Co.Ne.Pro
COMMERCIALISTI NETWORK PROFESSIONALE

IL FUTURO DELLA PROFESSIONE DI COMMERCIALISTA

L'INTELLIGENZA ARTIFICIALE A SERVIZIO DEL PROFESSIONISTA

EVOLUZIONE, SFIDE E NUOVE OPPORTUNITÀ
PER IL NETWORK PROFESSIONALE

IN COLLABORAZIONE CON
BANCA GENERALI PRIVATE

05 MAGGIO 2026
h. 15:00 – 19:00

LA LOCATION
Banca Generali Private
Via Bertoloni, 2 – Roma

DUE MODALITÀ DI PARTECIPAZIONE
In Presenza (posti limitati)
e In Streaming

NETWORKING
CONFRONTO
OPPORTUNITÀ

AI e LLM nello Studio Professionale

Guida pratica per commercialisti · 2025-2026 | CNDCEC Informativa 156/2025

Rag. Alessandro Scapuzzi ODCEC Livorno
https://www.scapuzzirusciano.it

Sommario

1

Cos'è un LLM e come funziona

LLM: Definizione e componenti principali

📖 LLM (Large Language Model)

Modello statistico addestrato su miliardi di testi per predire la parola successiva più probabile. Non 'capisce' davvero: calcola statistico.

🧠 Training (Apprendimento)

Fase in cui il modello legge enormi quantità di testo e aggiusta miliardi di parametri interni (pesi). Costa mesi e milioni di euro.

🔤 Tokenizzazione

Il testo viene spezzato in 'token' (parole o parti di parola). Il modello opera su sequenze di numeri, non lettere.

⚡ Inferenza (Utilizzo)

Quando noi scriviamo un prompt, il modello genera la risposta token per token, in tempo reale, basandosi sul contesto.

2

Come interagire con un LLM

Metodi di interazione e prompt engineering

- **Interfaccia web (Chat)**
  ChatGPT, Claude.ai, Le Chat… Si usa come una chat normale. Il più semplice per i neofiti.
- **Prompt: la chiave del risultato**
  Un prompt ben costruito = risposta utile. Specificare: ruolo, contesto, formato richiesto, vincoli.
- **Esempi pratici di prompt efficaci**
  ❌ 'Scrivimi una lettera' → ✅ 'Sei un commercialista italiano. Scrivi una lettera di risposta a un avviso bonario IRPEF per un cliente persona fisica. Tono formale, max 250 parole.'
- **API (accesso diretto)**
  Per sviluppatori: integrazione nei gestionali (es. MySolution, Zucchetti). Richiede competenze tecniche.
- **Plugin e strumenti integrati**
  Microsoft Copilot in Word/Excel, Google Gemini in Workspace: l'LLM entra direttamente nei programmi già in uso.

3

Rischi tecnici: allucinazioni e bias

Rischi tecnici nell'uso degli LLM

⚠️ Allucinazioni

- Il modello inventa fatti con sicurezza apparente
- Citazioni di norme inesistenti
- Calcoli errati presentati come certi
- Il testo è sempre grammaticalmente perfetto anche quando sbagliato
- Regola d'oro: verificare sempre le fonti primarie
- Mai copiare output fiscale/legale senza controllo del professionista
- Statistico ...quante fake-news esistono, anche create da AI

📊 Bias

- Il modello riflette i pregiudizi presenti nei dati di training (Groc-xAI = Musk)
- Bias geografico: prevalenza di testi anglosassoni → normativa italiana meno precisa
- Bias temporale: dati non aggiornati dopo la data di 'cutoff' addestramento
- Bias di conferma: tende ad assecondare l'utente
- La responsabilità finale rimane sempre del professionista
- Il CNDCEC: 'l'AI non sostituisce il giudizio esperto'

4

Privacy e GDPR: i rischi per lo studio

I 4 rischi privacy nell'uso degli LLM

- **1. Trattamento illecito di dati personali**
  Inserire nel prompt dati di clienti (nome, CF, redditi) = trattamento dati personali. Serve base giuridica (art. 6 GDPR). Il commercialista è titolare del trattamento.
- **2. Trasferimento extra-UE**
  ChatGPT (OpenAI = USA), Gemini (Google = USA). I dati potrebbero finire su server americani. Verificare sempre Data Processing Agreement e Standard Contractual Clauses.
- **3. Diffusione non autorizzata**
  I dati del prompt potrebbero essere usati per addestrare il modello (soprattutto nei piani free). Violazione dell'obbligo di riservatezza professionale.
- **4. Segreto professionale**
  Inserire dati di clienti in LLM consumer = potenziale violazione del segreto professionale ex art. 622 c.p. e del Codice Deontologico CNDCEC.

