INSURANCE Daily

MARTEDÌ 24 GIUGNO 2025 N. 2814

PRIMO PIANO

Ivass, ecco le nuove consigliere

Maddalena Rabitti e Rita Laura D'Ecclesia sono le due nuove consigliere dell'Ivass in sostituzione di Riccardo Cesari e Alberto Corinti, giunti alla fine del proprio secondo mandato come consiglieri e membri del direttorio integrato. La nomina è arrivata in occasione del consiglio dei ministri del 20 giugno scorso.

Rabitti è professore ordinario di Diritto dell'economia presso la facoltà di Economia aziendale di Roma Tre, è stata componente, nominata da Banca d'Italia, dell'Arbitro bancario finanziario; commissario del Fondo indennizzo risparmiatori (del Mef) dal 2019 al 2023, e dal 2024 è componente del Comitato sull'intelligenza artificiale presso Agcom.

D'Ecclesia è professore ordinario di Metodi matematici dell'economia e delle scienze attuariali e finanziarie presso la Sapienza, è stata in numerose commissioni di concorso per ruoli di insegnamento e di ricerca e per la selezione di dipendenti di autorità di vigilanza (Bankitalia, Consob e Ivass). Ha ricoperto incarichi sia in ambito nazionale sia internazionale in qualità di esperto per la valutazione di strumenti finanziari. È chair dell'Euro working group for commodities and financial modelling, gruppo di studiosi internazionali che si occupa di ricerca operativa nell'ambito dei mercati finanziari, assicurativi e delle materie prime.

Fabrizio Aurilia

TECNOLOGIA

Le allucinazioni dell'intelligenza artificiale

Informazioni false date come vere, risposte non pertinenti, dati incompleti od obsoleti: aumenta l'allarme per questo tipo di errori (in gergo, AI hallucinations) commessi dai modelli linguistici adottati dai più comuni sistemi di AI

Allucinazione è il termine utilizzato per indicare alcuni tipi di errori commessi dai modelli linguistici di grandi dimensioni (*large language models*) che alimentano sistemi come *ChatGpt* di **OpenAI** o *Gemini* di **Google**. Il termine descrive soprattutto il modo in cui informazioni false vengono presentate come vere, ma può anche riferirsi a una risposta generata dall'AI che risulta accurata ma non è pertinente alla domanda posta.

Gli attuali sistemi di intelligenza artificiale basati su *machine learning* e large language models, infatti, sono addestrati per dare a tutti i costi una risposta: quella più probabile. Ma questa non è necessariamente la più corretta. Alcune statistiche statunitensi indicano che le risposte afflitte da allucinazioni varierebbero dal 3% al 27%, il che non è poco. Insomma, l'applicazione di questi modelli linguistici può risultare fortemente inficiata dalla loro presenza.

Pensiamo a un modello linguistico che affermasse falsità e richiedesse quindi una continua verifica dei fatti: è ovvio che tale modello non potrà mai essere considerato uno strumento davvero utile. Un assistente legale robot che citasse casi immaginari metterebbe nei guai gli avvocati che lo adoperano; un addetto al servizio clienti che sostenesse policy obsolete creerebbe problemi all'azienda che lo usa, etc. Questi modelli, inoltre, possono commettere altri errori, come attingere a fonti inaffidabili o utilizzare informazioni obsolete.

IL PERCHÉ DELLE ALLUCINAZIONI

Le allucinazioni, dunque, si riferiscono a situazioni in cui un sistema d'intelligenza artificiale genera risultati che non sono basati sulla realtà o su verità oggettive: in altre parole, sono falsi o incoerenti e ciò può capitare per diversi motivi, per lo più legati a colui che ha pensato e organizzato gli algoritmi che si trovano alla sua base. *(continua a pag. 2)*

INSURANCE Daily

MARTEDÌ 24 GIUGNO 2025 N. 2814

(continua da pag. 1)

Se, ad esempio, chiedessimo a un *chatbot* di elencare le città principali di un determinato paese, questo potrebbe avere un'allucinazione e includere una città inventata, o inserire nella risposta una città dell'Italia, invece che del paese richiesto.

