

Il reportage. Le ultime rivelazioni di Assange scuotono la culla della tecnologia Usa: l'idea che la Cia sia in grado di violare i prodotti nati qui può creare danni enormi agli affari

WikiLeaks, così la Silicon Valley si scopre vulnerabile

“Il nostro mondo è a rischio”

I rapporti fra il governo e le imprese più potenti del pianeta sono da tempo ambigui

Alla base di tutto c'è lo scontro fra la ragion di Stato e le ragioni del capitalismo tecnologico

DAL NOSTRO INVIATO

FEDERICO RAMPINI

SAN FRANCISCO. La Silicon Valley è sotto shock per la nuova ondata di rivelazioni WikiLeaks. O almeno, vuole farci credere di esserlo. I giganti californiani della tecnologia digitale in queste ore ricordano quell'intervento di Donald Trump, da “elefante nella cristalleria”. Appena pochi mesi fa, alla fine della campagna elettorale, affrontò il tema della cyber-sicurezza con queste parole: «Da presidente radunerò tutti i grandi imprenditori della Silicon Valley e loro mi aiuteranno a sconfiggere i terroristi, a rendere più sicura l'America». In realtà qualcuno l'aveva fatto prima di lui: Barack Obama.

È molto ambigua la storia dei rapporti – talora conflittuali, talvolta incestuosi – tra i due grandi poteri: lo Stato e le imprese più potenti del mondo che si concentrano quasi tutte in quest'angolo della West Coast. Perciò dopo l'ultima fuga di notizie – sui nuovi metodi di hackeraggio della Cia che può spiarci con ogni gadget, “l'Internet delle cose”, dallo smartphone al televisore – le reazioni seguono un copione preciso. Massima riservatezza dei top manager, nell'attesa di saperne di più. Preoccupazione per l'immagine e la credibilità dell'industria hi-tech sui mercati mondiali. Incer-

tezza e interrogativi sulle reali intenzioni del nuovo presidente, in questo terreno minato che è l'incontro-scontro fra la ragion di Stato e le ragioni del capitalismo tecnologico.

Il conflitto di fondo che oppone questi due grandi poteri americani, è più esplosivo che mai alla luce delle ultime rivelazioni di WikiLeaks. Gli esperti aziendali che sotto garanzia di anonimato accettano di parlare, a Cupertino e Palo Alto e Mountain View, lo sintetizzano così. Primo punto: la Silicon Valley dove hanno sede Apple, Google, Facebook, Intel (e le propaggini come la Microsoft di Seattle, geograficamente più settentrionale) prospera perché ha conquistato da decenni l'egemonia sul mercato globale. Secondo punto: la fiducia sulla sicurezza dei suoi prodotti – gadget come gli iPhone o sistemi operativi come Windows, Android – è parte integrante del suo successo. Terzo punto: se il resto del mondo si convince che in realtà la tecnologia americana è un cavallo di Troia per lo spionaggio, o comunque che i suoi sistemi operativi sono dei “colabrodo” facilmente violati dalla Cia, per il capitalismo digitale sono guai (anche se non è chiaro che ci siano alternative: la Cia ha violato anche la coreana Samsung).

In quei tre punti c'è lo stato delle cose nella narrazione della Silicon Valley. Ma dice tutto? Quante sono le zone d'ombra inconfessate, gli episodi di cooperazione tra i giganti digitali e il governo di Washington, nella fattispecie le sue agenzie d'intelligence? Proprio qui nella Silicon Valley opera da quasi un ventennio un ramo della Cia che fa...

venture capital, cioè investe capitale di rischio nelle start-up. Per non parlare del Darpa, l'agenzia di ricerca del Pentagono, che fu all'origine dello sviluppo di Internet. Dietro gli allarmi e le proteste indignate, che cosa ci nasconde la Silicon Valley?

Un episodio-chiave avvenne un anno fa. Apple rifiutò la richiesta dell'Fbi – convalidata da un giudice – di decrittare e violare l'iPhone usato da uno dei terroristi di San Bernardino (strage del 2 dicembre 2015, in California: 14 morti). Il chief executive Tim Cook invocò la necessità vitale di «proteggere i clienti, di fronte a una richiesta del governo di distruggere decenni di progressi nella sicurezza dei nostri prodotti». Il conflitto legale minacciava di arrivare alla Corte suprema. Spaccò il mondo digitale, con Bill Gates schierato dalla parte di Obama e della magistratura. Alla fine l'Fbi riuscì a decrittare l'iPhone per conto suo, si dice con l'aiuto di un'impresa israeliana. Ma col tempo venne fuori un retroscena più ambiguo: per un “caso San Bernardino” in cui Apple aveva tenuto duro, ce n'erano tanti altri in cui le aziende digitali cooperano con la giustizia, zitte zitte.

Sullo sfondo c'è una lunga storia d'amore fra gli apparati di sicurezza degli Stati Uniti, il complesso militar-poliziesco-industriale, e il business hi-tech. E' dall'11 settembre 2001 che la comunità dell'intelligence ha imboccato una deriva verso il feticismo tecnologico, ab-



bracciando Big Data. L'idea è che lo stato di avanzamento del progresso tecnologico ha moltiplicato a dismisura la capacità di raccolta dati. In un delirio di onnipotenza, solo perché la tecnologia "consente" di farlo, le agenzie d'intelligence sono convinte che "devono" farlo. Tutto ciò che abbiamo appreso nelle puntate precedenti da WikiLeaks, conferma l'enorme rete globale da Grande Fratello costruita

dalla National Security Agency nel suo innamoramento per Big Data. Proprio la dimensione sconfinata di questa raccolta fa sì che bisogna parlare di meta-dati: per esempio nella stragrande maggioranza dei casi non s'intercettano i contenuti delle telefonate ma solo i numeri chiamati, che possono svelare segnali su reti di contatti. Ma è possibile farne un uso davvero efficace? Non ci sono risorse umane adeguate per interpretare masse di dati così sterminate; finora anche l'intelligenza artificiale non ha dato risultati soddisfacenti: dall'attentato alla maratona di Boston, alle stragi di San Bernardino e Orlando, gli ultimi attacchi terroristici sono avvenuti nell'era di Big Data, in barba alla formidabile potenza tecnologica dello spionaggio.

© RIPRODUZIONE RISERVATA

IPUNTI

INTELLIGENCE E BIG DATA

Dopo l'attacco alle Torri gemelle l'intelligence Usa ha puntato tutto sui Big Data, che ha portato le agenzie a raccogliere una immensa quantità di dati

CONTROLLI DI MASSA

Nel 2013 Snowden svelò l'esistenza programmi di sorveglianza di massa della NSA: come Prism capace di intercettare il traffico internet di milioni di persone

SAN BERNARDINO

Dopo la strage di San Bernardino avvenuta il 2 dicembre 2015 la Apple ha rifiutato di sbloccare l'iPhone dei terroristi. Tim Cook parlò della necessità di "difendere la privacy dei clienti"

LE IMPRESE

L'Fbi riuscì a decrittare l'iPhone di San Bernardino con l'aiuto di una azienda israeliana: ma si sa di altre aziende digitali che hanno collaborato sottobanco con l'Fbi