Il tempo di sparire

A quasi due anni dal giorno in cui Edward Joseph Snowden, un collaboratore di Booz Allen Hamilton, rese pubblico il proprio archivio di materiale segreto sottratto alla National Security Agency (NSA), il comico della HBO John Oliver andò a Times Square, a New York, per porre delle domande a persone scelte a caso per un segmento del suo spettacolo su privacy e sorveglianza. Le domande erano chiare. Chi è Edward Snowden? Cosa ha fatto?[1]

Nelle interviste mandate in onda da Oliver, nessuno sembrava in grado di rispondere. Persino quando le persone dicevano di ricordare quel nome, non riuscivano a ricostruire che cosa esattamente avesse fatto Snowden (o perché). Dopo essere diventato un collaboratore della NSA, Edward Snowden copiò migliaia di documenti top secret e riservati che successivamente passò ai giornalisti in modo che potessero renderli pubblici in tutto il mondo. Oliver avrebbe potuto chiudere quel passaggio dello show sulla sorveglianza con una nota depressiva, e cioè dicendo che dopo mesi di copertura mediatica, nessuno negli Stati Uniti sembrava davvero interessato allo spionaggio interno messo in atto dal governo; invece, scelse un'altra via. Volò in Russia, dove Snowden oggi vive in esilio, per un'intervista faccia a faccia.[2]

La prima domanda che pose a Snowden, a Mosca, fu: cosa speravi di ottenere? Snowden rispose che voleva mostrare al mondo quello che l'NSA stava facendo: raccogliere dati di fatto su chiunque. Quando Oliver gli mostrò le interviste di Times Square, dove una persona dopo l'altra dimostrava di non sapere chi fosse Snowden, lui rispose: "Be', non possono essere tutti ben informati".

1 https://www.youtube.com/watch?v=XEVlyP4_11M&t=33s.

2 Snowden si trasferì ad Hong Kong prima di ricevere l'autorizzazione a vivere in Russia. Da allora ha fatto domanda per vivere in Brasile e in altre nazioni, e non ha escluso di tornare negli Stati Uniti, a patto di ricevere un giusto processo.

Perché non siamo ben informati sulle questioni che riguardano la privacy, questioni che Snowden e altri hanno sollevato? Perché sembra che non ci interessi che il governo intercetti le nostre telefonate, le nostre email e persino i nostri messaggi di testo? Forse perché la NSA, in generale, non ha un impatto diretto sulle vite della maggior parte di noi, o almeno non è evidente, non un'intrusione di cui possiamo davvero renderci conto.

Tuttavia, come anche Oliver scoprì quel giorno a Times Square, gli americani si preoccupano davvero della propria privacy, basta colpire nel segno. Oltre alle domande su Snowden, Oliver propose questioni generali sulla privacy, per esempio chiedendo alle persone cosa pensassero di un programma del governo, segreto ma del tutto inventato, che raccoglieva le fotografie di nudo inviate via Internet: anche in questo caso la risposta dei newyorkesi fu univoca, tutti erano ferventemente contrari. Una persona ammise persino di aver inviato una foto del genere di recente.

Tutti gli intervistati a Times Square erano d'accordo: le persone negli Stati Uniti dovrebbero poter condividere su Internet quello che vogliono, anche la foto di un pene, in modo privato. E questo era proprio quello che sosteneva Snowden.

Si scoprì poi che il programma governativo fittizio, quello che registrava le foto di nudo, era meno lontano dalla realtà di quanto si potesse immaginare. Come spiegò Snowden a Oliver nell'intervista, dato che aziende come Google hanno i loro server allocati fisicamente in ogni parte del mondo, persino un semplice messaggio (magari con allegato una foto di nudo) scambiato tra marito e moglie nella stessa città degli Stati Uniti potrebbe rimbalzare su un server all'estero. Dato che i dati lasciano gli Stati Uniti, anche se per un nano secondo, il Patrioct Act permette all'NSA di raccogliere e archiviare quel messaggio o quell'email (inclusa la foto indecente) perché tecnicamente proviene dall'estero. È questo il punto di Snowden: l'americano medio è preso in una rete a strascico progettata per fermare i terroristi stranieri dopo l'11 settembre, ma che ormai nella pratica serve a spiare chiunque.

