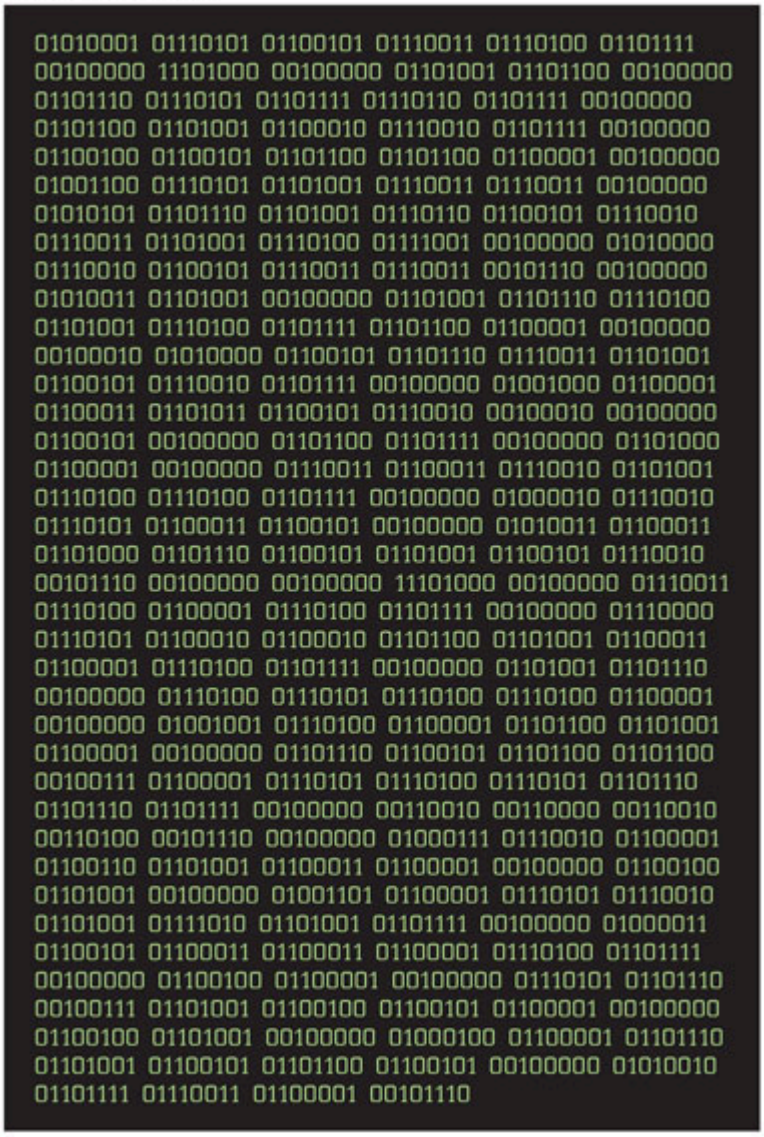
BRUCE SCHNEIER

LA MENTE DELL'HACKER

TROVARE LA FALLA PER MIGLIORARE IL SISTEMA

LUISS

BRUCE SCHNEIER



LA MENTE DELL'HACKER

LUISS

TROVARE LA FALLA PER MIGLIORARE IL SISTEMA

PENSIERO LIBERO

Bruce Schneier

La mente dell’hacker

Trovare la falla per migliorare il sistema

Traduzione di Paolo Bassotti

LUISS
University Press

Questa edizione è stata originariamente pubblicata negli Stati Uniti d'America
da W.W. Norton & Company con il titolo
A hacker's mind. How the powerful bend society's rules, and how to bend them back

ISBN 979-12-5596-179-6

Traduzione di Paolo Bassotti

Luiss University Press – LuissX srl
Viale Romania 32
00197 Roma
Tel. 06 85225486
E-mail universitypress@luiss.it
www.luissuniversitypress.it

Editing Tralerighe
Impaginazione Livia Pierini
Progetto grafico Maurizio Ceccato | IFIX

Prima edizione ottobre 2024

La traduzione dell'opera è stata realizzata grazie al contributo del SEPS
SEGRETARIATO EUROPEO PER LE PUBBLICAZIONI SCIENTIFICHE

Via Val d’Aposa 7 – 40123 Bologna
seps@seps.it – www.seps.it

Indice

Introduzione

They say that water, it never runs uphill.
It never has, and it never will.
But if you get enough money involved,
There's bound to be a loophole in the natural law.
And water, is gonna flow uphill.
(Jim Fitting, "Water Never Runs Uphill," *Session Americana*)[1]

Dal 1956, la Uncle Milton Industries produce formicai per bambini. Questi formicai sono costituiti da due pannelli di plastica trasparente distanti circa sei millimetri, sigillati ai lati ma con un coperchio in alto. Ci metti della sabbia e le formiche e osservi come queste scavano i tunnel.

Le formiche non sono incluse nella confezione. Difficilmente sopravviverebbero sullo scaffale di un negozio, e probabilmente è vietato da qualche legge per la tutela dell'infanzia. Nella scatola c'è invece una cartolina da inviare all'azienda, sulla quale si può scrivere il proprio indirizzo per ricevere per posta un tubo pieno di formiche. Molti si stupiscono che un'azienda possa spedire un tubo di formiche ai clienti. Il mio primo pensiero, quando vidi quella cartolina, fu: "Assurdo, posso fargli spedire un tubo di formiche a chiunque io voglia".

Chi, come me, si occupa di sicurezza tecnologica, guarda il mondo in modo diverso. Quasi tutti, di fronte a un sistema, si chiedono come funzioni. Gli esperti di sicurezza tecnologica invece si chiedono come sia possibile non farlo funzionare: come quel malfunzionamento possa costringerlo a fare qualcosa che non dovrebbe fare, e come sfruttare la cosa a proprio vantaggio.

Ecco che cos'è un *hack*: un'attività consentita da un sistema che sovverte gli scopi o gli intenti del sistema. Proprio come usare il sistema della Uncle Milton per inviare tubi di formiche a chi non saprebbe che farsene.

Insegno cybersicurezza alla Harvard Kennedy School. Alla fine

della prima lezione, dico agli studenti che la volta successiva terrò un test a sorpresa: dovranno scrivere a memoria i primi cento decimali del pi greco.[2] "So bene che non potrete imparare cento numeri a caso in due giorni", spiego loro. "Pertanto mi aspetto che proverete a fregarmi. Non fatevi beccare".

Due giorni dopo l'aula è in pieno fermento. La maggior parte degli studenti non si inventa niente di nuovo. Magari hanno nascosto da qualche parte un biglietto con le cifre decimali. Oppure hanno registrato un vocale nel quale leggono quei numeri, e cercano di nascondere i loro auricolari. Altri si dimostrano invece incredibilmente creativi. Una volta uno studente ha scritto le cifre con un inchiostro invisibile e ha indossato occhiali speciali per poterle vedere. Un altro le ha scritte in cinese. Un altro ancora le ha associate a un codice fatto di perline colorate, che ha indossato in una collana. Un quarto ha memorizzato le prime e le ultime e in mezzo ha scritto numeri a caso, presupponendo che non sarei stato troppo puntiglioso nel correggere il test.

Il mio preferito risale a qualche anno fa. Seppur molto lentamente, Jan ha scritto le cifre giuste una dopo l'altra. Ha terminato il compito per ultimo. Lo fissavo, senza capire che cosa stesse facendo. Gli altri studenti lo osservavano basiti. Mi chiedevo: "Starà mica calcolando a mente questa serie infinita?". No. Aveva programmato il telefono che aveva in tasca per comunicargli le cifre in alfabeto Morse tramite le vibrazioni.

Lo scopo dell'esercizio non era certo quello di trasformare i miei studenti in imbroglioni. Spiego sempre che a Harvard se si bara, si viene espulsi. Lo scopo è far capire loro che chi si occupa di politiche pubbliche in materia di cybersicurezza deve aspettarsi di essere ingannato. Deve coltivare la propria mente hacker.

Questo libro racconta la storia dell'*hacking*, una storia molto diversa da quella rappresentata dal cinema, dalla tv e dai giornali. Non è la solita storia che trovate nei libri su come hackerare i computer o su come difendersi dagli hacker. È una storia molto più endemica, intrinsecamente umana, e molto più antica dell'invenzione del computer. È una storia di soldi e potere.

I bambini sono hacker per natura. Lo fanno per istinto, perché non

capiscono le regole e il loro scopo (lo stesso vale per i sistemi di intelligenza artificiale, come vedremo alla fine del libro). E i ricchi si comportano proprio come loro. A differenza dei bambini, comprendono norme e contesti. Ma esattamente come loro, spesso i ricchi non accettano che le regole valgano anche per loro, o comunque ritengono che il proprio interesse debba avere la precedenza. Per questo non fanno altro che hackerare ogni sorta di sistema.