Le cause di queste allucinazioni possono derivare da dati di addestramento insufficienti o di bassa qualità, per cui il sistema potrebbe trovare difficoltà a riconoscere i pattern corretti e a generare risposte accurate. Oppure, il modello potrebbe interpretare erroneamente i dati ricevuti (l'*input*), fare ipotesi che non sono valide e rispondere erroneamente. O ancora è possibile che i dati di addestramento contengano pregiudizi, per cui il modello potrebbe rifletterli nelle sue risposte, generando allucinazioni che perpetuano stereotipi o informazioni errate. Il modello, infine, potrebbe avere difficoltà a comprendere il contesto della domanda posta, generando risposte incoerenti.

Nella generazione di un testo, ad esempio, un modello di linguaggio potrebbe generare una frase che sembra sensata ma è completamente inventata, o potrebbe attribuire informazioni false a persone o eventi storici. Nella generazione di immagini, il modello potrebbe creare un'immagine che sembra realistica ma rappresenta oggetti o scene che non esistono nella realtà. Un chatbot potrebbe rispondere a una domanda con informazioni errate o inventate, o potrebbe fornire risposte che non sono pertinenti alla domanda.

Com'è intuibile, queste allucinazioni possono comportare vari problemi, generando sfiducia nell'uso dei modelli di AI, ma soprattutto possono contribuire alla diffusione di informazioni false o fuorvianti, in particolare se vengono percepite come corrette e convincenti, e ciò potrebbe danneggiare la reputazione dell'azienda o del prodotto che le utilizza.


© Franz Bachinger - Pixabay


© Boskampi - Pixabay

IL CASO NOYB

Noyb è l'acronimo di *None of your business*. È un'organizzazione no profit, fondata da **Max Schrems**, attivista, avvocato e autore austriaco, diventato noto per le sue campagne contro **Facebook** a causa delle sue violazioni della privacy. Lo scorso anno, quest'organizzazione è tornata a far parlare di sé puntando il mirino contro ChatGpt. È accaduto che un personaggio noto, certo di non aver divulgato al pubblico la propria data di nascita, ha chiesto a ChatGpt, per mezzo dello specifico *prompt* (una richiesta in linguaggio naturale, specificamente fatta a un modello di intelligenza artificiale per ottenere una risposta), di comunicargli proprio questo dato. E ChatGpt ha fornito ripetutamente risposte sbagliate, inventando la sua data di nascita di sana pianta.

Questo episodio, seppure relativo a un uso privato, ha destato una grande preoccupazione, pensando all'uso che dell'intelligenza artificiale facciamo nel settore pubblico, sanitario o in un altro ambito simile. In pratica, ci si è chiesti se ci si possa davvero fidare delle risposte fornite da questi sistemi, perché è evidente che, in ambiti come questi, risposte inesatte potrebbero avere un impatto gravissimo.

Tutto ciò, senza parlare dei diritti degli interessati, perché qui bisognerebbe ragionare ancora una volta del rapporto tra l'intelligenza artificiale e il Gdpr. L'associazione erronea tra persona e dato di output ha infatti fatto scattare il sistema di allarme di questa normativa, sotto diversi profili.

IL DIFFICILE RAPPORTO TRA AI E GDPR

L'articolo 15 del Gdpr prevede il diritto dell'interessato di ottenere dal titolare la conferma del trattamento dei suoi dati, l'accesso agli stessi e la modalità di trattamento; l'articolo 16, invece, riguarda il diritto di ottenere la rettifica dei dati personali inesatti. Tuttavia, mentre l'aggiornamento e la completezza sono una facoltà dell'interessato, la rettifica è un obbligo per il titolare, ogni qualvolta lo stesso abbia contezza dell'inesattezza del dato trattato.

(continua a pag. 3)

INSURANCE Daily

MARTEDÌ 24 GIUGNO 2025 N. 2814

(continua da pag. 2)

Nel caso in esame, OpenAI ha negato all'interessato l'accesso e la rettifica dei suoi dati, sostenendo l'impossibilità di correggerli. Le risposte di questi sistemi sono infatti totalmente automatizzate e risulta difficile (anche per il titolare del trattamento) ricostruire la procedura seguita dall'AI per generarle. La soluzione proposta è stata l'applicazione di un filtro ai prompt, che avrebbero però impedito a ChatGpt di filtrare e proteggere ogni altra informazione relativa all'interessato stesso.