5

Piano gratuito vs. piano a pagamento

Free vs. Piano a pagamento: cosa cambia per la privacy

Aspetto	Piano FREE	Piano PRO / Business	Piano Enterprise/API
Uso dati per training	⚠️ Sì (di default)	❌ No (opt-out)	❌ No (contrattuale)
Data Processing Agreement	❌ Non disponibile	✅ Disponibile	✅ Incluso (DPA)
Conservazione dati	Lunga / indefinita	Limitata / configurabile	Configurabile / zero
Adeguato per dati clienti?	🚫 NO	⚠️ Solo con DPA firmato	✅ Sì, con precauzioni
Costo indicativo (mese)	Gratuito	€ 20-25/mese	Su preventivo

6

Uso senza governance e DPIA: i rischi legali

Uso non organizzato: cosa rischia lo studio

- **Assenza di policy interna sull'uso dell'AI**
  Senza regole scritte, ogni collaboratore può usare qualsiasi LLM con dati dei clienti. Il titolare dello studio risponde per violazioni GDPR (fino a €20M o 4% fatturato).
- **Nessuna DPIA (Data Protection Impact Assessment)**
  Il GDPR art. 35 richiede DPIA quando il trattamento è ad alto rischio. Usare un LLM con dati fiscali/contabili dei clienti rientra in questa categoria.
- **Mancanza di registro dei trattamenti aggiornato**
  L'uso dell'AI va inserito nel Registro dei trattamenti GDPR. Molti studi lo ignorano: è un illecito formale immediatamente sanzionabile.
- **Violazione della Legge 132/2025 (AI Act italiano)**
  Il professionista deve informare il cliente dell'uso dell'AI nel mandato professionale (clausola tipo CNDCEC). L'omissione è una violazione.
- **Responsabilità penale: segreto professionale**
  La divulgazione di dati riservati – anche involontaria tramite LLM – è reato. La 'buona fede' non vale! *semplifichiamo*

7

I principali LLM: confronto pratico

LLM generalisti a pagamento: quando usarli

ChatGPT (OpenAI)

Il più diffuso. Ottimo per testi, bozze, riassunti. GPT-4o ha capacità multimodali. Piano Team: no training sui dati. Sede: USA → serve DPA.
Meglio per: bozze lettere, FAQ clienti, analisi documenti.

Claude (Anthropic)

Eccellente per testi lunghi e ragionamento complesso. Molto preciso e 'cauto'. Piano Pro: no data retention. Sede: USA.
Meglio per: relazioni, pareri, contratti, documenti lunghi.

Gemini (Google)

Integrato in Google Workspace (Docs, Gmail, Drive). Ottimo se lo studio usa G-Suite. Sede: USA/UE.
Meglio per: chi usa già Google, sintesi di documenti Drive.

Le Chat (Mistral)

Modello europeo (Francia). Maggiore tutela GDPR rispetto ai competitor USA. Ottimo per testi in italiano e francese.
Meglio per: chi privilegia la compliance UE.

Copilot (Microsoft)

Integrato in Word, Excel, Outlook, Teams. Piano M365 Business: dati non usati per training. Molto pratico per chi usa già Office.
Meglio per: studi con licenza Microsoft 365.

DeepSeek (Cinese)

⚠️ SCONSIGLIATO? per dati professionali. Server in Cina, fuori da qualsiasi protezione GDPR/AI Act. Ottimi benchmark ma rischio privacy elevatissimo.

ma i pesi? sono Open-Source

Vibe Coding: quando l'AI scrive codice al posto tuo — i rischi per lo studio

🎵 Cos'è il Vibe Coding?