Si sarebbe potuto pensare, date le continue notizie sulle violazioni dei dati e sulle azioni di sorveglianza da parte del governo, che fossimo molto più indignati. Si sarebbe potuto pensare, data la velocità con cui tutto questo si sta evolvendo in una manciata di anni, che ne fossimo colpiti, che decidessimo di marciare per le strade. In realtà, accade l'opposto. Molti di noi, persino tra i lettori di questo libro, oggi accettano almeno fino a un certo punto che tutto ciò che facciamo (le nostre telefonate, i nostri messaggi, le nostre email, i nostri social) possa essere visto da altri.

E questo è deludente.

Magari non hai infranto la legge, forse vivi quella che credi una vita normale, tranquilla, e sei convinto di passare inosservato tra la folla delle persone online. Ma fidati: non sei invisibile. Per lo meno, non ancora.

Mi piace la magia, e alcuni potrebbero sostenere che per fare hacking sia necessaria destrezza di mano: sono famosi i trucchi di magia che consistono nel rendere invisibili degli oggetti. Il segreto, però, è sempre lo stress, ossia che l'oggetto non viene fatto fisicamente sparire, né diventa davvero invisibile: l'oggetto resta celato, dietro un telo, in una manica, in una tasca, che noi lo vediamo o meno.

Lo stesso accade coi molti dati personali su ciascuno di noi che oggi vengono raccolti e archiviati, spesso senza che ce ne accorgiamo. La maggior parte di noi semplicemente non sa quanto sia facile per gli altri vedere quei dati né dove si possa cercarli. E poiché noi non vediamo queste informazioni, potremmo credere che siano invisibili per i nostri o le nostre ex, i nostri genitori, le nostre scuole, i nostri superiori sul lavoro, o persino per i nostri governi.

Il problema è che, se sai dove guardare, tutte queste informazioni sono disponibili praticamente a chiunque.

Quando parlo a un pubblico – non importa quanto sia numeroso – spesso qualcuno mi contesta questo fatto. Dopo un evento di questo tipo sono stato sfidato da una giornalista molto scettica.

Mi ricordo che eravamo seduti al tavolo del bar di un hotel in una grande città degli Stati Uniti quando lei sostenne di non essere mai stata vittima di una violazione dei dati. Dato che era giovane, disse di avere poche proprietà a suo nome, e quindi pochi dati registrati; non metteva mai dettagli personali in nessuna delle sue storie o sui social media – li manteneva professionali. Si considerava invisibile, così le chiesi il permesso di trovare online il suo numero di Social Security (una sorta di equivalente del codice fiscale italiano, *ndt*) e altri dati personali: riluttante, me lo concesse.

Con lei seduta al mio fianco, accedetti a un sito riservato agli investigatori privati, dove posso entrare grazie al mio lavoro di indagine sugli hackeraggi nel mondo. Già sapevo il suo nome, così le chiesi dove abitasse, un'informazione che, altrimenti, avrei potuto comunque trovare su un altro sito.

Un paio di minuti dopo conoscevo il numero di Social Security, la sua città di nascita e persino il cognome da nubile di sua madre. Sapevo anche tutti i luoghi da cui avesse mai telefonato a casa, e tutti i numeri di telefono che aveva mai usato. Fissando lo schermo, con uno sguardo sorpreso, mi confermò che tutte le informazioni erano più o meno corrette.

Il sito che usai è riservato a società o individui verificati e approvati. Si paga una piccola somma mensile, e un costo aggiuntivo per ciascuna informazione ricavata, e di tanto in tanto vengo interrogato per verificare che ci fosse una ragione legittima per condurre una particolare ricerca.

Tuttavia simili informazioni possono essere trovate, su chiunque, a prezzi molto ridotti. E tutto è perfettamente legale.

Hai mai riempito un questionario online, inviato informazioni a una scuola o a un'organizzazione che le ha messe in rete, o hai una questione legale su cui hai postato in Internet? Se è così, hai volontariamente concesso dei dati a terze parti che possono fare di quelle informazioni ciò che vogliono. È possibile che alcuni – se non tutti – quei dati siano ora online e disponibili per aziende che fanno soldi raccogliendo ogni bit di informazioni personali da Internet. La Privacy Rights Clearinghouse ha una lista di oltre 130 aziende che raccolgono informazioni personali (che siano accurate o meno) su di te.

Poi, inoltre, ci sono i dati che non metti volontariamente online ma che tuttavia vengono ricavati da aziende e governi – informazioni su a chi mandiamo email, su chi chiamiamo e a chi mandiamo messaggi; su cosa cerchiamo online, su cosa compriamo, che sia in un negozio fisico in rete; e su dove andiamo, a piedi o in auto. Il volume dei dati raccolti su ciascuno di noi cresce esponenzialmente giorno dopo giorno.

