



**I QUADERNI
DEL CONSUMATORE**

AI AGENTICA:

la tecnologia è al servizio del consumatore?



PREMESSA

Siamo abituati a usare l'intelligenza artificiale soprattutto per ottenere risposte o creare contenuti. Con gli agenti AI questo rapporto cambia, perché il sistema può passare dal consigliare all'agire e svolgere alcune operazioni per conto dell'utente.

Questa possibilità può semplificare molte attività quotidiane, ma introduce una forma di delega più delicata. Quando una tecnologia interagisce con servizi esterni e prepara un'operazione sulla base delle indicazioni ricevute, il consumatore deve sapere fin dove può spingersi e in quale momento è richiesta la sua autorizzazione.

La comodità non può tradursi in una perdita di controllo. Ogni passaggio deve essere comprensibile e verificabile, lasciando all'utente la possibilità di correggere una scelta o interrompere il processo prima che produca effetti concreti.

L'autonomia degli agenti AI apre anche problemi nuovi sul piano della sicurezza. Un sistema incaricato di agire per nostro conto può essere manipolato oppure impiegato per rendere più rapide e credibili le frodi. Diventa quindi necessario proteggere l'identità dell'utente e rendere chiare le autorizzazioni concesse.

Per Adiconsum, questa nuova forma di delega richiede regole comprensibili e strumenti di tutela adeguati, perché la tecnologia può semplificare un'operazione senza rendere meno chiaro chi decide e chi ne risponde.

Buona lettura.



Che cos'è l'AI agentic?

L'AI agentic è una particolare applicazione dell'intelligenza artificiale, basata sui modelli linguistici di grandi dimensioni, o LLM, ma diversa dagli assistenti AI che siamo abituati a utilizzare. Con questa espressione si indica un sistema capace di raggiungere un obiettivo specifico senza una supervisione umana continua.

“Gli agenti AI sono sistemi software che sfruttano l'AI per perseguire obiettivi e completare attività per conto degli utenti. Mostrano capacità di ragionamento, pianificazione e memoria e hanno un livello di autonomia tale da essere in grado di prendere decisioni, apprendere e adattarsi.”¹

ChatGPT produce testi, codice, immagini o video in risposta alle nostre richieste, secondo un'interazione reattiva. L'AI agentic, invece, può compiere azioni autonome per raggiungere l'obiettivo assegnato, secondo un'interazione proattiva.



Organizzare un viaggio con l'intelligenza artificiale

Per capire meglio la differenza tra un chatbot e un agente AI, prendiamo come esempio l'organizzazione di un viaggio di tre giorni a Milano.

Utilizzando un chatbot AI:

Prompt: organizza un viaggio di 3 giorni a Milano con partenza la mattina del 9 luglio e un budget di 500 euro.

Riceviamo un **itinerario di tre giorni**, che può includere gli eventi previsti durante il soggiorno e indicazioni su dove mangiare o dormire. Possiamo personalizzarlo fornendo maggiori dettagli sui nostri gusti, ma **il lavoro del chatbot si ferma alla preparazione dell'itinerario**.

Utilizzando un agente AI:

Prompt: organizza un viaggio di 3 giorni a Milano con partenza la mattina del 9 luglio e un budget di 500 euro

Anche l'agente prepara un itinerario personalizzato, ma **può collegarsi a servizi esterni**, come Trenitalia o Booking, per verificare in tempo reale alberghi, treni, voli e attrazioni compatibili con il budget. Prima di effettuare le prenotazioni, chiede l'**approvazione dell'utente**, in modo simile a un **tour operator**.



Una risposta dell'agente potrebbe essere questa:

*"Ecco l'itinerario per Milano. Ho già controllato la disponibilità per l'Ultima Cena di Leonardo ed è quasi tutto esaurito, ma c'è un posto libero il 10 luglio alle 14:30. Ho anche selezionato tre hotel a Brera² in linea con il tuo budget e ho visto che il treno delle 8:00 costa meno di quello delle 9:00. **Procedo a bloccare i biglietti del museo e a prenotare la stanza d'hotel più conveniente?** Se mi dai l'ok, ti mando il link per il pagamento sicuro."*



Quanto può agire autonomamente un agente AI?

Questo passaggio, che richiede **l'approvazione esplicita** dell'utente-consumatore, viene definito **Human in the loop**³.

Altri tipi di agenti AI possono essere creati per agire più liberamente:

Human on the loop: L'agente agisce in autonomia, per esempio ottimizzando continuamente i prezzi su un sito di e-commerce, ma l'utente può monitorarlo e intervenire per bloccarlo se nota anomalie.

Human out of the loop: L'agente agisce in completa autonomia, per esempio nel trading algoritmico ad alta frequenza⁴, e l'utente vede soltanto il risultato finale.

Per i servizi rivolti ai consumatori, il modello più prudente è il primo, che richiede la conferma dell'utente prima di procedere.

³ Questo termine nasce per indicare l'attività di validazione umana da parte degli ingegneri del software all'interno del processo di addestramento delle intelligenze artificiali. Attualmente, nell'ambito dell'AI generica il significato è stato esteso, includendo l'utente nel processo di validazione del dato, cosa estremamente necessaria considerando che l'agente agisce per nostro conto.