Nella storia che vi racconterò, l'hacking non è semplicemente qualcosa che i teenager annoiati o i governi nemici fanno ai sistemi informatici, e nemmeno una scappatoia per gli studenti furbacchioni che non vogliono studiare. Non è una pratica antagonista controculturale di chi si vuole opporre al potere. È molto più probabile che un hacker sia al servizio di un *hedge fund*, col compito di aggirare le normative finanziare per spillare qualche soldo extra al sistema. Che lavori per una grande azienda. O per un politico. Per le grandi lobby, l'hacking è fondamentale. Inoltre è grazie all'hacking che i social media ci trattengono sulle loro piattaforme.

Parlerò dell'hacking come prerogativa di ricchi e potenti, spesso usata per rafforzare strutture di potere preesistenti.

Pensiamo ad esempio a Peter Thiel. Il Roth Ira è un fondo pensionistico approvato da una legge del 1997, e pensato per gli investitori della classe media, con limiti imposti al reddito dell'investitore e alla cifra che si può investire. Il miliardario Peter Thiel, uno dei fondatori di PayPal, ha però trovato un hack.[3] È riuscito a usare un investimento da 2000 dollari per acquistare 1,7 milioni di quote dell'azienda al prezzo di 0,001 dollari a quota, trasformandole in 5 miliardi di dollari, il tutto esentasse in eterno.

Se spesso abbiamo l'impressione che il governo non riesca a proteggerci dagli interessi delle grandi aziende o dei super-miliardari, è per via dell'hacking. È uno dei motivi della nostra sensazione di impotenza al cospetto dell'autorità pubblica. L'hacking è il sistema usato da ricchi e potenti per sovvertire le norme e diventare ancora più ricchi e potenti. Si danno da fare per trovare nuovi hack, e poi li difendono per poter continuare a sfruttarli. Il punto non è tanto che ricchi e potenti sono più bravi nell'arte di

hackerare, ma che è più difficile che vengano puniti per averlo fatto. Anzi, spesso i loro hack diventano parte integrante dei meccanismi sociali. Per porvi rimedio servono cambiamenti istituzionali: difficile a farsi, visto che è proprio chi comanda a truccare la partita.

Non c'è sistema che non possa essere hackerato. Molti sistemi attualmente vengono hackerati. E le cose non fanno che peggiorare. Se non impariamo a controllare tale processo, i nostri sistemi economici, politici e sociali sono destinati al fallimento: non serviranno più al proprio scopo e le persone non si fideranno più di loro. È un processo già in corso. Come vi fa sentire sapere che Peter Thiel non ha pagato 1 miliardo di dollari di tasse sugli utili capitali e se l'è cavata?

Come dimostrerò, l'hacking non è però sempre distruttivo. Se usato in modo giusto, può consentire ai sistemi di evolversi e migliorare. È così che la società progredisce. O meglio, è così che le persone fanno progredire una società senza fare tabula rasa del passato. L'hacking può essere una forza positiva. Il trucco è capire come incoraggiare gli hack buoni e fermare i cattivi, e come distinguerli tra loro.

L'hacking diventerà sempre più dirompente con la maggiore implementazione dell'intelligenza artificiale (AI) e dei sistemi autonomi.

Si tratta di sistemi informatici, e in quanto tali saranno inevitabilmente hackerati. Già stanno influenzando i sistemi sociali – i sistemi di AI prendono già decisioni su prestiti, assunzioni, libertà vigilata dei detenuti – e avranno un'influenza sempre maggiore sui nostri sistemi politici ed economici. Cosa ancor più rilevante, i processi di apprendimento automatico alla base dell'AI moderna porteranno i computer stessi a mettere in atto vari tipi di hack. Presto i sistemi di AI scopriranno nuovi hack, e tutto cambierà. Fino a oggi, l'hacking era stato un contesto umano, con hacker umani e hack soggetti ai limiti degli esseri umani. Questi limiti stanno per essere superati. La AI non hackererà solo i nostri computer, ma anche i nostri governi, i nostri mercati, o perfino le nostre menti. Le AI hackereranno i sistemi con velocità e abilità impensabili per gli hacker umani. Mentre leggerete il libro, non dimenticatevi mai del concetto di hacker AI, che ritroveremo nelle ultime pagine.

Proprio questo concetto rende il mio libro estremamente urgente: oggi più che mai dobbiamo riconoscere gli hack e difenderci da loro. E gli esperti di sicurezza tecnologica possono darci una mano.

Ricordo di aver sentito – mi piacerebbe rammentare dove[4] – un aforisma sull'analfabetismo matematico: "Certo, la matematica non può risolvere tutti i problemi del mondo, ma i problemi del mondo sarebbero più facili da risolvere se tutti conoscessero un po' di matematica". Penso che lo stesso valga per la sicurezza. Una mentalità orientata alla sicurezza, o un pensiero hacker, non risolveranno tutti i problemi del mondo. Ma i problemi del mondo sarebbero più facili da risolvere se tutti ne sapessero un po' di più sul tema della sicurezza. Siete pronti?

1. “Dicono che l’acqua non vada mai in salita. / Una cosa del genere non è mai accaduta. / Ma è solo questione di soldi: / una scappatoia alla legge di natura la si può sempre trovare. / E l’acqua se ne andrà in salita.” Massimo Materni (1° maggio 2021), “Water never runs uphill/Session Americana”, www.youtube.com/watch?v=0Pe9XdFr_Eo.
2. Non ho inventato io questo esercizio. Gregory Conti e James Caroland (luglio-agosto 2011), “Embracing the Kobayashi Maru: Why you should teach your students to cheat”, *IEEE Security & Privacy* n. 9, www.computer.org/csdl/magazine/sp/2011/04/msp2011040048/13rRUwbs1Z3.
3. Justin Elliott, Patricia Callahan e James Bandler (24 giugno 2021), “Lord of the Roths: How tech mogul Peter Thiel turned a retirement account for the middle class into a $5 billion tax-free piggy bank”, *ProPublica*, www.propublica.org/article/lord-of-the-roths-how-tech-mogul-peter-thiel-turned-a-retirement-account-for-the-middle-class-into-a-5-billion-dollar-tax-free-piggy-bank.
4. Non riesco a ricordare dove: se qualcuno se lo ricorda, per cortesia mi mandi una email.

PARTE PRIMA
LE BASI DELL'HACKING

CAPITOLO 1

Che cos'è l'hacking?

"Hack", "hacking", "hacker", parole cariche di significati e sottintesi.[1] Non ne darò una definizione precisa o canonica. Mi va bene così. Il mio scopo è dimostrare che una mente hacker aiuta a comprendere una vasta gamma di sistemi, come collassano e come possono invece diventare più resilienti.

> Definizione: *Hack*/hak/ (sostantivo):
> 1. Modalità ingegnosa e imprevista per lo sfruttamento di un sistema, in grado di (a) sovvertirne regole e norme (b) a discapito di un soggetto influenzato dal sistema stesso.
> 2. Una cosa consentita da un sistema ma non prevista o voluta da chi l'ha progettato.[2]

Hackerare non equivale a imbrogliare. Un hack può essere un imbroglio, ma è più probabile che non lo sia. Quando qualcuno imbroglia, va contro le regole: fa quello che un sistema proibisce esplicitamente. Inserire in un sito il nome e la password di un'altra persona senza averne il permesso, non dichiarare tutti i propri redditi al fisco o copiare le risposte di un'altra persona a un test sono modi di imbrogliare. Nessuna di queste cose si può definire hacking.

Un hack inoltre non è un miglioramento, un progresso o un'innovazione. Allenarsi a tennis e vincere più partite vuol dire migliorare. Le nuove caratteristiche di un iPhone della Apple sono progressi. Trovare un nuovo modo per usare un foglio di calcolo può essere un'innovazione. In certi casi, un hack può essere un'innovazione o un progresso – ad esempio hackerare il proprio iPhone per fargli fare cose che la Apple non vuole – ma non sempre.

L'hacking prende di mira un sistema e lo sfida con le sue stesse armi, senza però distruggerlo. Se uno ti sfonda il finestrino della macchina e la accende collegando i cavi, non è un hack. Se invece capisce come ingannare il sistema di apertura dell'auto per

convincerlo ad aprirgli la portiera e a mettere in moto la macchina, ecco un hack.

Soffermiamoci sulla differenza. L'hacker non si limita a dimostrarsi più astuto della sua vittima. Scova una falla nelle regole del sistema. Fa qualcosa che non dovrebbe essere possibile, ma invece lo è. E pertanto supera in astuzia chi ha progettato il sistema.

