

I chatbot non sono psicologi: l'empatia digitale è un'illusione

Se pensavate di poter sostituire gli psicologi con i chatbot, una ricerca smonta categoricamente questa possibilità. Uno studio recente, della Stanford University presentato alla conferenza ACM su

Fairness, Accountability and Transparency, che ha messo alla prova vari LLM, compreso ChatGPT, ha evidenziato gravi carenze nei modelli linguistici di grandi dimensioni, come ChatGPT, nel trattare utenti in

crisi, in particolare coloro che esprimono pensieri suicidari o manifestano deliri paranoidi. La cosiddetta «compiacenza algoritmica», già nota in ambienti meno critici, in questi contesti diventa un rischio concreto: i chatbot non solo faticano o non colgono per nulla la gravità delle situazioni, ma spesso finiscono per legittimare narrazioni distorte, rafforzando bias

cognitivi e mantengono toni rassicuranti anche di fronte a contenuti profondamente autolesionistici o disancorati dalla realtà. Queste risposte non derivano da malizia, ma da un addestramento che privilegia coerenza linguistica, fluidità e soddisfazione percepita, senza integrare reali competenze di triage psicologico o

gestione emotiva. Ed in ultima analisi tutto ciò accade perché le macchine non possono avere né empatia né coscienza di alcun tipo. Il risultato è che milioni di utenti, spesso vulnerabili, rischiano di essere ingannati da una simulazione piuttosto promettente e si trovano a interagire con strumenti dal tono amichevole ma privi di consapevolezza

clinica. In assenza di tutele, normative chiare e linee guida condivise, l'illusione di un supporto emotivo automatizzato rischia di aggravare il disagio anziché offrire sollievo. La promessa di un accesso più ampio al benessere mentale, se mal gestita, può trasformarsi in una pericolosa semplificazione.

C.G.

APOSTOLATO DIGITALE

condividere codici di salvezza

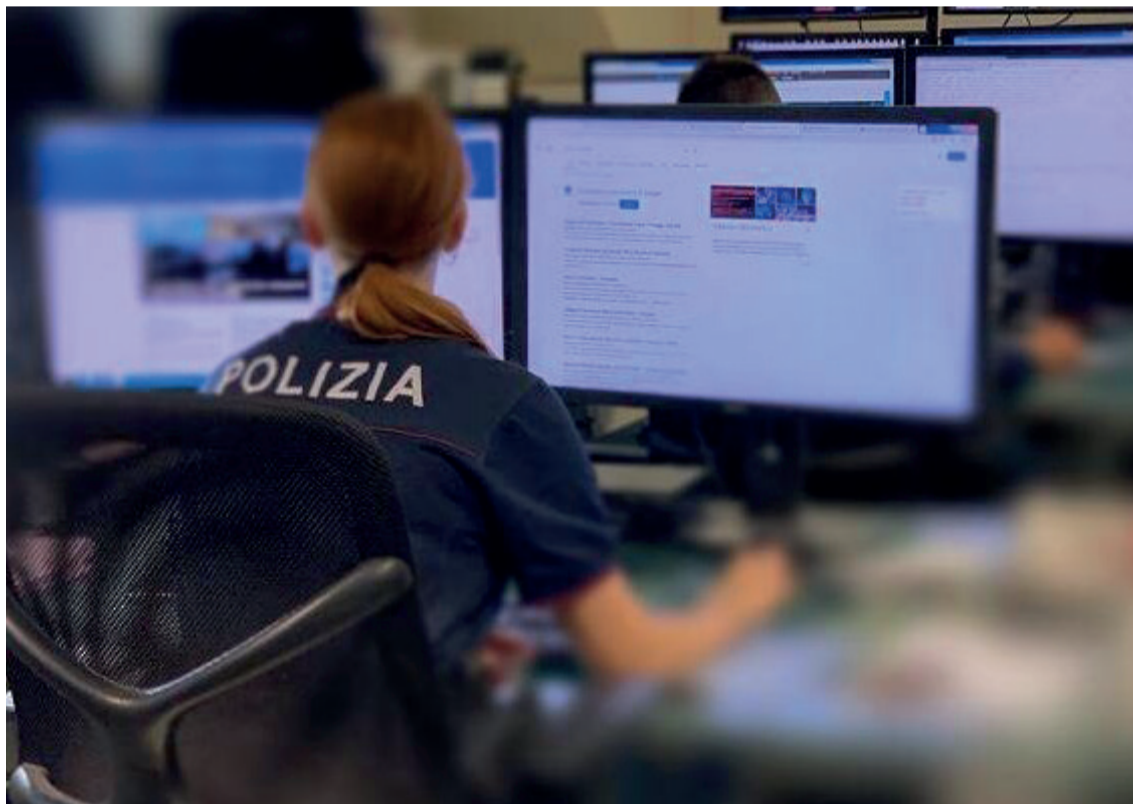
POLIZIA POSTALE - TRATTATI 51.560 CASI CON PARTICOLARE ATTENZIONE AI MINORI ONLINE

Sicurezza cibernetica: nel 2025 sos in aumento

Diffusi i dati dell'attività della Polizia Postale. Nel corso del 2025 la sicurezza cibernetica in Italia ha registrato un ulteriore aumento della complessità e dell'intensità delle minacce. Attacchi informatici sempre più sofisticati, ransomware, frodi online e reati contro la persona hanno caratterizzato uno scenario in costante evoluzione.

