Il Grande Fratello è GIÀ QUI

Ricavare il perfetto identikit di una persona dalle tracce che lascia sul web, e il tutto in un tempo brevissimo. Ora è possibile con un software utilizzato dalle forze dell'ordine e dalle agenzie investigative americane. Fino a che punto le ragioni della sicurezza pubblica possono invadere lo spazio individuale?

di Stefano Piazza e Luciano Tirinnanzi

Il sogno delle agenzie di intelligence e delle polizie di tutto il mondo si è avverato. Attraverso un unico software spia oggi è possibile scandagliare contemporaneamente le attività di una singola persona sull'intera rete internet, ricavandone la più accurata mappa di attività - anche offline - di un utente.

In pratica, chi lo usa può vedere la cosiddetta «impronta digitale» che ognuno di noi lascia ogni volta che naviga in rete o apre un'app. Il software in questione, realizzato dall'azienda americana ShadowDragon, è denominato *SocialNet*, mentre un suo omologo èstato battezzato *OIMonitor*. Entrambi sono capaci di penetrare ovunque e catturare email, foto, numeri di telefono, conversazioni scritte o audio, finanche le attività del dark web, la sottorete illegale di internet.

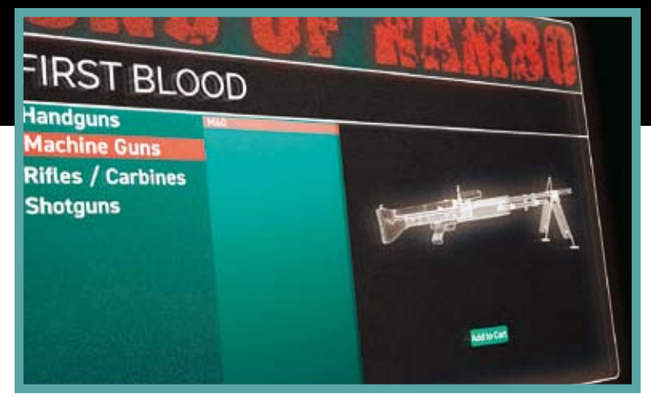
L'obiettivo? Rintracciare persone dappertutto, profilarle e scovare eventuali segnali che potrebbero rappresentare una minaccia, al fine di prevenire crimini. Pensati per dare alle forze dell'ordine la possibilità di identificare in tempo reale soggetti coinvolti in indagini e impedire loro di mettre in pratica future attività illecite, *SocialNet* e *OIMonitor* hanno già surclassato il famigerato software israeliano *Pegasus*, pietra dello scandalo internazionale perché usato illecitamente dai governi per spiare gli smartphone di giornalisti, oppositori politici, attivisti per i diritti umani e manager.

Con la recrudescenza del fenomeno terroristico di matrice islamica e l'allargamento esponenziale delle attività criminali in rete, la sorveglianza informatica è ormai diventata un luogo obbligato per l'attività delle forze dell'ordine e delle agenzie di sicurezza. Tuttavia, i confini della liceità del suo impiego - con tutte le concrete conseguenze sulla privacy - non sono ancora stati opportunamente approfonditi. A chiarire l'uso possibile del software-spia statunitense ci ha dovuto pensare un pool di giornalisti d'inchiesta della testata americana *The Intercept*. I reporter sono riusciti a ottenere copia del contratto d'acquisto siglato dalla polizia del Michigan con l'azienda Kaseware (che ha venduto due dei software prodotti dalla ShadowDragon), gestore di numerosi asset informatici della polizia statunitense e, in particolare, degli algoritmi anticrimine.

Secondo quanto dichiarato dalla stessa ShadowDragon, la piattaforma *SocialNet* permette alla polizia di accedere ai dati di oltre 120 reti di social

Controlli «secondo la legge»
«Gli strumenti investigativi a nostra disposizione vengono utilizzati solo in combinazione con indagini penali, seguendo tutte le leggi statali e federali» garantisce a *Panorama* una fonte della polizia del Michigan.

Analisi accelerata
Il sistema *SocialNet* è in grado di analizzare un centinaio di piattaforme social - tra cui le diffusissime WhatsApp e Telegram ma anche dati nel dark web - e di tracciare in pochi secondi l'«identikit» delle attività digitali di una persona.



GettyImages

media, siti web d'ogni sorta, compresi gli e-commerce (per esempio, traccia ogni ricerca e/o acquisto su Amazon) e analizza tutte le news sulle quali ci si è soffermati.