L'hacking sovverte lo scopo di un sistema modificandone le regole o le norme. "Si prende gioco del sistema". Si pone a metà tra imbroglio e innovazione.

"Hack" è una parola soggettiva. La tipica cosa che "riconosciamo quando ce l'abbiamo davanti". Ci sono cose che senza dubbio sono hack, così come altre indubbiamente non lo sono. Altre ancora si posizionano in una zona grigia intermedia. La lettura veloce: non è un hack. Nascondere un microdot nel punto a capo di un testo stampato: è un hack, senza dubbio. I "bignami": forse, non saprei.

Gli hack sono intelligenti. Un hack suscita ammirazione, seppur con riluttanza (spesso accompagnata da una giusta rabbia), e ti fa dire "avrei voluto pensarci io", anche se in verità non l'avresti fatto mai. E questo vale anche quando un hack è opera di persone cattive, o perfino di assassini. All'inizio del mio libro del 2003 *Beyond Fear*,[3] mi sono dilungato a spiegare perché gli attacchi dell'11 settembre fossero "fenomenali". I terroristi hanno infranto le regole tacite dei dirottamenti aerei. Prima, con un dirottamento si costringeva il pilota di un aereo ad andare da qualche parte, spesso avanzando richieste politiche, negoziando col governo e la polizia, e arrivando in genere a una soluzione pacifica. Quanto fatto dai terroristi l'11 settembre, seppur orribile e crudele, mi è sembrato un hack ingegnoso. Hanno utilizzato armi consentite dalla sicurezza aeroportuale, hanno trasformato aerei di linea in missili, e hanno riscritto unilateralmente le norme del terrorismo aereo.

Gli hacker ci costringono a guardare con nuovi occhi i nostri sistemi. Ci mostrano quel che presupponiamo o diamo per scontato, spesso mettendo in imbarazzo chi ha il potere, e a volte costringendoci a pagare un prezzo terribile.

Terrorismo a parte, alla gente gli hack piacciono proprio perché sono intelligenti. MacGyver era un hacker. I film sulle rapine e sulle

evasioni dal carcere sono pieni di hack geniali: *Rififi*, *La grande fuga*, *Papillon*, *Mission: Impossible*, *Un colpo all'italiana*, *Ocean's 11*, *12*, *13* e *8*.

Gli hack sono sorprendenti. Ci fanno esclamare "ma si può fare?" o "non immaginavo che fosse possibile!". Che cosa sia o meno un hack cambia anche col tempo. Le "cose risapute" cambiano. Un hack, una volta messo in atto, verrà vietato o consentito, per questo alcune cose che prima erano hack ora non lo sono più. Un tempo bisognava hackerare il proprio smartphone per trasformarlo in un hotspot per il wi-fi, mentre ora la modalità hotspot è inclusa nei sistemi iOS e Android. Un tempo nascondere una lima in una torta inviata in prigione poteva essere considerato un hack, ma oggi è un cliché da cinema che qualunque secondino conosce.

Nel 2019, qualcuno usò un drone per fare arrivare un cellulare e un po' di marijuana all'interno di un carcere dell'Ohio.[4] All'epoca l'avrei definito un hack. Oggi fare arrivare un drone in una prigione è espressamente vietato in alcuni Stati, e non lo giudicherei più un hack. Di recente ho letto un articolo su qualcuno che ha fatto entrare merce proibita in un penitenziario usando una lenza da pesca,[5] e un altro su alcuni carcerati dello Sri Lanka che si sono serviti di un gatto per farsi inviare droghe e Sim telefoniche (il gatto è stato intercettato, ma poi è riuscito a scappare).[6] Sono due esempi di hack, senza nessun dubbio.

Spesso gli hack sono legali. Seguono le disposizioni normative senza rispettarne lo spirito, e pertanto divengono illegali solo in presenza di una legge onnicomprensiva che li vieta esplicitamente. In Italia si usa il termine "furbizia", riferendosi all'ingegno necessario per aggirare burocrazia e leggi scomode. Il termine *hindi jugaad*, che mette l'accento su intelligenza e intraprendenza, ha un significato simile. Il suo equivalente nel portoghese brasiliano è la parola GAMBIARRA.

A volte gli hack hanno un aspetto morale. C'è chi presuppone che solo perché un comportamento o un'attività sono legali debbano essere anche morali, ma ovviamente le cose non sono così semplici. Così come esistono leggi immorali, esistono anche crimini morali. In questo libro parleremo soprattutto di hack tecnicamente legali ma

che vanno contro lo spirito delle leggi (e i sistemi giuridici sono solo uno dei vari tipi di sistemi che possono essere hackerati).

La parola “hack”, nata nel 1955 nel Tech Model Railroad Club del Mit,[7] ben presto venne usata anche nell’ambito informatico, all’epoca agli albori. Inizialmente descriveva un sistema di *problem solving* basato sull’innovazione o l’intraprendenza, senza evocare alcun aspetto illegale o antagonistico. Negli anni Ottanta, il termine “hacking” cominciò però a riferirsi soprattutto all’infrazione dei sistemi di sicurezza informatici. Non solo alla possibilità di far fare a un computer qualcosa di nuovo, ma a quella di fargli fare qualcosa che non avrebbe dovuto fare.

Per come la vedo io, dall’hacking dei computer a quello dei sistemi economici, politici e sociali il passo è breve. Tutti questi sistemi sono solo una serie di regole, o talora di norme. Sono vulnerabili proprio come i sistemi informatici. Non è una novità. Nel corso della storia abbiamo sempre hackerato i sistemi sociali.

1. Finn Brunton ha fatto una lista dei "significati fondamentali" di questo termine. Finn Brunton (2021), "Hacking", in Leah Lievrouw e Brian Loader (a cura di), *Routledge Handbook of Digital Media and Communication*, Routledge, pp. 75-86, http://finnb.net/writing/hacking.pdf.
2. Alla compianta hacker Jude Mihon (St. Jude) piaceva questa definizione: "Hackerare significa aggirare i limiti imposti in modo intelligente, che si tratti di limiti imposti dal governo, dalla nostra personalità o dalle leggi della fisica", Jude Mihon (1996), Hackers Conference, Santa Rosa, CA.
3. Bruce Schneier (2003), *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, Copernicus Books.
4. Lauren M. Johnson (26 settembre 2019), "A drone was caught on camera delivering contraband to an Ohio prison yard", *CNN*, www.cnn.com/2019/09/26/us/contraband-delivered-by-drone-trnd/index.html.
5. Selina Sykes (2 novembre 2015), "Drug dealer uses fishing rod to smuggle cocaine, alcohol and McDonald's into jail", *Express*, www.express.co.uk/news/uk/616494/Drug-dealer-used-fishing-rod-to-smuggle-cocaine-alcohol-and-McDonald-s-into-jail.
6. Redazione del Telegraph (3 agosto 2020), "Detained 'drug smuggler' cat escapes Sri Lanka prison", *Telegraph*, www.telegraph.co.uk/news/2020/08/03/detained-drug-smuggler-cat-escapes-sri-lanka-prison.
7. Jay London (6 aprile 2015), "Happy 60th birthday to the word 'hack,' *Slice of MIT*, https://alum.mit.edu/slice/happy-60th-birthday-word-hack.

CAPITOLO 2

L'hacking dei sistemi

Ogni sistema è hackerabile, ma può esserci d'aiuto confrontare i vari sistemi per scoprire come operano gli hack. Possiamo ad esempio riscontrare le differenze tra il codice che stabilisce le tasse da versare e un codice informatico. Quello delle tasse non è un software. Non viene eseguito da un computer. Ma lo si può comunque concepire come "codice" in senso informatico. È una serie di algoritmi che prende un input – le informazioni finanziarie relative a un determinato anno – e produce un output – l'ammontare di tasse dovuto. Si tratta di un codice incredibilmente complesso. Contiene un fantastiliardo di eccezioni e minuzie, magari non per tutti, ma di certo per ricchi e imprese. È fatto di norme statali, decreti amministrativi, decisioni giurisprudenziali e pareri legali. Comprende anche le leggi e i regolamenti che governano le aziende e i vari tipi di partnership. Difficile stimarne le dimensioni, perfino per gli esperti. La sola legislazione fiscale statunitense riempie circa 2600 pagine.[1] Le normative dell'Irs, l'Internal Revenue Service, e i decreti fiscali portano la cifra a circa 70mila pagine. La legislazione societaria e quella sulle partnership sono altrettanto complicate: tagliando la testa al toro, direi che nel complesso il codice che determina le tasse da pagare negli Stati Uniti arriva a 100mila pagine, o a 3 milioni di righe. Le righe di codice di Microsoft Windows 10 sono circa 50 milioni.[2] Paragonare le righe di un testo e un codice informatico è difficile, ma è comunque utile. In entrambi i casi, gran parte della complessità deriva dall'interazione tra le varie parti del codice.