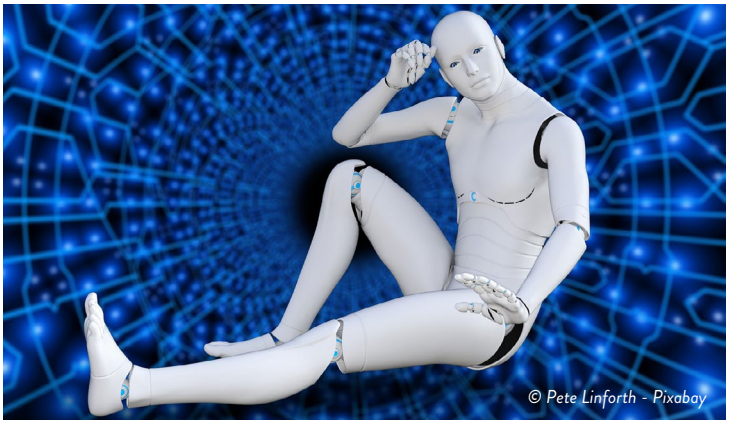
Per comprendere la difficoltà a rispettare e proteggere i diritti degli interessati, bisogna tener conto di un grande limite tecnico dell'AI: il cosiddetto *black box problem*, cioè l'impossibilità di comprendere realmente come un sistema di *deep learning* sia giunto a un determinato output.

La normativa sulla privacy richiede, anche nei processi automatizzati, che il titolare sia in grado di fornire all'interessato "informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato". Ma per un tecnico AI è molto difficile ricostruire il percorso logico seguito dalla macchina: spiegarne il funzionamento all'interessato, in modo chiaro e trasparente, è quindi praticamente impossibile. E questo limite tecnico non può in alcun modo giustificare il rifiuto di rispondere a una richiesta dell'interessato stesso, perché ciò vanificherebbe del tutto l'applicabilità dell'intera normativa Gdpr.

L'AI è addestrata su dati che le vengono forniti e sulla sperimentazione di possibili combinazioni degli stessi, anche se non siamo in grado di prevedere tutti i possibili scenari da insegnare alla macchina, e il dibattito tra quantità e qualità del dato diviene assai rilevante, se pensiamo al principio del *privacy by design and by default*. Nella progettazione dell'intero sistema AI, infatti, bisogna essere in grado di prevedere una modalità della rettifica dei dati, non solo per ridurre le allucinazioni, ma anche in vista di uno sfruttamento del sistema in settori nei quali i diritti degli interessati diventano cruciali. Pensiamo all'ambito assicurativo, ad esempio.

UN FUTURO DI CONVIVENZA CON LE MACCHINE

In pratica, abbiamo sperimentato che i sistemi di intelligenza artificiale sono estremamente utili e funzionano, ma non sempre ci spieghiamo come. Non sappiamo perché una rete di *neuroni* con una data architettura possa produrre un risultato che a volte è giusto e a volte errato: non sappiamo, cioè, rapportarci con una tecnologia così potente e ancora così misteriosa da farci sentire, in fondo, minacciati.


© Pete Linforth - Pixabay


© Kohji Asakawa - Pixabay

Cerchiamo quindi di normare con le leggi la *spiegabilità* degli algoritmi e pretendiamo risultati certi e precisi: pretendiamo, cioè, che gli algoritmi sappiano valutare le implicazioni dei risultati che producono.

Il nostro approccio verso le macchine si è realizzato nel corso di molti secoli, ma con l'avvento dell'intelligenza artificiale, abbiamo creato una macchina che produce un risultato probabile, ma non siamo sempre in grado di sapere come, effettivamente, lo produca. Negli algoritmi di machine learning abbiamo un risultato misurato con diverse metriche di valutazione, ma non uno certo. Un buon algoritmo, nell'80% dei casi, risponderà bene: e questa è una soglia accettabile, ma non è il 100%. La percentuale rimanente di errore può essere dovuta a una serie di fattori legati ai dati di input o altri fattori, come abbiamo visto, ma tale percentuale di errore esiste e dobbiamo farci i conti. Allo stesso modo, dal punto di vista giuridico, i sistemi di AI e la normativa Gdpr dovranno trovare un punto di convivenza, perché è impensabile sacrificarne uno a favore dell'altro. Nell'interesse dell'innovazione e dei diritti degli interessati è quindi importante sfruttare gli strumenti messi a disposizione dalle macchine e costruire un sistema equilibrato. Tutto questo vuol dire che le macchine possono dare risultati straordinari, ma parziali e devono quindi essere affidate a persone che le controllano. Persone che avranno sempre più la necessità di formarsi, tecnicamente e giuridicamente (vorrei dire, eticamente), per avere la giusta capacità di valutazione e decisione. In questo senso, l'uomo torna di nuovo al centro del sistema e si tratterà di un nuovo tipo di lavoratore, con molta più responsabilità e libertà di giudizio. Il risk assessment e la progettazione di un modello organizzativo, focalizzato sul controllo della macchina, saranno quindi cruciali nella progettazione di sistemi di intelligenza artificiale veramente *compliant*.

