



USA, via al maxi piano di sorveglianza sui social

Descrizione

(Adnkronos) Le autorità statunitensi stanno pianificando un'espansione radicale delle proprie capacità di sorveglianza online. Secondo documenti federali esaminati da Wired, l'agenzia ICE sta cercando aziende private per realizzare un programma pluriennale di monitoraggio dei social media, gestito da due centri strategici poco conosciuti situati in Vermont e in California meridionale. L'obiettivo è trasformare i contenuti pubblici pubblicati su piattaforme come Facebook, TikTok, Instagram, YouTube e Reddit in dossier operativi per alimentare retate e arresti.

Il progetto è ancora nella fase preliminare di raccolta dell'interesse da parte dei potenziali appaltatori, ma le bozze interne mostrano un piano estremamente ambizioso. L'ICE vuole strutturare un sistema attivo 24 ore su 24, con team di analisti in grado di gestire centinaia di casi in tempi strettissimi e supportati dai più avanzati strumenti di sorveglianza in abbonamento. Il cuore dell'operazione sarà costituito da due dei tre centri di targeting dell'agenzia: il National Criminal Analysis and Targeting Center di Williston (Vermont), responsabile della costa orientale, e il Pacific Enforcement Response Center di Santa Ana (California), operativo sette giorni su sette, ventiquattr'ore su ventiquattro.

A Williston sarà dispiegata una squadra di una dozzina di analisti, compreso un program manager, mentre a Santa Ana lavoreranno 16 addetti, tra cui senior analyst e ricercatori. In ogni momento, almeno un analista senior e tre ricercatori saranno presenti per garantire continuità operativa. Questi team agiranno come vere e proprie antenne d'intelligence per la divisione Enforcement and Removal Operations di ICE: riceveranno segnalazioni, condurranno ricerche approfondite online e produrranno dossier da trasmettere agli uffici sul campo per pianificare interventi.

Gli analisti dovranno concentrarsi su open source intelligence: post pubblici, foto, commenti e messaggi visibili su social network e forum, inclusi siti meno noti o basati all'estero come VKontakte. A disposizione avranno anche potenti archivi commerciali come LexisNexis Accurint e Thomson Reuters Clear, che aggregano dati personali provenienti da utenze domestiche, registrazioni di veicoli, bollette e proprietà immobiliari, rendendo ogni profilo facilmente consultabile.

Le tempistiche saranno serratissime: i casi di massima priorità, come potenziali minacce alla sicurezza nazionale o persone nella "Top Ten" dei ricercati, dovranno essere analizzati entro 30 minuti, i

casi urgenti entro un'ora, quelli ordinari entro la giornata lavorativa. L'obiettivo minimo è evadere almeno il 75% delle pratiche nei tempi stabiliti, con le aziende migliori attese a raggiungere il 95%. Il piano non riguarda solo il personale. L'ICE chiede espressamente ai futuri appaltatori di integrare algoritmi e sistemi di intelligenza artificiale per automatizzare parte delle operazioni, in linea con altre iniziative recenti. Oltre un milione di dollari l'anno sarà destinato all'acquisto dei software di sorveglianza più sofisticati disponibili sul mercato.

Negli ultimi anni ICE ha costruito un'infrastruttura di sorveglianza digitale sempre più ramificata. Ha acquistato strumenti come SocialNet di ShadowDragon, capace di aggregare dati da oltre 200 piattaforme, e Locate X di Babel Street, che permette di ricostruire movimenti fisici attraverso i dati di localizzazione di app comuni, senza bisogno di mandato. Ha inoltre firmato contratti multimilionari con Clearview AI, l'azienda di riconoscimento facciale che ha costruito il suo database estraendo miliardi di immagini dal web.

Il programma arriva dopo rivelazioni inquietanti. All'inizio dell'anno, The Intercept ha riportato che l'ICE stava valutando sistemi per individuare automaticamente sui social media sentimenti negativi verso l'agenzia, segnalando utenti con presunta propensione alla violenza. Osservatori e associazioni per i diritti civili hanno denunciato il rischio che tali sistemi non distinguano tra minacce reali e critica politica, aprendo la strada a una sorveglianza del dissenso. Organizzazioni come l'Electronic Privacy Information Center e l'ACLU hanno intentato cause contro l'agenzia, sostenendo che la raccolta massiva di dati tramite broker privati e software di localizzazione costituisca una minaccia grave alla privacy e ai diritti costituzionali, aggirando i controlli giudiziari previsti dalla legge.

??

tecnologia

webinfo@adnkronos.com (Web Info)

Categoria

1. Tecnologia

Tag

1. tec

Data di creazione

Ottobre 6, 2025

Autore

redazione