In tutti i codici informatici ci sono bug. Si tratta di errori: di specificazione, di programmazione, errori avvenuti nel corso della creazione del software, errori banali come refusi o errori di sintassi. Nelle applicazioni di software moderne ci sono centinaia, se non migliaia di bug. Sono presenti in tutti i software che utilizziamo: nel

nostro telefono, in qualunque device IoT (Internet of Things, Internet delle cose) abbiamo in casa o al lavoro. Questo software in genere funziona alla perfezione, segno che i bug sono nascosti e spesso irrilevanti. Difficilmente si incappa in un bug nel corso di una normale operazione, eppure ci sono (lo stesso vale per gran parte delle normative fiscali, con le quali non veniamo mai in contatto).

Alcuni bug creano falle nella sicurezza. Mi riferisco a una cosa molto specifica: un aggressore può deliberatamente innescare il bug per ottenere un effetto non voluto dai progettisti e dai programmatori del codice. Nel linguaggio della sicurezza informatica, chiamiamo questi bug "vulnerabilità".

Anche nel codice che determina il sistema fiscale ci sono bug. Possono essere errori nella scrittura delle leggi fiscali: errori nelle parole che sono state soggette al voto del Congresso e alla firma del presidente. Possono essere errori nell'interpretazione del codice. Possono essere leggerezze a livello di scrittura della legge, oppure omissioni sfuggite per un motivo o per l'altro. Possono nascere dall'interazione di varie parti del codice.

Un esempio recente è quello del Tax Cuts and Jobs Act del 2017, stilato in gran fretta e in segreto, e approvato senza che i legislatori avessero il tempo di esaminarlo, o anche solo di correggerne l'ortografia. Alcune sue parti erano scritte a mano, ed è impensabile che chiunque abbia votato a favore o contro questa legge ne conoscesse i contenuti nel dettaglio. Un errore nel testo faceva rientrare i risarcimenti per la morte di un soldato nel reddito familiare. La conseguenza pratica è stata che le famiglie si sono viste recapitare senza preavviso cartelle esattoriali di 10.000 dollari o anche più.[3] Senz'altro si tratta di un bug. Non è però una vulnerabilità, perché nessuno può sfruttare questa cosa per pagare meno tasse.

Nel codice ci sono però bug che sono anche vulnerabilità. Ad esempio, c'era un trucchetto usato dalle aziende chiamato "Double Irish with a Dutch Sandwich" ("sandwich con doppia irlandese e un'olandese"), una vulnerabilità derivata dall'interazione delle normative fiscali di diversi Paesi, alla quale finalmente gli irlandesi hanno posto rimedio. Funzionava così: un'azienda statunitense

trasferisce i suoi asset a una sussidiaria irlandese.[4] La sussidiaria fa pagare all'azienda statunitense royalties enormi derivanti dalle vendite ai clienti americani. In tal modo il reddito, e quindi il carico fiscale, dell'azienda negli Stati Uniti viene ridotto notevolmente e le tasse vengono pagate in Irlanda dove l'imposizione sulle royalties è più bassa. Usando un *loophole*, una falla offerta dalla legge fiscale irlandese, l'azienda può girare i profitti a entità residenti in paradisi fiscali come Bermuda, Belize, Mauritius o Isole Cayman, assicurandosi che i profitti non vengano tassati. In seguito, si aggiunge un'altra azienda irlandese, stavolta per le vendite ai clienti europei, anch'essa soggetta a una tassazione molto bassa. Infine, viene sfruttata un'altra vulnerabilità, stavolta tramite un'azienda intermediaria olandese, per trasferire di nuovo i profitti alla prima azienda irlandese e a sua volta al paradiso fiscale offshore. Le aziende tecnologiche sono perfette per sfruttare tale vulnerabilità; possono assegnare i diritti di proprietà intellettuale a sussidiarie all'estero, che potranno trasferire la liquidità nei paradisi fiscali. È così che aziende come Google e Apple hanno evitato di pagare il giusto ammontare di tasse negli Stati Uniti, pur essendo aziende statunitensi.[5]

Si tratta di un uso del sistema fiscale senza dubbio imprevisto e non voluto, per quanto le normative fiscali irlandesi mirassero proprio ad attrarre le aziende americane. E gli hacker possono guadagnarci parecchio. Si stima che le aziende americane, nel solo 2017, abbiano evitato di pagare quasi 200 miliardi di dollari di tasse negli Stati Uniti, tutto a spese di qualcun altro. Nel mondo delle tasse, bug e vulnerabilità vengono chiamati *loophole*, scappatoie. C'è chi le sfrutta, attuando la cosiddetta elusione fiscale. Ci sono migliaia di persone paragonabili ai *black-hat researcher* del mondo informatico: avvocati e commercialisti specializzati in tasse, persone che esaminano ogni riga del codice in cerca di vulnerabilità da sfruttare.

Noi sappiamo come si riparano le vulnerabilità di un codice informatico. Per prima cosa, possiamo servirci di strumenti che le individuino prima di completare il codice. In secondo luogo, una volta diffuso il codice, esistono sistemi per rintracciarle e – cosa

fondamentale – metterci una patch, una toppa, alla svelta.

In ambito fiscale possiamo fare lo stesso. La legge fiscale del 2017 stabiliva un tetto per le deduzioni sulle tasse di proprietà,[6] un provvedimento che sarebbe entrato in vigore solo nel 2018. Qualcuno aveva pertanto pensato di anticipare nel 2017 il pagamento delle tasse di proprietà del 2018. Poco prima della fine dell'anno, l'Irs ha messo una patch a questa vulnerabilità, stabilendo in quali casi tale pratica fosse legale o meno. Per farla breve: non lo era quasi mai.

Ma in genere non è così facile. Ci sono hack insiti nelle stesse leggi, o che non possono essere prevenuti con nuove norme. L'approvazione di una legge fiscale non è mai cosa di poco conto, soprattutto negli Usa, dove il tema tende a polarizzare le fazioni. Solo nel 2021 si è cominciato a porre rimedio al bug che tassava le famiglie delle vittime di guerra. Il Congresso non è intervenuto sul bug del 2017, ma su uno precedente che interagiva con quello del 2017. L'intervento correttivo è durato fino al 2023[7] (ed era un intervento semplice, visto che tutti riconoscevano che si trattasse di un errore). Non possiamo mettere patch al codice che regola le tasse con la stessa facilità con la quale si può intervenire su un software.

Può accadere anche un'altra cosa: che non si ponga riparo alla vulnerabilità e lentamente divenga parte del *modus operandi*. È il destino di molti loophole fiscali. Talvolta l'Irs li accetta. A volte qualche tribunale ne attesta la legalità. Per quanto non riflettano l'intento del legislatore, sono comunque consentiti dal testo della legge. A volte vengono perfino legalizzati retroattivamente dal Congresso, se supportati da un collegio elettorale. Tramite questo processo, i sistemi si evolvono. Un hack sovverte le finalità di un sistema. Il sistema legislativo che ne ha competenza decide se bloccarlo o consentirlo. A volte lo consente esplicitamente, mentre in altri casi non fa niente e di fatto lo consente implicitamente.

1. Dylan Matthews (29 marzo 2017), “The myth of the 70,000-page federal tax code”, *Vox*, www.vox.com/policy-and-politics/2017/3/29/15109214/tax-code-page-count-complexity-simplification-reform-ways-mean.
2. Microsoft (12 gennaio 2020), “Windows 10 lines of code”, https://answers.microsoft.com/en-us/windows/forum/all/windows-10-lines-of-code/a8f77f5c-0661-4895-9c77-2efd42429409.
3. Naomi Jagoda (14 novembre 2019), “Lawmakers under pressure to pass benefits fix for military families”, *The Hill*, https://thehill.com/policy/national-security/470393-lawmakers-under-pressure-to-pass-benefits-fix-for-military-families.
4. *New York Times* (28 aprile 2012), “Double Irish with a Dutch Sandwich” (infografica), https://archive.nytimes.com/www.nytimes.com/interactive/2012/04/28/business/Double-Irish-With-A-Dutch-Sandwich.html.
5. Niall McCarthy (23 marzo 2017), “Tax avoidance costs the U.S. nearly $200 billion every year” (infografica), *Forbes*, www.forbes.com/sites/niallmccarthy/2017/03/23/tax-avoidance-costs-the-u-s-nearly-200-billion-every-year-infographic.
6. US Internal Revenue Services (27 dicembre 2017), “IRS Advisory: Prepaid real property taxes may be deductible in 2017 if assessed and paid in 2017”, www.irs.gov/newsroom/irs-advisory-prepaid-real-property-taxes-may-be-deductible-in-2017-if-assessed-and-paid-in-2017.
7. Jim Absher (29 gennaio 2021), “After years of fighting, the military has started phasing out ‘Widow’s Tax’”, Military.com, www.military.com/daily-news/2021/01/19/after-years-of-fighting-military-has-started-phasing-out-widows-tax.html.

