

Nella primavera del 2020, lo Stato del Minnesota si è trovato sotto i riflettori di tutto il mondo a causa della tragica morte di George Floyd, ennesimo afroamericano deceduto tra le mani degli agenti di polizia. All'omicidio seguirono i moti di protesta del movimento Black Lives Matter, ma anche la creazione **Operation Safety Net (OSN)**, un programma governativo pensato per condividere documenti e semplificare le indagini sui disordini che hanno accompagnato le manifestazioni. Due anni dopo, le marce di massa si sono significativamente ridimensionate, ma l'OSN è più attivo che mai e **in Minnesota si schedano persino i giornalisti.**

Sia chiaro, non stiamo parlando di sospetti o di criminali, ma di soggetti che nell'ultimo anno sono stati presi da parte durante le manifestazioni per poi essere **immortalati dagli smartphone delle Forze dell'ordine.** Nessuna accusa, nessun arresto, solamente un approccio forzato e informale utile a strutturare un non meglio specificato "sistema". Questo sistema, ha scoperto un'indagine del *MIT Technology Review*, altri non è che una delle molte app che le polizie a stelle e strisce acquistano da imprenditori privati, app che in questo caso adotta la dimensione della sorveglianza e dell'intimidazione.

Nello specifico si parla di **Intrepid Response**, un prodotto della Intrepid Networks che consiste in un database personalizzabile attraverso cui gruppi di persone possono ottimizzare la "*situational awareness*" durante le operazioni di emergenza. Come capita regolarmente in queste occasioni, il reparto marketing dell'azienda rimarca come il software sia pensato per «salvare delle vite», tuttavia lo strumento viene effettivamente usato per avere una maggior consapevolezza di chi stia partecipando a eventi di protesta, cosa che va di fatto ad annullare l'elemento di anonimato garantito dalla folla.

Una volta registrati i dati, l'app tiene a mente la foto, l'anagrafica del soggetto immortalato e la geolocalizzazione del luogo in cui è stato compiuto lo scatto. Di per sé, il programma non è dotato di algoritmi di riconoscimento facciale, ma, bisogna ricordare, il Minnesota Fusion Center può facilmente rimediare a questa mancanza facendo affidamento allo **Homeland Security Information Network**, la quale contiene a sua volta meccanismi di registrazione biometrica [forniti da entità terze](#) quali Clearview AI, Vigilant Solutions, Acuant FaceID o altri ancora.

Le autorità del Minnesota hanno dichiarato che i file di Intrepid Response non siano usciti al di fuori dei confini statali e che non siano nemmeno stati processati attraverso algoritmi di riconoscimento facciale, tuttavia le foto **non sono ancora state cancellate**, se non altro perché queste rappresentavano una prova essenziale per una causa che si è recentemente conclusa con un patteggiamento.

Ora, a rigore di logica, la polizia dovrebbe ripulire i propri server dalle informazioni raccolte in maniera coercitiva, tuttavia è facile credere che gli agenti si terranno ben saldi i dati raccolti, magari giustificando la propria inefficienza con il fatto che il processo di analisi e rimozione delle schede richieda molto tempo. Certo, a questo punto potrebbe intervenire Intrepid Networks stracciando il contratto siglato con le autorità, tuttavia questo scenario pare assai poco probabile, visto che il CEO Britt Kane, informato di questo abuso, ha semplicemente detto di «non voler dar voce a preoccupazioni o a mancanza di queste», tacitamente adottando una posizione di neutralità che lascia a intendere una certa malizia.

[di Walter Ferri]