Fondamentalmente, si risale al codice identificativo che ciascuno di noi utilizza per navigare, e lo si «aggancia».

***Panorama*, che ha potuto visionare in esclusiva una versione «demo» del prodotto**, non può che confermare che possono essere monitorate anche le chat su WhatsApp, Telegram e altri strumenti di messaggistica criptata, considerati sino a oggi «sicuri» e «impenetrabili».

La conferma di ciò deriva implicitamente anche dal fatto che tra i clienti che usano maggiormente i servizi di ShadowDragon non figurano soltanto la polizia del Michigan e del Massachusetts ma pure, solo per citarne alcuni: l'agenzia americana per l'immigrazione e le dogane; decine di altri dipartimenti di polizia degli Stati Uniti; persino le due grandi agenzie di intelligence Usa - l'Fbi e la Cia.

Tutte realtà costantemente sotto pressione sia a causa di allarmi terroristici legati alla jihad globale, sia agli estremisti di destra (che, il caso più clamoroso, lo scorso gennaio hanno occupato il Congresso Usa).

Il portavoce della polizia del Michigan, Shanon Banner, è stato l'unico sinora a commentare le potenzialità del software, dichiarando che «gli strumenti investigativi a nostra disposizione come parte di questo contratto vengono utilizzati solo in combinazione con indagini penali, seguendo tutte le leggi statali e federali».

In realtà, *SocialNet* era nata con l'idea di fermare «l'uomo qualunque» ovvero quei soggetti insospettabili che, d'improvviso, colti da un impulso omicida, si armano fino ai denti e fanno irruzione nelle scuole, nei supermercati o nei campus universitari, compiendo stragi apparentemente senza premeditazione. Un fenomeno purtroppo ben noto in America, e oggi diffuso anche altrove.

«È UN PROCESSO CHE RISALE INDIETRO NEL TEMPO E PER FARE QUESTO ANALIZZA UN'ENORME MOLE DI DATI»

Secondo Pierluigi Paganini, ceo di Cybhorus ed esperto di cybersecurity, «il sistema è in grado di correlare questi dati con informazioni provenienti da altre fonti, quali conversazioni in gruppi e canali delle principali app di "instant messaging" e "feed" commerciali utilizzati da aziende specializzate in "threat intelligence», al fine di tracciare il profilo di persone che hanno come obiettivo quello di compiere delitti e di seguirne l'evoluzione del tempo. In questa ricerca della minaccia si può anche risalire indietro negli anni, analizzando ingenti moli di dati estratte dal passato».

Anche se simili strumenti investigativi sono in dotazione alle forze dell'ordine già da molto tempo, non ne sono mai stati chiariti fino in fondo i limiti, le modalità d'uso, le regole d'ingaggio e, in particolare, la legittimità secondo le leggi vigenti. Oltretutto, questi software-spia stanno per essere impiegati anche nel settore privato dei sistemi di sorveglianza. E ciò agita comprensibilmente i sonni delle organizzazioni in difesa dei diritti umani e della libertà di espressione. Anche perché è tutt'altro da escludere che in questo modo le «impronte digitali» possano essere seguite e usate dalle persone sbagliate.

Secondo il giurista e accademico italiano Francesco Pizzetti, già presidente dell'Autorità garante per la privacy, «al momento sembra essenzialmente un servizio di analisi piuttosto che di vero spionaggio di dati. Sul caso, i garanti italiani faranno le opportune ispezioni per chiarire ogni dubbio. Ma a oggi non è evidente che il servizio muova dalla violazione di regole dell'appropriazione di informazioni personali».

Quando parliamo di social network, infatti, dobbiamo considerare che si tratta di fonti aperte: «Ritengo che il tema irrisolto sia proprio se la protezione dei dati individuali vada estesa o meno anche alle fonti aperte. Se simili software analizzano informazioni ricavate da tali fonti non si può parlare di illecito, perché se io mi espongo volontariamente alla visione pubblica, non posso poi appellarmi alla privacy. Ciò che fa il software è solo collegare e analizzare dati reperibili».

E se invece quel software analizzasse i comportamenti e «seguisse» sempre le persone? «Allora ci troveremmo di fronte all'intelligenza artificale, una materia che oggi non è ancora stata normata. Un *vulnus* da sanare quanto prima, di cruciale importanza per la serenità dei cittadini. Ed ecco perché l'Ue è in prima linea nel pretendere da subito nuovi regolamenti». La tecnologia, come sempre però, corre più della legislazione. ■