CAPITOLO 3

Che cos'è un sistema?

Un hack segue la lettera delle regole di un sistema, violandone però spirito e intento. Perché possa esserci un hack, è necessario un sistema di regole da hackerare. Devo pertanto fare un passo indietro e definire con maggiore esattezza il significato della parola "sistema", perlomeno per come la utilizzo.

> Definizione: *Sistema*/sistèma/ (sostantivo):
> Un processo complesso, determinato da una serie di regole o norme, pensato per produrre uno o più esiti desiderati.

Il word processor col quale ho scritto questo paragrafo è un sistema: una serie di segnali elettronici regolati da un set di regole di un software con lo scopo di fare apparire tali parole sullo schermo, secondo l'esito da me voluto. La creazione di questo libro è il prodotto – l'esito, l'*outcome* – di un altro sistema, con processi che includono l'impaginazione, la stampa e la rilegatura e infine la distribuzione. Ogni singolo processo viene completato secondo una serie di regole. Questi due sistemi, insieme a molti altri, portano al libro che tenete in mano o al file elettronico che state leggendo sul vostro e-reader, o ai file che ascoltate col vostro sistema audiobook. Questo è vero sia quando gli elementi di un sistema si trovano sotto lo stesso tetto sia quando sono sparpagliati per il mondo. È vero sia con un esito reale sia con un esito virtuale, che il libro sia gratis o molto costoso, fatto male o di difficile reperibilità. Di mezzo c'è sempre un sistema, o più di uno.

I sistemi seguono delle regole. Spesso sono leggi, ma può trattarsi anche delle regole di un gioco, delle norme informali di un gruppo o di un processo, o delle tacite regole della società. Anche i sistemi cognitivi seguono delle leggi: le leggi naturali.

Ribadiamo che gli hack sono una cosa consentita dal sistema.

Quando dico “consentito” mi riferisco a qualcosa di molto specifico. Non riguarda ciò che è legale, permesso, socialmente accettabile o perfino etico, per quanto possa includere queste categorie. Mi riferisco invece al fatto che il sistema, per come è costruito, non impedisce all’hack di verificarsi entro i suoi confini. Il sistema non consente gli hack deliberatamente, ma solo incidentalmente e involontariamente, per via di come è stato progettato. Nei sistemi tecnici, significa in genere che è il software a consentire l’hack. Nei sistemi sociali, significa in genere che sono le norme – di solito le leggi – che controllano il sistema a non vietare espressamente l’hack. Per questo talvolta usiamo il termine “loophole” per parlare di questi hack.

Significa che gli hack vengono messi in atto contro sistemi ai quali i partecipanti hanno in primo luogo dato il loro consenso – esplicito o implicito – accettando di obbedire a una serie di regole comuni. A volte le regole del sistema non sono uguali alle leggi che governano il sistema. So che può non esser chiaro, pertanto cercherò di spiegarlo con un esempio. Un computer viene controllato da una serie di regole determinate dal suo software. Hackerare il computer significa sovvertire tale software. Ci sono però anche leggi che in potenza governano quel che è legalmente consentito fare. Negli Usa, ad esempio, il Computer Fraud and Abuse Act stabilisce che gran parte delle forme di hacking costituiscono reato (facciamo attenzione: il sistema hackerato è quello informatico, che viene però protetto dal più ampio sistema giuridico). L’ampiezza della legge crea una serie di problemi: in genere la legge è infatti diventata una sorta di ombrello onnicomprensivo per dichiarare illegale ogni tipo di hacking informatico.

Gli sport professionali vengono costantemente hackerati, in quanto governati da una serie di regole esplicite. La legge viene spesso hackerata, in quanto non è altro che una serie di regole.

In alcuni sistemi, naturalmente, le leggi equivalgono alle regole, o comunque ne determinano la maggioranza. Come vedremo parlando di hacking finanziario o di hacking del sistema giuridico, bastano un refuso o un passaggio poco chiaro in una legge, un contratto o una sentenza, e si possono spalancare le porte di un’infinità di soluzioni

senza dubbio non previste dagli estensori originali o dai giudici stessi.

Soffermiamoci su un tratto importante: non è necessario che le regole siano esplicite. Esistono molti sistemi, in particolare quelli sociali, regolati da norme. Le norme sociali sono meno formali delle regole; spesso non sono scritte, ma servono comunque da bussola per i comportamenti. Siamo costantemente limitati da una serie di norme sociali: norme diverse per situazioni diverse. Anche la politica è governata tanto da norme di comportamento quanto da leggi: negli Usa lo sappiamo bene, visto che negli ultimi anni abbiamo assistito all'infrazione di una norma dopo l'altra.

Nella mia definizione uso anche l'espressione "pensato per", che presuppone la presenza di un "progettista", qualcuno in grado di determinare l'esito desiderato di un sistema. È una parte importante della definizione, anche se non è sempre vera. Nel caso dei computer, i sistemi hackerati vengono creati deliberatamente da una persona o un'organizzazione, e pertanto l'hacker supera in furbizia i progettisti del sistema. La cosa vale però anche per i sistemi di regole stabilite da una istituzione, che si tratti di procedure aziendali, regole sportive o trattati dell'Onu.

Molti dei sistemi che analizzeremo in questo libro non sono stati progettati da singole persone. Non c'è stato un singolo ideatore del mercato capitalista; molte persone hanno dato il proprio contributo nel corso degli anni. Lo stesso vale per il processo democratico; negli Usa è una combinazione di Costituzione, leggi, pronunce giudiziarie e norme sociali. Quando qualcuno hackera un sistema sociale, politico o economico, supera in furbizia una combinazione costituita dai designer del sistema, dal processo sociale che ha consentito al sistema sociale di evolversi, e dalle norme sociali che governano il sistema.

Col tempo si sono evoluti anche i nostri sistemi cognitivi, senza l'intervento di alcun designer. L'evoluzione è parte integrante dei sistemi a base biologica: emergono nuovi usi per i sistemi già esistenti, i vecchi sistemi vengono riconvertiti a un nuovo scopo, i sistemi superflui si atrofizzano. Parliamo comunque di "scopo" di un sistema biologico: lo scopo della milza o lo scopo dell'amigdala.

L’evoluzione è il modo in cui un sistema si “progetta” da solo senza un designer. Il punto di partenza di tali sistemi è la loro funzione all’interno di un corpo o di un ecosistema, anche quando nessuno l’ha volutamente progettata.

L’hacking è il frutto naturale di un pensiero sistemico. I sistemi permeano gran parte delle nostre vite. Sono alla base di ogni società complessa, e con la complessità della società cresce anche la complessità dei sistemi. E lo sfruttamento di tali sistemi – l’hacking – si fa sempre più importante. Se comprendi a fondo un sistema, non devi sottostare alle stesse regole degli altri. Puoi andare in cerca di difetti e omissioni nelle regole. Puoi svelare in quali punti i limiti dettati dal sistema non funzionano. Hackerarlo senza sforzo. E se sei ricco e potente, probabilmente la farai franca.

CAPITOLO 4

Il ciclo vitale dell'hacking

In termini di sicurezza informatica, un hack è composto da due parti: una vulnerabilità e un exploit.

Una *vulnerabilità* è la caratteristica di un sistema che offre la possibilità di un hack. In un sistema informatico, è un difetto. Può essere un errore o una svista: di progettazione, di specificazione, o nel codice stesso. Può trattarsi di una minuzia come la mancanza di una parentesi, o essere grande come una proprietà dell'architettura del software. È il motivo sotteso al funzionamento di un hack.

L'*exploit* è il meccanismo impiegato per sfruttare tale vulnerabilità. Ti logghi in un sito e quel sito diffonde la tua password e il tuo username in tutta la rete: è un esempio di vulnerabilità. L'exploit in questo caso potrebbe essere un software che sbircia le connessioni internet e poi usa il tuo username e la tua password per accedere in quel sito. Un altro esempio di vulnerabilità: un frammento di software che espone i file privati di un altro utente. In questo caso l'exploit sarebbe un software per vederli. Una porta che può essere aperta senza una chiave è un altro caso di vulnerabilità. In tal caso l'exploit sarebbe un grimaldello o un altro strumento per aprirla.

