I social media sono utilizzati dalla polizia e dalle agenzie di intelligence per raccogliere dati biometrici. Nicholas West

Tra la crisi di **Facebook/Cambridge Analytica** sulla sorveglianza generale e sull'utilizzo abusivo dei dati privati degli utenti, c'è una tendenza emergente che è **infinitamente più inquietante**.

Il primo episodio è apparso recentement nel Regno Unito, dove la polizia ha ammesso di aver utilizzato una **foto inviata tramite WhatsApp** per raccogliere le **impronte digitali** che in seguito sono state utilizzate per **condannare 11 persone** per reati di droga. Non si tratta di un caso isolato o particolare, ma di

> **una tecnica sviluppata appositamente per utilizzare la grande quantità di foto pubbliche disponibili**

e per estrarre prove da immagini pubblicate o trasmesse online.

Come riportato da Dawn Luger per *The Daily Sheeple*, questa nuova tecnica è in fase di implementazione e le forze dell'ordine la definiscono "innovativa", in quanto è in grado di estrarre informazioni anche da foto parziali:

> *Tutto è iniziato con una busta contenente droga. La busta ha permesso alla polizia di individuare un telefono contenente un messaggio di WhatsApp e un'immagine di pillole di ecstasy sul palmo della mano di una persona. Il messaggio diceva: "In vendita – pillole di ecstasy con marchio Skype e Ikea … sei interessato?"*
>
> *Il telefono è stato inviato alla polizia del Galles del Sud, dove è stata migliorata la foto che mostra la parte centrale e inferiore di un mignolo.*
>
> *[…]*
>
> *"Nonostante sia stata fornita solo una piccola parte dell'impronta digitale visibile nella fotografia, il team è stato in grado di identificare con successo l'individuo", ha affermato Dave Thomas, responsabile delle operazioni forensi presso l'Unità di supporto scientifico.*

Nessuna informazione specifica è stata effettivamente fornita dal dipartimento di polizia su questa “tecnica pionieristica delle impronte digitali”, ma è abbastanza chiaro che questo è uno strumento che sono pronti e disposti a usare.

Nel frattempo, si scopre che Facebook sembra utilizzi le informazioni sul riconoscimento facciale per molto più che il semplice riconoscimento delle persone che rientrano nella tua cerchia sociale privata. E’ stata appena approvata da un giudice dell’Illinois una causa multimiardaria in cui si illustra la portata dei dati personali che Facebook conserva sulle persone, come sono disposti a distribuire questi dati e la mancanza di garanzie contro le violazioni esterne:

> *La classe di utenti di cui si parla risale al giugno 2011, quando Facebook aveva un data base utenti dell’Illinois di oltre 6 milioni di persone, secondo gli avvocati dei querelanti. “…nel gennaio 2011 l’utente medio è stato taggato in 53 foto, molto più delle 10 necessarie per generare un modello di faccia”, secondo un deposito giudiziario di dicembre.*
>
> *I difensori della privacy hanno affermato che i miliardi di immagini che si ritiene raccolga Facebook potrebbero essere ancora più preziosi per i* ***ladri di identità*** *rispetto ai nomi, agli indirizzi e ai numeri delle carte di credito ora presi di mira dagli hacker. Mentre questi tipi di informazioni sono modificabili, i dati biometrici delle retine, impronte digitali, mani, geometria del volto e campioni di sangue sono identificatori univoci.*
>
> *(Fonte)*

Eppure, non solo gli hacker e le società di social media trovano importanti questi dati. Secondo un nuovo rapporto di *Forbes*, anche gli ex agenti dell’intelligence militare stanno creando i propri database da informazioni biometriche pubblicamente disponibili.

Forbes ha identificato una società israeliana di nome Verint composta da ex spie che hanno creato un servizio chiamato **Face-Int** basato sulla raccolta biometrica online. Inoltre, il loro sistema di raccolta dei dati è un sistema che si diffonderà quasi sicuramente (se non lo è già) dato che "sono stati a lungo collaboratori del governo degli Stati Uniti, fornendo tecniche spionistiche all'avanguardia alla NSA, alla Marina degli Stati Uniti e a innumerevoli altre agenzie di informazione e sicurezza."

> **Naturalmente, l'obiettivo dichiarato delle attività della compagnia è di perseguire i terroristi**

Questa è la giustificazione generica per introdurre nuove tecnologie di sorveglianza. Si dovrebbe dare credito a *Forbes* per capire qual è la realtà che c'è dietro questa propaganda, come afferma il loro articolo (enfasi aggiunta):

> *Sebbene Terrogence (ora Verint – Ed.) si concentri principalmente nell'aiutare le agenzie di intelligence e le forze dell'ordine a combattere il terrorismo online, i profili di LinkedIn di impiegati attuali e precedenti indicano* ***che è coinvolta in altri settori, anche politici.*** *Un ex membro dello staff, descrivendo il suo ruolo di analista di Terrogence, ha affermato che avrebbe* ***"condotto operazioni di gestione della percezione pubblica per conto di clienti governativi stranieri e nazionali"*** *e utilizzato* ***"pratiche di intelligence open source e metodi di ingegneria dei social media per indagare su questioni politiche e gruppi sociali."***

Naturalmente, dal momento che nessuno dei problemi relativi all'utilizzo dei nostri dati online privati □□per le applicazioni delle forze dell'ordine è stato mai divulgato completamente prima dell'implementazione, ora siamo affiancati da un intrusivo apparato di sorveglianza in tempo reale che raccoglie le nostre informazioni senza consenso.

Inoltre, questa rete di informazioni pubblica-privata si sta

rapidamente evolvendo. Ci stiamo trasformando da esseri umani in **algoritmi digitali** in cui la nostra intera esistenza si trova a un solo clic di distanza.

di Nicholas West

Fonte: Activist Post

Traduzione: www.altreinfo.org

***

Sorvegliati via smartphone: Singapore, governa Big Data

Tech-Gleba senza alternative (parte I). Paolo Barnard

Arrivano gli scarafaggi cyborg, insetti veri controllati come robot. Madison Margolin

Atlas: "se qualcuno non ti permette di raggiungere il tuo obbiettivo, sopprimilo". Kian Brandon

Il microchip RFID: che cos'è e come funziona

La UE ci renderà devoti europeisti. Col sistema cinese. Maurizio Blondet

***