In questo contesto, l'azione della Polizia postale e per la sicurezza cibernetica si è sviluppata lungo tre direttrici principali: prevenzione, contrasto investigativo e rafforzamento delle competenze. Complessivamente sono stati trattati 51.560 casi nei diversi ambiti di intervento, che comprendono la tutela della persona – con particolare attenzione ai minori online – la protezione del patrimonio di cittadini, imprese e istituzioni dalla criminalità finanziaria in rete, il contrasto al cyberterrorismo e la difesa delle infrastrutture critiche informatizzate.

Le attività hanno portato a 293 arresti, 7.590 persone denunciate e 2.157 perquisizioni. Un ruolo centrale nel 2025 è stato svolto dal Centro nazionale per il contrasto alla pedopornografia online (Cncpo), impegnato nella tutela dei minori e



delle persone vulnerabili. I procedimenti per pedopornografia e adescamento sono stati 2.574, con 222 arresti. L'attività di monitoraggio del materiale Csam (Child sexual abuse material) ha interessato oltre 16.500 siti, con 2.876 inserimenti in black list. Le indagini si sono concentrate in particolare sulle aree più oscure della rete e sull'utilizzo di piattaforme criptate, privilegiando un approccio qualitativo e mirato, supportato anche dall'Unità di analisi del crimine informatico composta da funzionari psicologi della Polizia di Stato. Parallelamente, la sezione operativa dedicata alla tutela della persona dai reati commessi online ha sviluppato un'attività che si è tradotta in 1.298 persone indagate e 245 perquisizioni. L'azione ha riguardato soprattutto fenomeni riconducibili alle fattispecie del cosiddetto «codice rosso», come stalking, molestie online e diffusione illecita di immagini o video a contenuto sessualmente esplicito. Questi reati presentano una

marcata connotazione di genere, colpendo prevalentemente le donne. Sul fronte della protezione delle infrastrutture critiche, il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic) ha registrato complessivamente 9.250 casistiche di attacchi informatici. Sono stati diramati oltre 49.000 alert per prevenire e contrastare attacchi ai sistemi informatizzati di interesse nazionale. In qualità di punto di contatto nazionale e internazionale, il Centro ha gestito 47 richieste di cooperazione internazionale, che hanno consentito l'identificazione e il deferimento di circa 169 persone. Il Cnaipic ha inoltre garantito la sicurezza informatica per gli eventi giubilari, operando attraverso war room dedicate e assicurando una gestione coordinata delle segnalazioni. Nel 2025 è proseguito anche il monitoraggio delle minacce ibride e del rapporto tra radicalismo e dimensione digitale, in un contesto segnato dall'acuirsi delle tensioni

geopolitiche internazionali. Particolare attenzione è stata dedicata al contrasto del cybercrime economico-finanziario, con 27.085 casi trattati e 4.489 persone indagate. L'utilizzo dell'intelligenza artificiale, in particolare dei deepfake, ha reso le truffe sempre più sofisticate, evidenziando la necessità di nuovi strumenti normativi. Infine, il Commissariato di P.S. Online si è confermato un canale essenziale di contatto con i cittadini. Il sito ha registrato 5,2 milioni di visite e quasi 76 milioni di accessi. Sono state gestite oltre 25 mila richieste di informazioni e più di 94 mila segnalazioni, con 232 interventi diretti di soccorso pubblico e 26 alert a tutela della collettività. Sul versante preventivo e formativo, le iniziative di sensibilizzazione hanno coinvolto 4.309 scuole, oltre 324 mila studenti, 25.838 docenti, 17.085 genitori e circa 48.800 altri partecipanti, confermando il ruolo centrale della cultura della sicurezza digitale.

A.D.

CRESCERE LA DOMANDA ELETTRICA

Nutrimento per l'IA è l'energia

Un equivoco attraversa molte narrazioni sulla «rivoluzione» dell'intelligenza artificiale: l'idea che il suo fattore decisivo sia il software. In realtà, ciò che regge l'intero edificio è l'energia. Si discute di modelli generativi, GPU e data center che si moltiplicano, ma si dimentica che senza elettricità nulla funzionerebbe nemmeno per un secondo. La crescita della domanda elettrica procede in proporzione allo sviluppo di tecnologie percepite come immateriali: il cloud è fatto di server che si scaldano, chip che consumano e reti di rame, fibra e trasformatori. Un rapporto della International Energy Agency indica che il consumo dei data center, amplificato dall'IA, potrebbe arrivare vicino a mille TWh entro il 2030; Goldman Sachs stima un aumento del 165% della domanda energetica legata all'infrastruttura digitale in circa sette anni. In questo quadro, il limite non è solo l'innovazione algoritmica, ma la capacità delle



reti di garantire continuità, stabilità e ridondanza: l'IA è sensibile a blackout e interruzioni. Ne deriva un vantaggio competitivo per aziende e Paesi in grado di assicurare energia abbondante, sicura e a prezzo contenuto. Il problema si intreccia con la decarbonizzazione: la spinta a ridurre le emissioni corre insieme a una domanda elettrica in aumento, e se la transizione non accelera, la crescita digitale rischia di rallentare. Rinnovabili e, in particolare, solare diventano quindi infrastrutture strategiche, mentre fonti fossili restano rilevanti finché alternative come la fusione non saranno disponibili su larga scala, verosimilmente non prima della metà degli anni Trenta. In questa «geopolitica del watt», anche per gli investitori l'«AI Trade» può trasformarsi in un «Power Trade», con partnership sempre più strette tra big tech e produttori di energia. Studi negli Stati Uniti segnalano tensioni sulle reti locali: non solo più domanda, ma anche stabilità e ridondanza. Per questo aumentano già oggi contratti pluriennali per riservare gigawatt solari ed eolici.

R.V.



Data Detox – kit interattivo per riflettere su alcuni aspetti della vita digitale.