di velocità impensabili fino a poco tempo fa. Anche la formazione di tutti gli operatori di studio (partner, dipendenti, collaboratori) deve essere continua e soprattutto obbligatoria, così da assicurare consapevolezza sia delle potenzialità dell'AI sia dei suoi limiti e rischi.

Quanto visto precedentemente porta all'elaborazione di un documento di policy sull'intelligenza artificiale che definisce regole, responsabilità e procedure per l'adozione e l'utilizzo conforme degli strumenti AI nello studio professionale, diventandone una guida pratica e operativa.