Termine coniato da Andrej Karpathy (co-fondatore OpenAI) nel febbraio 2025. Consiste nel descrivere in linguaggio naturale ciò che si vuole ottenere e lasciare che l'AI generi tutto il codice.

Non serve saper programmare: si accetta l'output, lo si esegue, si incolla l'errore all'AI e si ripete finché «sembra funzionare».

📊 I dati (Veracode GenAI Report 2025)

- 45% del codice AI-generated fallisce i test di sicurezza (OWASP Top 10)
- 62% presenta difetti architetturali non rilevati nei test funzionali
- 2,74× più vulnerabilità rispetto al codice scritto da sviluppatori senior
- 92% degli sviluppatori USA usa già AI tools ogni giorno (2025)

⚠️ I 4 rischi chiave per il commercialista

🔍 Debug impossibile senza competenze

Il commercialista non sa leggere il codice prodotto dall'AI. Se smette di funzionare o produce dati errati, non può individuare dove si trova il problema. Il debug diventa dipendenza cieca dall'AI stessa.

🔒 Vendor lock-in automatico

Il codice generato è spesso ottimizzato per una piattaforma specifica (es. Replit, Cursor). Spostarsi altrove è difficile o impossibile: si è prigionieri dello strumento scelto e delle sue vulnerabilità.

🦠 Rischio malware e backdoor

L'AI attinge a codice pubblico di bassa qualità e può inserire librerie con vulnerabilità note o token hard-coded. Caso reale: Moltbook violato in 48h dal lancio. Lo «slopsquatting» usa pacchetti con nomi simili a quelli

🏗️ Debito tecnico invisibile

Il codice «funziona» ma nessuno capisce come. In pochi mesi diventa una scatola nera ingestibile. Ogni modifica genera nuovi errori a cascata. L'AI stessa perde coerenza su progetti grandi (limite del context window).

Regola per lo studio: non usare il vibe coding per gestire dati dei clienti, elaborazioni fiscali o automatizzazioni aziendali. Senza sapere cosa fa il codice, non si può garantire né la correttezza né la sicurezza. NON SIAMO SOFTWARE HOUSE!

LLM Open Source: libertà e responsabilità

🔓 Modelli disponibili

- Llama (Meta) – il più usato, modelli da 8B a 405B
- Mistral / Mixtral – europeo, ottimo italiano
- Phi-3 (Microsoft) – piccolo ma preciso
- Gemma (Google) – leggero, per dispositivi locali
- Falcon – sviluppato negli Emirati, molto capace
- Qwen (Alibaba) – ottimo per testi asiatici

⚖️ Pro e Contro

- ✅ Dati rimangono in locale (massima privacy)
- ✅ Nessun costo per token / API
- ✅ Personalizzabile per il proprio settore (fine-tuning)
- ❌ Richiede hardware potente (GPU)
- ❌ Gestione tecnica a carico dello studio
- ❌ Qualità inferiore ai top model proprietari
- Quando usarli: studi con IT interno, elaborazione massiva dati riservati

📊 I pesi aperti (open weight)

Immagina di voler insegnare a qualcuno a riconoscere se una frase è formale o informale. All'inizio non sa nulla. Gli fai leggere milioni di esempi, e man mano che impara, si costruisce nella sua testa una rete di associazioni.

I pesi sono il risultato dell'addestramento. Se sono aperti sono "ispezionabili e auditabili", possono essere riprodotti in locale (CPU/GPU), e possono essere personalizzati (fine Tuning = studia di più; RAG (Retrieval-Augmented Generation, cerca in documenti esterni)

8

LLM generalisti vs. LLM verticali

Generalisti vs. Verticali: quando usare cosa

🌐 Generalisti

ChatGPT, Claude, Gemini, Le Chat, DeepSeek, Qwen..

