

## Una fuga di dati rivela il panorama dietro alle “fidanzate” IA

Il portale **Muah.ai**, specializzato in “**fidanzate IA**” prive di censura, è stato hackerato. Per una volta, non si è trattato di uno dei sempre più frequenti attacchi ransomware, di cybercriminali pronti a chiedere un riscatto, bensì di un normale utente che, incuriosito, si è infiltrato negli archivi dell’azienda, scoprendo contenuti pensati per simulare rapporti abusivi nei confronti di **minori**.

“Ho fatto un salto sul sito per masturbarmi e ho notato che il portale era messo in piedi alla bene e meglio”, ha riferito l’uomo a [404 Media](#), testata che ha avuto l’occasione di consultare i file trafugati a Muah.ai. “In pratica è un insieme di progetti open-source che sono stati uniti insieme con lo sputo. Ho iniziato a guardarmi in giro e ho scoperto rapidamente alcune vulnerabilità”. Infastidito da ciò che ha visto, l’hacker ha fatto trapelare le discussioni registrate dal chatbot alla stampa.

Nell’archivio sono presenti richieste relative a argomenti più o meno spinti. Le sollecitazioni dalle tinte sadomaso sono comuni, quindi ci sono derive che si concentrano sulle più controverse fantasie di rapporti non consensuali. Ad allarmare l’informatico sono però stati i **richiami espliciti alla pedopornografia**, a orge incestuose e alla sessualizzazione dei bambini in fasce. I file esfiltrati all’azienda non riportano quali risposte abbia prodotto lo strumento, ma rivelano comunque quali siano i contenuti prevalenti cercati tramite *prompt* dagli utenti della piattaforma.

Ufficialmente, Muah.ai si appoggia su policy che proibiscono qualsiasi forma di eroticizzazione dell’infanzia, una posizione che è stata recentemente ribadita dai moderatori del portale, interpellati in occasione di questa fuga di dati. L’azienda non ha tuttavia negato la **veridicità delle informazioni** fornite dall’hacker, lamentando piuttosto che “la fuga di dati è stata finanziata dai nostri concorrenti dell’industria IA priva di censure, i quali sono guidati dal profitto. Muah Ai si presta a essere un bersaglio poiché è un progetto alimentato dalla comunità”.

L’azienda ha scoperto di essere stata compromessa la settimana scorsa e ha prontamente notificato la situazione ai suoi utenti attraverso il social network Discord. Il messaggio pubblicato dai gestori malcelava la loro frustrazione, tuttavia assicurava al pubblico che “i vostri messaggi di chat non sono mai conservati, tutto viene cancellato”. L’evolversi della vicenda dimostra l’opposto: attingendo ai dati dell’hacker, *404 Media* è riuscita a **risalire ai contatti degli utenti**, chiedendo loro un commento. Nessuno di loro ha offerto un riscontro.

Il fenomeno dei servizi parasociali su base IA è esploso durante il 2020, in concomitanza con la pandemia e con la progressiva diffusione dei modelli di *machine learning*. Dal nulla sono

## Una fuga di dati rivela il panorama dietro alle “fidanzate” IA

emerse realtà di piccole dimensioni dalla natura finanziaria e gestionale vagamente torbida. Spesso, il servizio viene erogato in via gratuita previa registrazione, magari riservando le funzioni “adulte” a dei contratti di abbonamento. Gli strumenti generativi IA e i chatbot sono d'altronde sempre più semplici da programmare e condividere online, un'accessibilità che da una parte favorisce virtuose possibilità, ma che dall'altra offre potenti mezzi con cui truffatori e dilettanti possono imbastire servizi tutt'altro che sicuri.

Essendo un raro spaccato di - involontaria - trasparenza, quanto accaduto a Muah.ai rappresenterà un caso studio importante attraverso cui ricercatori e legislatori potranno sondare i vari utilizzi delle intelligenze artificiali. Allo stesso tempo, questo genere di situazioni rischiano di essere manipolate, più che studiate. Sempre più Governi stanno facendo leva sulle paure riguardanti terrorismo e pedopornografia per suggerire che la società debba eliminare ogni forma di anonimato digitale, una posizione che è spesso più propedeutica a favorire il controllo statale, piuttosto che la tutela degli individui.

[di Walter Ferri]