Un altro esempio dal mondo dei computer: EternalBlue. Nel codice della Nsa, la National Security Agency statunitense, è il nome di un exploit contro il sistema operativo Windows, utilizzato dalla Nsa per almeno cinque anni prima del 2017, quando i russi glielo rubarono. EternalBlue sfrutta una vulnerabilità dell'implementazione del protocollo Server Message Block (Smb) di Windows, che controlla la comunicazione client-server. A causa del modo in cui il protocollo Smb è stato codificato, l'invio di un determinato pacchetto di dati da internet a un computer col sistema operativo Windows permetteva all'aggressore di eseguire un codice arbitrario sul computer ricettore, per poi prenderne il controllo. La Nsa era pertanto in grado di usare EternalBlue per controllare in remoto ogni computer Windows

connesso alla rete.

Un hack può coinvolgere diverse persone – ognuna con le sue competenze – e il termine "hacker", generando un po' di confusione, può fare riferimento a ognuna di loro. C'è innanzitutto l'hacker creativo, che usa ingegno ed esperienza per scoprire l'hack e creare l'exploit. Nel caso di EternalBlue, fu uno scienziato informatico della Nsa a scoprirlo. Nel caso della falla "Double Irish", fu qualche esperto di tasse su scala internazionale a studiare nei minimi dettagli le varie leggi e il loro modo di interagire.

In secondo luogo, c'è la persona che usa praticamente l'exploit. Alla Nsa fu l'impiegato che utilizzò l'exploit contro un bersaglio. Negli studi contabili, era il dipendente che sfruttava le leggi fiscali irlandesi e olandesi per la strategia elusiva di una corporation. L'hacker che attua hack di questo genere si serve della creatività di qualcun altro. Nel mondo dell'informatica li prendiamo in giro chiamandoli *script kiddies*, "marmocchi dello script". Non sono abbastanza svegli o creativi da trovare nuovi hack, ma sanno usare programmi – script – che sfruttano l'ingegno degli altri.

Infine c'è l'organizzazione o la persona che trae vantaggio dall'intero processo. Per questo diciamo magari che la Nsa ha hackerato una rete straniera, che la Russia ha hackerato gli Usa o che Google ha hackerato il sistema fiscale. È un punto importante, visto che ritorneremo costantemente su come ricchi e potenti hackerano i sistemi. Non sto dicendo che siano ricchezza e potere a renderti un hacker migliore, ma solo che ti consentono maggior spazio di manovra. Come nel caso degli Usa, della Russia o di Google, ricchezza e potere permettono di avvalersi delle competenze di chi sa hackerare al meglio i sistemi.

Un hack può essere inventato o scoperto. Per essere più specifici, la vulnerabilità viene scoperta, mentre l'exploit viene inventato. Si usano entrambi i termini, ma io preferisco "scoperto": ribadisce infatti che stiamo parlando di una caratteristica già presente nel sistema prima che qualcuno se ne accorga.

Quel che accade dopo la scoperta di un hack dipende dallo scopritore. In genere, la persona o l'organizzazione che scopre l'hack lo sfrutta a proprio vantaggio. In un sistema informatico, può

trattarsi di un hacker criminale o di un'agenzia di intelligence come la Nsa, o di qualunque cosa tra questi due estremi. A seconda di chi comincia a usarlo e come, la notizia si può diffondere, o può accadere che anche altri lo scoprano per caso. Perché questo accada possono volerci settimane, mesi o anni.

In altri sistemi, l'utilità di un hack dipende da quanto spesso viene usato e dal fatto che la cosa avvenga pubblicamente o meno. Una vulnerabilità segreta in un sistema bancario può venire sfruttata di tanto in tanto da hacker criminali, senza che per anni la banca se ne accorga. Un hack fiscale di qualità può proliferare semplicemente perché chi lo scopre decide di approfittarne vendendolo in giro.[1] Una buona manipolazione psicologica, una volta che abbastanza persone ne parlano, può diventare pubblica, ma può anche restare segreta per generazioni.

Prima o poi il sistema reagisce. L'hack può essere neutralizzato se viene messa una patch sulla vulnerabilità di base: qualcuno aggiorna il sistema per rimuovere la vulnerabilità o trova comunque un sistema per renderla inutilizzabile. Senza vulnerabilità non c'è hack, è elementare.

Questo presuppone che ci sia qualcuno che controlla il sistema target occupandosi dei processi di aggiornamenti. È una cosa scontata se parliamo del sistema operativo Microsoft Windows o di qualunque altro grosso software: sarà sempre difeso dai suoi sviluppatori. Aziende come Microsoft e Apple sono diventate molto brave con le patch.

Lo stesso vale per i software open source e di dominio pubblico, in genere possono contare su una persona o un'organizzazione che se ne occupa, e inoltre il codice è visibile a tutti. Non si può dire lo stesso per i software IoT a basso prezzo: spesso sono stati progettati all'estero, con margine di profitto molto esiguo, da software team che magari nel frattempo non esistono più. Cosa ancor più grave, molti device IoT non offrono la possibilità di mettere patch. Non perché non si sappia come fare, ma perché il codice di molti device IoT non è inserito nel software, bensì nell'hardware, cosa che lo rende immodificabile. È un problema che si aggrava quando le fabbriche chiudono e le aziende falliscono, lasciandosi alle spalle una scia di

milioni di device connessi a internet.

Nei sistemi tecnici, gli hack in genere vengono affrontati con una patch non appena vengono scoperti. Lo stesso processo non può avvenire con altrettanta rapidità nei sistemi sociali dei quali parlo in questo libro. L'aggiornamento del sistema fiscale, ad esempio, richiede un processo legislativo lungo anni. Si può legittimamente discutere del fatto che un hack faccia o meno del bene alla società. Inoltre, come vedremo spesso nel resto del libro, ricchi e potenti hanno forte voce in capitolo sul processo apparentemente democratico di delibera. Quando non viene messa una patch, l'hack viene integrato nelle regole del sistema, e diviene la nuova normalità. Quel che in principio è un hack può in men che non si dica diventare un'abitudine. Molti hack non tecnici dei quali parlerò in questo libro hanno seguito questo percorso.

1. Ricordo di aver letto di un loophole fiscale rivelato ai possibili investitori solo dopo la firma di un accordo di non divulgazione, e comunque senza spiegare tutti i dettagli. Mi piacerebbe poter ritrovare quell'articolo.

CAPITOLO 5

L’hacking è dappertutto

Per quanto un sistema possa essere a tenuta stagna presenterà sempre qualche vulnerabilità, consentendo di mettere in atto degli hack. Nel 1930, il matematico austriaco Kurt Gödel dimostrò che tutti i sistemi matematici sono incompleti o incoerenti. Secondo una mia teoria, questo vale anche in senso più generale. Tutti i sistemi sono destinati a presentare ambiguità, incoerenze interne o sviste, e per questo saranno sempre esposti a possibili exploit. I sistemi di regole, in particolare, devono camminare sul filo sottile tra l’essere completi e l’essere comprensibili, secondo i molti limiti del linguaggio e della comprensione umani. Se a questo aggiungiamo l’inevitabilità delle vulnerabilità e la naturale esigenza umana di superare le costrizioni e sfidare i limiti, ecco che tutto viene hackerato in continuazione.

Club Penguin era un gioco online Disney per bambini, attivo dal 2005 al 2017. Il fatto che i bambini possano parlare con degli sconosciuti online è sempre fonte di preoccupazione, pertanto Disney creò una modalità “Ultimate Safe Chat” (chat super sicura) che impediva di scrivere liberamente, e offriva agli utenti la possibilità di usare solo una serie di messaggi preimpostati. L’idea era quella di mettere i bambini al sicuro da chat a ruota libera con predatori sessuali veri o presunti. Ai bambini piaceva però parlare tra di loro, e hackerarono tale restrizione usando le posture corporee dei propri avatar per comunicare cose come lettere e numeri. I bambini sono hacker naturali. Non comprendono le intenzioni dietro a una scelta, e pertanto non osservano i limiti come farebbero gli adulti. Considerano i problemi in modo olistico, e possono inventare un hack senza rendersene conto. Non si sentono limitati dalle norme, e di sicuro non vedono la legge allo stesso modo. Per loro, sfidare le regole è una dimostrazione di indipendenza.

