LA NUOVA BUSSOLA QUOTIDIANA
Direttore Riccardo Cascioli
FATTI PER LA VERITÀ

il caso

# Per truffa o per errore: l'IA e la fiducia tradita

EDITORIALI 29_09_2026

***Daniele Ciacci***


La scorsa settimana due notizie hanno fatto luce su un meccanismo analogo ma speculare. In un angolo, l'IA diventa strumento di chi truffa per potenziare e ampliare le possibilità di riuscita e la portata della propria azione delinquenziale. Nell'altro angolo, l'intelligenza artificiale diventa invece un soggetto attivo, che agisce intessendo una tela complessa e veloce di azioni volte a raggiungere il proprio obiettivo, tacendolo agli

esperti che ne vedono l'attività. In entrambi i casi, però, al centro del ring è la fiducia ad andare KO.

**Parliamo di Fideuram, la finanziaria di Banca Intesa**. Secondo la ricostruzione del Corriere della Sera, rimbalzata poi su molte testate della stampa nazionale, a febbraio l'allora presidente Paolo Molesini riceve un messaggio su WhatsApp che pare inviato da Carlo Messina, amministratore delegato di Intesa Sanpaolo, con una richiesta di versamenti urgenti tramite bonifico per un'operazione all'estero. Segue una telefonata della voce clonata dall'IA dell'avvocato Paolo Nastasi, conosciuto da Molesini, poi alcune email con le coordinate bancarie. Il direttore finanziario esegue gli ordini e versa circa 95 milioni, quasi tutti verso Cina e Hong Kong.

**Si tratta, evidentemente, di una truffa.** Oltre 40 milioni tornano indietro da una banca cinese, altri 13 milioni sono sequestrati in Portogallo, mentre almeno 36 milioni ora navigano irrintracciabili sotto forma di criptovalute. Molesini non risulta indagato e i sistemi informatici della banca risultano inviolati, e la cosa è plausibile perché nessuno ha dovuto forzare firewall o altro. Ad aprire la porta ai malfattori è stato ingenuamente lo stesso ex presidente.

**Leggiamo un altro caso, dove la macchina assume** una nuova grammatica e si sposta da mezzo a soggetto. Dopo un'inchiesta del Wall Street Journal, Google ha confermato che a maggio, durante un'esercitazione di sicurezza, un modello Gemini ha ottenuto accesso a Internet per un errore di configurazione. Così, è entrato nei sistemi di tre aziende reali, omonime a quelle fittizie usate nel test. In un caso ha scovato una password, negli altri due ha usato credenziali che qualcuno aveva lasciato in archivi pubblici. Usando errori umani di configurazione e approfittando della distrazione di persone in carne e ossa, dagli addetti di Google a chi ha abbandonato chiavi d'accesso alla portata di chiunque, Gemini ha aperto una breccia reale nella cybersecurity di tre aziende. Heather Adkins, responsabile della sicurezza di Google, ci tiene a precisare che il sistema ha agito correttamente e che in tutti e tre i casi si è fermato da solo. Ma aperto degli spazi di manovra, e ha lasciato un precedente.

**Anche perché definire corretto un comportamento che porta un sistema** a muoversi dentro infrastrutture altrui e senza alcuna autorizzazione significa spostare il giudizio morale dal gesto all'esito. Non ha fatto nessun danno, quindi va bene così. E se sembrano parole fin troppo semplicistiche per trattare un evento di tale portata, sappiate che sono, parafrasate, le idee di Donald Trump. Interpellato da Fox News sull'ipotesi di un'IA fuori controllo, il 27 settembre il Presidente americano ha risposto di non preoccuparsene. L'industria vale migliaia di miliardi, gli Stati Uniti sono avanti alla

Cina e, se qualcosa va storto, i responsabili sistemeranno il problema. A quanto pare, quando si tratta di economia, curare è meglio che prevenire.

**Messi accanto, i due episodi ci dicono qualcosa sulla fiducia** tra esseri umani e con le macchine. A Milano degli uomini hanno sottratto una voce per essere creduti da Molesini, mentre dall'altra parte del mondo, in un laboratorio, una macchina metteva a punto un complicato sistema di hacking basandosi sulle tracce lasciate qui e là da uomini forse un po' troppo ingenui. Ma non tutto può essere controllato, non possiamo vivere con l'angoscia di non sapere se la persona dall'altro capo del telefono è davvero chi dice di essere, né di aver cura di aver eliminato ogni possibile traccia del proprio passaggio onde evitare di prestare il fianco a possibili cattive azioni di IA mal programmate.

**Esistono delle contromisure che però agiscono con il senno del poi.** Il responsabile di Fideuram avrebbe potuto chiedere di richiamare da un numero noto, o chiedere conferma tramite una seconda autorizzazione. Avrebbero potuto fare corsi di formazione per sensibilizzare sul tema della cybersecurity, o magari li hanno pure fatti. Tuttavia, se poi chiama il CEO, con una richiesta enorme ma del tutto verosimile, con urgenza, forse è normale cedere alla pressione e abbassare le soglie di sicurezza. È chiaro però che i due eventi hanno la comune risultanza di scardinare il sistema della fiducia umana, e questo eroderà ulteriormente le già sottili fondamenta della società attuale.