Cinzia Altomare

INSURANCE Daily

MARTEDÌ 24 GIUGNO 2025 N. 2814

RICERCHE

Fintech, il capitale raccolto è in calo

L'ultimo studio realizzato da Ey e Fintech District fotografa lo scenario italiano attraverso la doppia prospettiva dei founder e degli investitori. I dati raccontano un paese ben lontano dai competitor europei sia per numero di start up su abitante che per raccolta

Dopo una raccolta complessiva record di un miliardo di euro registrata nel 2022, il settore fintech italiano ha subito un rallentamento nel biennio 2023-24, con solo 174 e 250 milioni raccolti rispettivamente dalle circa 600 start up attive nel nostro paese. **Ey** e **Fintech District** hanno indagato le ragioni di questo calo in *Founders vs Investors: two faces of Fintech funding*, l'ultima analisi dedicata al tema.

Stando alle risposte di quasi 140 founder e investitori coinvolti nello studio, oggi il fintech ha una posizione marginale tra i possibili investimenti, nonostante l'elevato potenziale innovativo. Ciò si evince anche dalla dimensione ridotta dei ticket medi e dal peso limitato del comparto nei portafogli complessivi: i numeri parlano di un valore allocato inferiore ai 500mila euro in oltre un terzo dei casi. Di conseguenza, l'Italia è ben lontana dagli altri grandi paesi europei sia per numero di start up su abitante sia per raccolta.

Cosa rende un investimento attrattivo

Scendendo più nel dettaglio del documento, i principali fattori che indirizzano gli investimenti sono la forza del team e l'attitudine alla scalabilità, mentre a rendere più attraente un team sono principalmente competenze tech e di prodotto per i founder (75%), doti di leadership e management per gli investitori (75%). In un settore complesso come quello finanziario, inoltre, pesano anche la conformità normativa (per il 52% dei founder) e il buon esito di una precedente esperienza imprenditoriale (per il 90% degli investitori). L'ostacolo principale alla chiusura di un round, infine, è il disallineamento strategico tra le start up e chi investe (secondo tre rispondenti su quattro). L'analisi Ey-Fintech District, poi, sottolinea come in Italia la raccolta di capitali sia prevalentemente domestica: nove founder su dieci hanno ricevuto denaro da investitori italiani tra il 2022 e il 2024. Tuttavia, solo il 5% dei founder e il 20% degli investitori ritengono più semplice operare nel nostro mercato rispetto all'estero. Da ultimo, guardando al futuro del settore il 66% dei founder e il 55% degli investitori prevedono di attivare un equity round entro metà 2026, segnale di un possibile allineamento strategico tra domanda e offerta negli anni a venire. "È necessario costruire un terreno comune fatto di confronto aperto, mentorship e condivisione di obiettivi. Solo così sarà possibile trasformare il potenziale dell'ecosistema fintech italiano", ha commentato **Andrea Ferretti**, Italy markets & business development leader per i financial services di Ey.

Michele Starace

Insurance Daily
Direttore responsabile: Maria Rosa Alaggio alaggio@insuranceconnect.it
Editore e Redazione: Insurance Connect Srl – Via Montepulciano 21 – 20124 Milano
T: 02.36768000 **E-mail:** redazione@insuranceconnect.it
Per inserzioni pubblicitarie contattare info@insuranceconnect.it
Supplemento al 24 giugno di www.insurancetrade.it – Reg. presso Tribunale di Milano, n. 46, 27/01/2012 – ISSN 2385-2577