⁴ Il trading algoritmico ad alta frequenza è una tecnica di negoziazione in cui potenti computer eseguono un numero enorme di ordini di borsa in frazioni di secondo, sfruttando algoritmi complessi e infrastrutture ultra-veloci per trarre profitto da minime variazioni di prezzo.

Gli agenti AI negli acquisti online

Un altro esempio di agente rivolto ai consumatori è quello proposto da Amazon:

Amazon Buy for Me⁵ è una funzionalità (attualmente attiva solo negli Stati Uniti) integrata nell'app Amazon Shopping che permette di cercare e acquistare prodotti **direttamente dai siti di altri brand**, qualora l'articolo non sia venduto direttamente su Amazon.

L'utente resta nell'app **Amazon**, mentre il sistema completa il checkout sul sito esterno e trasmette in forma crittografata i dati necessari all'ordine. La consegna, l'assistenza e gli eventuali resi **restano a carico del venditore**, mentre lo stato dell'ordine può essere seguito dall'app Amazon.

I rischi per il consumatore

L'introduzione degli **agenti AI** cambia il modo in cui svolgiamo alcune attività e **può farci risparmiare tempo**. Questo non permette di ignorare i rischi. Con la diffusione di questi strumenti sono emerse **truffe** che cercano di manipolare gli agenti, insieme a **frodi** realizzate attraverso il loro utilizzo.

La motivazione è piuttosto chiara. Alcune **società di consulenza** come **Edgar, Dunn & Company** hanno previsto che **nei prossimi anni il valore dell'e-commerce generato dall'intelligenza artificiale passerà da 136 miliardi di dollari di oggi a 1.7 trilioni di dollari entro il 2030**.

5 <https://www.aboutamazon.com/news/retail/amazon-shopping-app-buy-for-me-brands>

Una delle sfide principali è verificare che l'agente sia stato davvero autorizzato dall'utente e che non stia operando attraverso un'identità sottratta.

I siti fraudolenti potrebbero essere progettati per ingannare direttamente gli agenti incaricati di cercare prodotti o servizi, senza rivolgersi prima alla persona.

Agenti AI e frodi automatizzate

Visa PERC ha rilevato un **aumento superiore al 450%** delle menzioni degli agenti AI nei canali underground del dark web rispetto al semestre precedente. Secondo l'analisi, questi strumenti possono automatizzare attività che prima richiedevano il **lavoro coordinato di più truffatori**, rendendo le frodi più rapide, credibili e difficili da individuare.⁶

Rispetto ai bot tradizionali, gli agenti AI possono adattare il proprio comportamento mentre cercano di raggiungere l'obiettivo assegnato. Nel 2025 Anthropic ha segnalato una **campagna di cyberspionaggio** che ha tentato di colpire circa trenta organizzazioni, con un intervento umano limitato ad alcuni passaggi decisionali.⁷

Gli agenti attivi senza interruzioni possono quindi aumentare la velocità e la portata delle frodi. La stessa intelligenza artificiale può però diventare **uno strumento prezioso per riconoscere e contrastare queste minacce**.

6 Fonte: Sito Corporate VISA <https://corporate.visa.com/en/sites/visa-perspectives/security-trust/the-threats-landscape-of-agentic-commerce.html>

7 Fonte: <https://www.anthropic.com/news/disrupting-AI-espionage>

IL PROGETTO

Il progetto **“DICO Sì. Diritti, Consapevolezza, Opportunità, Strumenti, Inclusione (III edizione)”**, promosso da Adiconsum e finanziato dal **Ministero delle Imprese e del Made in Italy** nell’ambito delle **Iniziative a vantaggio dei consumatori**, ai sensi dell’articolo 148, comma 1, della legge 23 dicembre 2000, n. 388 e del Decreto direttoriale 12 maggio 2025, nasce per aiutare i cittadini-consumatori a orientarsi nei cambiamenti prodotti dalla digitalizzazione e dall’intelligenza artificiale, che incidono ormai sulle scelte di acquisto e sull’accesso ai servizi.

La terza edizione dedica particolare attenzione al divario digitale legato all’età e al genere, con attività rivolte soprattutto alle persone over 60 e alle donne. Il progetto intende:

- rendere più comprensibili le nuove tecnologie e il modo in cui influenzano la vita quotidiana;
- accompagnare i consumatori verso un uso del digitale più consapevole, prestando attenzione alla sicurezza e alla tutela dei propri diritti;
- diffondere una cultura della sostenibilità digitale, attenta agli effetti dell’innovazione sulle persone e sull’ambiente;
- favorire il confronto tra cittadini, esperti, istituzioni, imprese e mondo della ricerca.

Il progetto prevede un’indagine nazionale sull’impatto dell’intelligenza artificiale sui consumi, cinque incontri formativi online e materiali pratici dedicati all’uso sicuro delle tecnologie. È previsto anche un gioco interattivo per conoscere il funzionamento degli algoritmi, mentre due forum e una rete di sportelli territoriali offrono occasioni di confronto e assistenza diretta.

Per maggiori informazioni visita il sito www.adiconsum.it



III EDIZIONE

Finanziato dal MIMIT - D.D. 12 maggio 2025

Facciamo
crescere
le tue tutele
di consumatore!

Firma il tuo **5xmille** ad Adiconsum
C.F. 96107650580

seguici su



www.adiconsum.it



ADICONSUM

Associazione Difesa Consumatori APS

dal 1987