RATIO QUOTIDIANO
Il commento e la critica delle più importanti notizie del momento

CONSULENZA AZIENDALE, COMMERCIALE E MARKETING

di ALESSANDRO MATTAVELLI

GPT e dati dei clienti: prima di incollare, anonimizza

Incollare un bilancio in ChatGPT sembra innocuo. Non lo è. I dati dei clienti restano nei server di terze parti ed espongono il professionista a violazioni del GDPR. Ecco cosa fare prima di usare qualsiasi AI esterna.

La scena è comune: si riceve un estratto conto, un bilancio, una dichiarazione e la prima cosa che viene in mente è incollarlo in ChatGPT per avere un'analisi rapida. Funziona. **Il problema è che insieme ai numeri si stanno trasferendo nome del cliente, codice fiscale, IBAN, dati patrimoniali,** tutto su server americani, fuori da qualsiasi accordo di trattamento dati firmato con il cliente.

I termini di servizio dei principali strumenti AI prevedono che i dati inviati possano essere usati per migliorare i modelli, salvo opzione *"non migliorare il modello"* non sempre attivato per default, ma anche quando non vengono usati per il training, restano registrati nei log del provider per un periodo variabile. Un dato che entra in un sistema esterno non è più sotto il controllo del professionista.
Sotto il GDPR il commercialista è titolare del trattamento dei dati dei propri clienti. Trasferire quei dati a un servizio AI esterno senza aver designato il provider come responsabile del trattamento con apposito DPA, Data Processing Agreement è una violazione. Non serve che accada qualcosa di grave: il trasferimento non autorizzato è già l'infrazione.
La posizione in tema di privacy è chiara: **gli strumenti AI rientrano nella catena del trattamento e devono essere governati come qualsiasi altro fornitore.** L'ingenuità tecnologica non è un'attenuante: la responsabilità rimane in capo al professionista che ha inviato i dati.

La soluzione non è smettere di usare l'AI. È anonimizzare prima di incollare. Significa sostituire il nome del cliente con 'Cliente A', il codice fiscale con *"CF_01",* l'IBAN con *"IBAN_01"* e qualsiasi dato identificativo con un segnaposto. I numeri economici ricavi, costi, margini possono restare: senza il soggetto a cui appartengono, non costituiscono dato personale.
Per velocizzare il processo si può costruire un *template* di anonimizzazione: un documento Word o un foglio Excel con le sostituzioni da fare prima di ogni incolla. Chi vuole automatizzare può usare uno script Python o una macro che cerca i pattern tipici (codici fiscali, IBAN, partite Iva) e li sostituisce con segnaposto prima che il testo arrivi all'AI. Si va quindi dalla mera sostituzione manuale (trova e sostituisci) alla creazione di workflow (flussi di lavoro) automatizzati anche con l'ausilio della stessa AI. Ciò che non deve mancare mai è la formazione agli utenti su cosa è privato e cosa è pubblico e sui metodi di mantenimento della privacy dei soggetti che ci hanno affidato i dati.
Esistono anche alternative strutturali. Le versioni *enterprise* di ChatGPT, Copilot for Microsoft 365 e Claude for Teams offrono contratti che escludono l'uso dei dati per il training e garantiscono isolamento dell'ambiente. Per i casi più sensibili si possono usare modelli in locale grazie ai quali i dati non escono mai dal computer dello studio.

Quando ho iniziato a lavorare nel mio primo studio professionale, molto prima dell'introduzione della L. 675/1996, mi è stato subito detto: *"Non si discute mai dei clienti fuori dallo studio! Al massimo, si utilizza uno pseudonimo".*
Fondamentalmente, **questa regola è rimasta invariata,** anche se oggi ci sono molte più occasioni di trovarsi fuori dall'ambiente lavorativo.

Riproduzione vietata - sabato 11 aprile 2026