- Addestrati su tutto (web, libri, codice…)
- Ottimi per scrittura, sintesi, brainstorming
- Non conoscono normativa italiana aggiornata
- Possono allucinare su circolari recenti
- Non integrati con i gestionali dello studio
- Utili per: lettere, FAQ, spiegazioni ai clienti, bozze

🎯 Verticali (dominio specifico)

- Commerciali da commercialisti o avvocati
- Addestrati su banche dati fiscali/legali italiane
- Aggiornati con circolari, risoluzioni, prassi
- Integrati nel gestionale: conoscono il cliente
- Rispondono con riferimenti normativi verificati
- Costo maggiore, ma più affidabili per consulenza
- Utili per: ricerca normativa, pareri fiscali, dichiarazioni

Business Intelligence vs. Large Language Model

	📊 Business Intelligence (BI)	🤖 LLM (AI Generativa)
Cosa fa	Analizza e visualizza dati strutturati	Genera testo, risponde a domande, ragiona
Input	Database, Excel, ERP, gestionali	Testo in linguaggio naturale (prompt)
Output	Dashboard, grafici, KPI, report	Testo, riassunti, codice, analisi qualitative
Affidabilità	Alta (dati certi se DB corretto)	Variabile (rischio allucinazioni)
Esempi	Power BI, Tableau, QlikSense	ChatGPT, Claude, Mia, Copilot
Uso in studio	Analisi finanziaria, trend cliente, budget	Bozze documenti, ricerca normativa, FAQ
Integrazione	Si integrano: BI legge i dati, LLM li racconta	

BI, ML, Deep Learning, LLM — Non è tutto AI

Distinguere gli strumenti è il primo passo per usarli correttamente

BI

Business Intelligence

Cosa fa: analizza I dati storici
Come: Query, report, dashboard

Es. PowerBI, Tableau, Excel, Metabase, apache sunset

✗ Non-AI

ML

Machine Learning

Cosa fa: apprende dai dati → predice
Come: tramite algoritmi statistici (regressione, alberi, SVM)

Es.filtri antispa,. scoring rate credito, frodi informatiche

✓ AI

DL

Deep Learning

Cosa fa: Reti neurali profonde → pattern complessi
Come: Layer di neuroni artificiali, GPU massiva

Es. Riconoscimento immagini, voce, testo

✓ AI

LLM

Large Language Model

Cosa fa: Genera testo (e codice, ragionamento…)
Come: Transformer + miliardi di parametri + RLHF

Es.: ChatGPT, Claude, Gemini, LLaMA

? Dipende

💡 *Gli LLM sono sofisticati sistemi di predizione statistica del testo — non 'pensano', non 'capiscono', non 'sanno'. Stallman aveva ragione.*

10

Decalogo: le 10 regole per usare l'AI in studio

Le 10 regole d'oro per il commercialista che usa l'AI

1. Mai inserire dati personali di clienti in LLM consumer free
2. Usa solo LLM con DPA firmato (piano Business/Enterprise)
3. Verifica sempre l'output: l'AI può inventare norme
4. Aggiorna il Registro dei Trattamenti includendo l'uso dell'AI
5. Fai la DPIA se usi LLM con dati fiscali/patrimoniali dei clienti
6. Inserisci la clausola AI nel mandato professionale
7. Preferisci LLM europei (Mistral) o soluzioni verticali italiane
8. Forma i collaboratori: stabilisci una policy interna scritta
9. Per ricerca normativa: usa LLM verticali verificati, non ChatGPT
10. Rimani il professionista: l'AI è un assistente, tu sei il responsabile

11

Uso sicuro dell'AI con accesso al computer

Cowork: quando l'AI opera sul tuo computer

- **Cos'è Cowork (Anthropic)**
  Funzione di Claude Desktop che permette all'AI di agire sul tuo computer: leggere file, aprire app, navigare il web, eseguire operazioni automatiche. Disponibile solo per piani a pagamento

- **Rischio 1 – Accesso ai file locali**
  Claude può leggere, modificare ed eliminare file. Non concedere mai accesso a cartelle con documenti fiscali, credenziali o dati dei clienti. Usa una cartella dedicata e tieni backup.
- **Rischio 2 – Prompt injection via web**
  Contenuti malevoli nascosti in siti web o email possono 'istruire' Claude a compiere azioni non volute. Limita l'accesso solo a siti fidati. Il web è il principale vettore di attacco.
- **Rischio 3 – Attività pianificate non presidiate**
  Le task schedulate girano in autonomia. Evita di automatizzare operazioni su dati sensibili, invii di messaggi o acquisti. Controlla sempre i risultati dopo ogni esecuzione.
- **Rischio 4 – Condivisione dati tra app**
  Con i plugin (Excel, PowerPoint), Claude può spostare dati tra applicazioni senza istruzione esplicita. Evita di avere dati riservati aperti mentre Cowork è attivo.