Potresti pensare di non dovertene preoccupare. Fidati: dovresti. Spero che entro la fine di questo libro sarai sia ben informato, sia che avrai abbastanza nozioni per fare qualcosa.

Il fatto è che viviamo in un'illusione di privacy, e probabilmente è così da decenni.

A un certo punto possiamo sentirci poco a nostro agio rispetto a quanto accesso alla nostra vita privata abbiano i nostri governi, i datori di lavoro, i nostri superiori, gli insegnanti o i genitori, solo che, poiché quell'accesso è stato guadagnato gradualmente, dato che abbiamo accolto ogni piccola comodità digitale senza resistere al suo impatto sulla nostra privacy, è diventato sempre più difficile mandare all'indietro le lancette dell'orologio. E poi, chi tra noi vorrebbe rinunciare ai suoi giocattolini?

Il problema di vivere in uno stato di sorveglianza digitale non è tanto il fatto che i dati vengano raccolti (possiamo farci poco) ma è *cosa viene fatto con i dati* una volta raccolti.

Immagina cosa farebbe un pubblico ministero troppo zelante con il grosso dossier di dati grezzi disponibili su di te, che forse gli permettono di scavare nel passato per alcuni anni. I dati di oggi, spesso

raccolti fuori contesto, vivranno per sempre. Persino Stephen Breyer, giudice della Corte Suprema degli Stati Uniti, concorda sul fatto che sia "difficile per chiunque sapere, in anticipo, quando un particolare insieme di informazioni possa poi apparire (a un giudice) rilevante per una certa investigazione". In altre parole, una tua foto da ubriaco che qualcuno ha postato su Facebook potrebbe essere l'ultimo dei tuoi problemi.

Potresti pensare di non avere nulla da nascondere, ma ne sei sicuro? In un editoriale ben argomentato su *Wired*, Moxie Marlinspike, stimato ricercatore nel campo della sicurezza, rileva come una cosa semplice come il possedere una piccola aragosta sia attualmente, negli Stati Uniti, un crimine federale.[3] "Non importa se l'hai comprata al supermercato, se qualcuno te l'ha data, se è viva o morta, se l'hai trovata dopo che è morta per cause naturali o persino se l'hai uccisa per autodifesa: puoi finire in prigione per quell'aragosta"[4]. Il punto è che esistono una serie di piccole leggi inapplicate che potresti infrangere senza saperlo, solo che ora esiste una traccia di dati che ne è la prova, ed è disponibile per chiunque voglia seguirla, sono sufficienti pochi semplici clic.

La privacy è complessa: non è un vestito a taglia unica. Abbiamo tutti ragioni diverse per condividere liberamente con estranei alcune informazioni su di noi e tenere privati altri aspetti delle nostre vite. Forse è solo che non vuoi che il tuo o la tua partner leggano il tuo diario personale; forse non vuoi che il tuo datore di lavoro sappia della tua vita privata; o, forse, hai davvero paura che il governo ti stia spiando.

Si tratta di situazioni molto diverse, e pertanto nessuno dei suggerimenti che saranno offerti andrà bene per tutte. Dato che abbiamo tutti atteggiamenti complessi e quindi molto differenti riguardo alla privacy, ti guiderò attraverso la questione più importante – ciò che oggi accade nella raccolta surrettizia di dati – e starà a te decidere cosa è importante per te.

Spero che questo libro ti metterà a conoscenza di alcuni modi per mantenere uno spazio privato nel mondo digitale e ti offrirà soluzioni che potresti (o meno) scegliere di adottare. Dato che la privacy è una questione personale, anche i gradi di invisibilità variano da individuo a individuo.

3 https://www.law.cornell.edu/uscode/text/16/3372.

4 http://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/.

In questo libro, partiremo dall'assunto che ciascuno di noi è osservato, a casa e nel mondo esterno – quando cammina per strada, siede a un caffè o guida in autostrada. Il tuo computer, il tuo telefono, la tua auto, l'allarme della tua casa e persino il tuo frigorifero sono tutti punti d'accesso potenziali alla tua vita privata.

La buona notizia è che, oltre a spaventarti, ti mostrerò cosa fare contro la mancanza di privacy, cioè nella situazione che è ormai la norma.

In questo libro imparerai come:

- crittografare e inviare una email sicura;
- proteggere i tuoi dati con una buona gestione delle password;
- nascondere il tuo vero indirizzo IP ai siti che visiti;
- evitare che il tuo computer venga tracciato;
- difendere il tuo anonimato
- e molto altro.

Preparati, quindi, a padroneggiare l'arte dell'invisibilità.