Proprio come Club Penguin, molti altri giochi online per bambini

hanno cercato di limitare il linguaggio, per prevenire bullismo e molestie, ma i bambini hanno hackerato ogni sorta di restrizione.[1] Ad esempio hanno scritto volutamente male alcune parole, per aggirare i filtri contro le parolacce, scrivendo cose come “phuq”, dividendo le frasi in vari messaggi in modo che nessuna infrangesse le regole, oppure servendosi di acrostici. Alcuni siti hanno impedito agli utenti di scrivere i numeri e i bambini hanno reagito utilizzando le parole: “won” per dire uno, “too” per dire due, “tree” al posto di tre, e così via. Lo stesso vale per gli insulti: “lose her” per dire *loser*, perdente, o “stew putt” invece di *stupid*.

Alcune scuole hanno cercato di porre dei limiti all’utilizzo dei propri computer da parte degli studenti, che hanno controbattuto hackerandoli. Gli hack più riusciti vengono scambiati tra amici. Un distretto scolastico ha provato a limitare i siti visitabili dagli studenti, che però hanno scoperto di poter aggirare le restrizioni con una Vpn. Un altro distretto ha bloccato le chat, ma gli studenti hanno cominciato a chattare con un Google Doc condiviso.

Un hack del genere non è una novità. Ha perfino un nome: *foldering*.[2] È stato usato da persone diverse come il generale Petraeus (ex direttore della Cia), Paul Manafort (imprenditore e lobbista americano condannato per frode fiscale) o i terroristi dell’11 settembre. Questi ultimi hanno capito di poter sfuggire alla sorveglianza condividendo un account email con gli altri cospiratori: bastava che salvassero i messaggi come bozze senza mai spedire le email.

Ricordo che quando ero bambino esistevano hack per aggirare le regole del sistema telefonico. Nel caso siate troppo giovani per ricordare come funzionasse, cercherò di spiegarvelo. Una prima persona parlava con un centralinista e gli diceva di voler fare una chiamata a carico del destinatario. L’operatore effettuava la chiamata, e chiedeva a chiunque rispondesse se fosse disposto a ricevere una chiamata a proprio carico. Le chiamate a carico del destinatario erano molto costose, ma visto che si veniva chiamati dall’operatore, uno scambio di informazioni avveniva ancor prima di accettare di pagare. Pertanto facevamo così: chiedevamo una chiamata a carico del destinatario, in genere ai nostri genitori; loro la

rifiutavano e poi ci richiamavano a una tariffa standard, molto meno costosa. Un sistema che qualcuno riusciva a rendere ancor più efficiente. Certe famiglie avevano stabilito una serie di nomi in codice da dire all'operatore: "Bruce" significava "sono arrivato sano e salvo", "Steve" significava richiamatemi, e così via (l'operatore non aveva idea di come si chiamasse davvero chi effettuava la chiamata). Ancora oggi esistono hack telefonici per risparmiare sulle bollette. In Nigeria si chiama *flashing*:[3] si chiama qualcuno e si attacca prima che possa rispondere (l'equivalente di quando in Italia si "faceva uno squillo", *N.d.T.*). In India, poco dopo il 2010, questo sistema andava per la maggiore, visto che i costi dei cellulari e della rete fissa erano molto diversi.[4] Tutti questi hack mirano a scardinare il sistema telefonico, consentendo uno scambio di informazioni senza pagare.

La Dad, didattica a distanza, durante la pandemia di Covid-19 ha spinto molti studenti a scoprire il proprio animo hacker.[5] Uno studente ha cambiato il proprio nickname in "Sta riconnettendo..." e ha spento il video, per far finta di avere problemi di connessione. Nel marzo del 2020, nella città cinese di Wuhan, tra le prime ad aver adottato il lockdown, le scuole hanno cominciato a tenere le lezioni a distanza e gli studenti hanno provato a far fuori la app per i compiti a casa Ding Talk, bombardandola di pessime recensioni, con la speranza che gli app store la rimuovessero (non ha funzionato).[6]

I sistemi tendono a essere rigidi e a seguire pedissequamente le proprie regole. Per loro natura, cercano di limitare quel che possiamo fare, ed è inevitabile che qualcuno cerchi di fare qualcos'altro. Una volta capito che cosa sono i sistemi e come operano, li vedrete dappertutto. E allo stesso modo comincerete a vedere ovunque possibili hack.

Non significa che nessun sistema funzioni. Ripensiamo a Gödel.[7] Come dicono gli avvocati, "Tutti i contratti sono incompleti". Un contratto funziona non perché impedisca rigidamente alle parti in causa di violarne gli intenti, ma perché i suoi loophole sono riempiti dalla fiducia e dalle buone intenzioni, e nel caso le cose vadano male ci si potrà comunque rivolgere a un sistema giudiziario o di arbitrato. Per quanto possa sembrare ingenuo e idealista, sono i sistemi basati sulla fiducia a fare funzionare la società.[8] Quando stringiamo un

accordo, non richiediamo una protezione impeccabile, in quanto

1. non è possibile averla,
2. cercare di farlo sarebbe un processo lungo e inutile,
3. non ci serve davvero.

Lo stesso vale per i sistemi più generali. A far funzionare un sistema non è la sua presunta invulnerabilità, ma lo stesso mix di fiducia e tutela legale. In questo libro parlo di hack e hacking, ma in genere si tratta di eccezioni. La maggior parte delle persone non hackera i sistemi, e a loro volta i sistemi tendono in genere a funzionare bene per la maggior parte del tempo. Disponiamo inoltre di sistemi per affrontare un hack, nel caso venga messo in atto. Questa è resilienza. È questo che fa funzionare la società. È così che da millenni gli esseri umani reagiscono all'hacking.

Non tutti i sistemi sono hackerabili in egual misura. Nel corso del libro, vedremo varie caratteristiche dei sistemi che li rendono più o meno vulnerabili all'hacking. I sistemi complessi e pieni di regole sono particolarmente vulnerabili, semplicemente perché è più facile che si verifichino cose impreviste o non desiderate. Questo vale senza dubbio per i sistemi informatici – come ho scritto in passato, la complessità è il peggior nemico della sicurezza[9] – e per sistemi come quello fiscale, le norme finanziarie e l'intelligenza artificiale. I sistemi umani definiti da norme e regole sociali più flessibili sono più vulnerabili all'hacking, in quanto lasciano spazio all'interpretazione e alla scoperta di loophole.

D'altro canto, i sistemi meno fondamentali, di scala minore e marginali – e, volendo, più sperimentali e indefiniti – causano meno danni una volta violati: meglio lasciare che evolvano tramite l'hacking che preoccuparsi di che cosa possa andar male. Invece non è una buona idea, ed è pericoloso, lasciare che le persone hackerino la progettazione e la costruzione di un ponte: un errore può portare a una catastrofe. Ben diverso è il caso di quell'hacking che può portare a nuovi spettacolari e inattesi modi di usare internet.

L'hacking è una componente naturale della condizione umana. È ovunque, e come vedremo, è un processo evolutivo: costante,

interminabile e in grado di creare, come direbbe Darwin, “infinite forme, sempre più belle e meravigliose”, oppure strane e terribili.

1. Stephanie M. Reich, Rebecca W. Black e Ksenia Korobkova (ottobre 2016), "Connections and communities in virtual worlds designed for children", *Journal of Community Psychology* 42, n. 3, https://sites.uci.edu/disc/files/2016/10/Reich-Black-Korobkova-2014-JCOP-community-in-virtual-worlds.pdf
2. Steven Melendez (16 giugno 2018), "Manafort allegedly used 'foldering' to hide emails. Here's how it works", *Fast Company*, www.fastcompany.com/40586130/manafort-allegedly-used-foldering-to-hide-emails-heres-how-it-works.
3. Cara Titilayo Harshman (22 dicembre 2010), "Please don't flash me: Cell phones in Nigeria", *North of Lagos*, https://northoflagos.wordpress.com/2010/12/22/please-dont-flash-me-cell-phones-in-nigeria.
4. Atul Bhattarai (5 aprile 2021), "Don't pick up! The rise and fall of a massive industry based on missed call", *Rest of World*, https://restofworld.org/2021/the-rise-and-fall-of-missed-calls-in-india/.
5. Tribune Web Desk (14 maggio 2020), "Students find 'creative' hacks to get out of their Zoom classes, video goes viral", *Tribune of India*, www.tribuneindia.com/news/lifestyle/students-find-creative-hacks-to-get-out-of-their-zoom-classes-video-goes-viral-84706.
6. Anthony Cuthbertson (9 marzo 2020), "Coronavirus: Quarantined school children in China spam homework app with 1-star reviews to get it off appstore", *Independent*, www.independent.co.uk/life-style/gadgets-and-tech/news/coronavirus-quarantine-children-china-homework-app-dingtalk-a9387741.html.
7. Kimberly D. Krawiec e Scott Baker (2006), "Incomplete contracts in a complete contract world", *Florida State University Law Review* 33, https://scholarship.law.duke.edu/faculty_scholarship/2038.
8. Bruce Schneier (2012), *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*, John Wiley & Sons.
9. Bruce Schneier (19 novembre 1999), "A plea for simplicity: You can't secure what you don't understand", *Information Security*, www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html.