Cowork: le 6 regole di sicurezza operative

A

Inizia con attività a basso rischio

Comincia con task semplici (riassunti, compilazione info) prima di automatizzare operazioni complesse. Costruisci fiducia gradualmente.

B

Blocca le app sensibili

Impedisci a Claude di accedere a home banking, portali sanitari, app personali. Ogni app deve essere esplicitamente autorizzata.

C

Monitora le azioni, non solo i comandi

Osserva se Claude accede a file o siti che non hai menzionato. Se qualcosa non torna, interrompi subito il task.

D

Attenzione al controllo da mobile

Se usi Claude da smartphone, il telefono diventa un 'telecomando' del tuo desktop. Valuta se il livello di accesso concesso è appropriato.

E

Usa solo plugin verificati

Installa solo estensioni dal catalogo ufficiale Claude Desktop. Ogni plugin amplia le capacita' di azione di Claude: valuta con attenzione le autorizzazioni.

F

Segnala comportamenti anomali

Se Claude inizia a discutere argomenti non richiesti, tenta di accedere a risorse non menzionate o chiede info sensibili: ferma il task e segnala ad Anthropic.

Chi e' responsabile quando Claude agisce in autonomia?

Principio (Anthropic / Legge 132/2025 / GDPR): rimani responsabile di tutte le azioni compiute da Claude per tuo conto, anche se automatizzate.

- Contenuti pubblicati o messaggi inviati da Claude
- Acquisti o transazioni finanziarie eseguiti da Claude
- Dati acceduti, modificati o cancellati da Claude
- Azioni delle task schedulate in esecuzione automatica
- Operazioni tramite computer use su desktop e app
- Rispetto dei termini di servizio dei siti web visitati

12

Le raccomandazioni

Non ho niente da nascondere, la privacy non mi interessa
Ho sempre fatto così
Fanno tutti così
Mi torna meglio in quest’altro modo
Non funziona

Errori e raccomandazioni

All’epoca era il fax, poi la mail; le collane editoriali poi le banche dati; le telefonate poi il VOIP
ma da allora ci siamo mai evoluti?
Excel e Whatsapp …. ed infine abbiamo iniziato ad usare impropriamente gli strumenti che conosceva invece di sostituirli con quelli nuovi ed idonei.

Parliamo di AI, ma nella maggioranza dei casi non conosciamo I CRM, I DMS, il mailing ma nemmeno come funziona Internet o la posta elettronica.

Il problema non è tecnologico. È culturale, commerciale e strutturale: ecosistema chiuso ed I nostri consulenti sono in realtà I venditori delle software house

I dati sono il motore del futuro: se ce ne riappropriamo potremo esser parte attiva anche nell’AI altrimetni saremo solo una interfaccia tra altri soggetti, finchè serviremo! Un ecosistema aperto e open source ne favorisce la circolazione e ci permette di fare finetuning e di creare RAG.

Rag. Alessandro Scapuzzi ODCEC Livorno
https://www.scapuzzi.it
[mob] 393 401 3332

Grazie per l'attenzione

Riferimenti normativi e di categoria

- CNDCEC – Guida operativa AI #3 'L'aiuto intelligente al Commercialista' (Informativa 156/2025, ottobre 2025)
- CNDCEC – Linee guida vigilanza Collegio Sindacale sull'AI (Informativa 179/2025, dicembre 2025)
- Legge 132 del 23 settembre 2025 – Disposizioni in materia di intelligenza artificiale
- Regolamento UE 2024/1689 – AI Act europeo
- Regolamento UE 2016/679 – GDPR
- Anthropic – 'Use Cowork safely' (support.claude.com, 2025)