

La pigrizia dei sorvegliati

- Andrea Fabozzi, 21.11.2019

SCAFFALE. I nostri dati sono «frammenti di libertà» che disperdiamo in modo disattento

Che sia stato un magistrato della pubblica accusa la prima vittima del «trojan libero» la possibilità di utilizzare largamente il virus informatico che trasforma i telefoni in microspie è un curioso scherzo del destino. L'Associazione nazionale magistrati, di cui Luca Palamara il pm intercettato e indagato per corruzione è stato presidente, aveva infatti criticato le regole più stringenti sull'utilizzo dei virus informatici previste dalla riforma Orlando nel 2017. Grazie alla collaborazione del gestore telefonico, Palamara ha inconsapevolmente installato sul suo telefono un software che ha trasformato lo smartphone in un potente microfono ambulante, consentendo così l'ascolto e la registrazione di tutte le conversazioni alle quali era presente, in qualunque luogo. Nel nostro ordinamento le intercettazioni tra presenti, le cosiddette «ambientali», non possono essere effettuate nei luoghi di «privata dimora», con la sola eccezione che vi sia «fondato motivo» di ritenere che in quel luogo «si stia svolgendo lattività criminosa». La riforma Orlando, diventata indispensabile dopo una sentenza della Cassazione che aveva spalancato la porta ai trojan, ma subito sospesa dal governo gialloverde, ha introdotto due eccezioni alla regola generale della inviolabilità delle mura domestiche. Quando si procede per mafia o terrorismo si può utilizzare il captatore informatico anche all'interno delle «private dimore», vi sia o non vi sia il sospetto di crimini in corso. E l'ascolto può essere libero: per i sospetti terroristi o mafiosi non è necessario, come in tutti gli altri casi, che il giudice indichi i tempi e i luoghi di attivazione del microfono. Può restare sempre aperto. La legge «spazzacorrotti» ha esteso queste possibilità estreme anche ai «delitti dei pubblici ufficiali contro la pubblica amministrazione». Assimilando la corruzione alla mafia e al terrorismo.

MA ANCHE QUEL TANTO che è consentito dalle maglie larghe della legge bandiera dei 5 Stelle, impallidisce di fronte a quanto sta accadendo fuori dalla legge. Come nel caso di Exodus, un software spia sviluppato per le indagini di polizia giudiziaria ma finito come app su Google play store, per essere scaricato da circa un migliaio di inconsapevoli utenti Android. Persone del tutto estranee a qualsiasi indagine. Probabilmente si trattava di un modo per testare la funzionalità del trojan, capace di attivare la fotocamera del telefono, estrarre i log da tutte le app, copiare i dati delle foto e della rubrica oltre che registrare le telefonate e tutte le conversazioni a portata di microfono. Per conservare poi questa massa di informazioni non sui server protetti dell'autorità giudiziaria ma su quelli privati di Amazon collocati (almeno per il momento) fuori dal territorio nazionale.

Alla riflessione su questi potenti «agenti intrusori» dedica adesso convincenti pagine Antonello Soro, presidente uscente del Garante della privacy e autore di *Democrazia e Potere dei dati* (sottotitolo Libertà, algoritmi, umanesimo digitale, con la collaborazione di Federica Resta, Baldini+Castoldi, pp. 190, euro 18). Sulla scia delle osservazioni critiche avanzate dal garante alla riforma Orlando, Soro mette in luce i rischi di questi software spia «in grado di concentrare in un unico atto una pluralità di strumenti investigativi (perquisizioni del contenuto del dispositivo, pedinamenti con il sistema satellitare, intercettazioni di ogni tipo, acquisizioni di tabulati)». Tutte azioni, nota nella prefazione Giuliano Amato «che esigerebbero ciascuna una singola autorizzazione del giudice».

AL CENTRO del libro di Soro, però, non ci sono le indagini e le spie, piuttosto le abitudini della vita quotidiana. La nostra «assuefazione alla cessione indiscriminata e disattenta di quei frammenti di libertà che sono i dati». Le informazioni sensibili finiscono sui server di Amazon assai più frequentemente per libera scelta che in seguito a furto. E non solo perché facciamo acquisti online, per esempio sono sempre più diffusi gli assistenti vocali. A ben vedere oggetti molto simili a un trojan, con la differenza che vengono liberamente acquistati e sistemati al posto donore al centro

della casa. In teoria l'assistente vocale dovrebbe attivarsi solo a seguito di un comando (come «Ok Google», oppure «Alexa»). Ma evidentemente non è così, tant'è che, dopo un primo caso nel 2015 in Arkansas, sempre più frequentemente i giudici negli Stati Uniti stanno ordinando ad Amazon di consegnare le registrazioni delle conversazioni domestiche per risolvere casi di omicidi in cui è sospettato un familiare.

SPOSTANDO LA RIFLESSIONE sulla profilazione, e dunque sull'enorme massa di dati, sempre più raffinati, raccolta dai social e dalle piattaforme gratuite (dove la moneta sono gli utenti) sulla base di un modello sviluppato per la pubblicità e implementato per la propaganda politica, l'autore del libro arriva a porsi la domanda cruciale: come ci si difende dalla condizione servile in cui siamo velocemente precipitati? Partiti che eravamo dalle promesse di libertà della rete, siamo ormai di proprietà di pochi grandi gestori di piattaforme in competizione tra loro. Siamo costretti a cercare la libertà «negli interstizi» della rete. La risposta lascia la questione aperta. «La soglia di tutela dei dati», scrive Soro, va anticipata «alla fase della progettazione dei sistemi, inscrivendo così nelle stesse tecnologie le garanzie per gli utenti».

Ma il rischio è che in questo modo venga trasferito altro potere alle piattaforme. Non troppo diversamente da quello che accade quando si affida ai social il compito di distinguere le «fake news» dalla «verità». Una strada lungo la quale è arduo fissare dei confini. Un paio di anni fa, in Australia, Facebook ha annunciato (e sospeso per proteste) un programma per combattere il revenge porn che si basava sull'invio volontario di foto di nudo degli utenti. In modo da consentire al software di riconoscere e bloccare immagini intime delle stesse persone, se poste da altri.

© 2019 IL NUOVO MANIFESTO SOCIETÀ COOP. EDITRICE