PARTE SECONDA
HACK E DIFESE FONDAMENTALI

CAPITOLO 6

L'hacking dei bancomat

Cominceremo da una serie di hack contro sistemi evidentemente limitati. Ci servirà per poi capire meglio gli hack contro ben più vasti sistemi politici, sociali, economici e cognitivi.

Un bancomat è essenzialmente un computer coi soldi dentro. È collegato alla rete della banca da internet – un paio di decenni fa era collegato tramite una linea telefonica e un modem – e usa un sistema operativo Windows. E ovviamente può essere hackerato.

Nel 2011, Don Saunders, un barista australiano, scoprì il sistema per prendere denaro gratis dal bancomat. Incappò in questo hack a tarda notte (la storia è più divertente se ce lo immaginiamo ubriaco). Scoprì un sistema per trasferire da un conto all'altro denaro che non aveva, e poi prendersi i contanti senza che il sistema registrasse la transazione. Questa cornucopia era conseguenza di una vulnerabilità nel software del bancomat usato per registrare i trasferimenti tra conti, associata a un'altra vulnerabilità di natura temporale, in quanto di notte i vari conti sui quali spostava il denaro tramite il bancomat andavano offline. Saunders non lo sapeva. L'aveva scoperto per caso, e si era reso conto di poter riprodurre il risultato. Nei cinque mesi seguenti, Saunders prelevò 1,6 milioni di dollari australiani, pari a circa 1,1 milioni di dollari americani.[1] Non venne smascherato, ma smise di farlo, si sentì in colpa, andò in terapia, e confessò pubblicamente. La banca non aveva ancora capito perché stesse perdendo tanti soldi.

Riflettiamo un attimo: in questo caso, che cosa viene hackerato? Rubare denaro a una banca è sempre illegale. Non viene però hackerato il sistema bancario nel suo insieme: vengono hackerati il bancomat e il software della banca. Saunders aveva trovato un sistema imprevisto e non voluto per usare tali sistemi – per fare cose che questi sistemi permettevano – in un modo che ne sovvertiva l'intento. Ecco qual era l'hack.

Decenni di attacchi ai bancomat e di contromisure di sicurezza sono stati una sorta di corsa agli armamenti per hacker e banche. Ci fanno capire soprattutto una serie di temi che ritroveremo nel corso del libro. I sistemi non esistono in modo isolato. Sono composti di sistemi più piccoli e fanno parte di un sistema più grande. I bancomat sono costituiti da un software informatico, certo. Ma sono anche oggetti fisici. Il loro utilizzo richiede un cliente e una rete bancaria in remoto. Gli hacker possono mettere nel proprio obiettivo uno qualunque di questi aspetti di un bancomat.

I primi attacchi ai bancomat erano rozzi, somigliavano più che altro a semplici furti. I criminali incollavano gli sportellini che dispensavano il denaro, e dopo che il cliente frustrato si era arreso e se n'era andato, li aprivano a forza per prendere i suoi soldi. Oppure trovavano un sistema per "intrappolare" le carte dei clienti nella fessura, per poi prelevarle e usarle. Staccavano interi bancomat e li portavano via per aprirli in un posto sicuro, come abbiamo visto in *Breaking Bad*. Le banche hanno sempre cercato di difendersi: hanno progettato bancomat nei quali gli sportelli per l'erogazione del denaro non avevano porticine da incollare, hanno fissato meglio i bancomat alle pareti e hanno cominciato a ricaricare con più frequenza i depositi di contanti, in modo che ci fosse meno denaro da rubare (i ladri più furbi hanno reagito colpendo i bancomat la sera prima di un ponte, quando erano più pieni di soldi). I bancomat moderni hanno i propri sistemi di videosorveglianza, non tanto per evitare attacchi del genere, ma per identificare e magari arrestare i criminali.

Alcuni attacchi sfruttavano il modo in cui il cliente percepisce l'autorità: ad esempio, un criminale vestito in modo elegante o con un completo della banca interrompe un cliente che sta usando un bancomat: "Questa macchina è fuori servizio, usi quest'altra". Il cliente si sposta alla macchina accanto senza fare storie, mentre il criminale mette un cartello "fuori servizio" sul primo bancomat. Il cliente completa la sua transazione e se ne va, e il cliente completa la transazione iniziale interrotta e preleva il denaro.

Furti del genere hanno portato a molti altri cambiamenti nella progettazione dei bancomat.[2] Il primo è stato quello di trattenere la

carta fino alla fine della transazione, in modo che qualche sconosciuto dall'aria distinta non interrompesse il cliente. In seguito, il sistema è stato riprogrammato per evitare che una sola carta potesse effettuare più operazioni contemporaneamente. Ma gli hack basati sull'autorità non sono scomparsi. Si dice che in Indonesia ne sia stata messa in atto una versione più spiccia: un falso impiegato finge di chiamare la banca per cancellare la carta di un cliente, dopodiché lo convince a consegnargliela.

Un altro tipo di hack prevede il furto di informazioni per creare e usare una carta duplicata. Si chiama *skimming*, e nel corso degli anni si è diffuso ed evoluto. Nella sua versione canonica viene montato un secondo lettore della striscia magnetica, nel quale l'ignaro cliente inserisce per sbaglio la sua card. Con l'aggiunta di una videocamera nascosta o di un sensore sulla tastiera, il criminale può impadronirsi anche del Pin. Una variante prevede l'uso di finti bancomat, ad esempio in un centro commerciale. Per quanto sembri un bancomat, la finta macchina si limita a rubare Pin e informazioni dalle carte, prima di allontanare i clienti a metà operazione con la scritta "fuori servizio". Questi hack sfruttano una serie di vulnerabilità. Innanzitutto il cliente non è abbastanza competente per accorgersi di uno skimmer o di un falso bancomat. In secondo luogo, la striscia magnetica di una carta bancomat può essere duplicata facilmente. Infine, il sistema di autenticazione del bancomat, basato sul possesso della carta e sulla conoscenza del Pin, non è poi tanto sicuro.

Altri hack dei bancomat prendono di mira il software. Nel gergo degli hacker si parla di *jackpotting*: fare in modo che il bancomat sputi banconote come fa una slot machine con le monete, senza dover rubare carte o Pin.[3] Nel 2016, a Taiwan venne lanciato un attacco del genere, che si è poi rapidamente diffuso in Asia, Europa e America Centrale, con perdite di decine di milioni di dollari.

Un altro attacco, che sfrutta un'altra vulnerabilità del software, è cominciato in Europa nel 2020 e si sta ancora diffondendo in tutto il mondo.[4]

Il jackpotting è composto di diverse fasi. La prima è capire tutti i dettagli tecnici: per farlo bisogna procurarsi un vecchio bancomat da smontare e studiare. Non è difficile: ce ne sono molti in vendita su

eBay. Una volta capiti i dettagli, gli hacker aprono il pannello di un bancomat attivo, lo collegano a un'uscita Usb, scaricano un malware nel suo computer e installano un software che consenta loro di accedervi da remoto. Può essere d'aiuto travestirsi: un criminale vestito da tecnico desta meno sospetti. Una volta eseguite queste operazioni, il criminale può spostarsi in un luogo sicuro e mandare un complice con una borsa da riempire di soldi, al quale comunicherà le giuste istruzioni per svuotare la macchina. Non abbiamo dati precisi su quanti soldi siano stati rubati in questo modo – le banche non amano di certo diffondere dettagli del genere – ma già dal 2018 il Secret Service degli Stati Uniti, l'agenzia governativa che si occupa, tra l'altro, della sicurezza valutaria, sta mettendo in guardia dal jackpotting le istituzioni finanziarie.[5] Erano comunque passati otto anni da quando, alla Def Con Hacker Conference del 2010, l'esperto di sicurezza Barnaby Jack aveva dato una dimostrazione pratica di jackpotting.[6] Il suo sistema non prevedeva che qualcuno dovesse armeggiare di persona con un bancomat; aveva trovato alcune vulnerabilità del software sfruttabili da remoto per ottenere lo stesso risultato.

1. Jack Dutton (7 aprile 2020), “This Australian bartender found an ATM glitch and blew $1.6 million”, *Vice*, www.vice.com/en_au/article/pa5kgg/this-australian-bartender-dan-saunders-found-an-atm-bank-glitch-hack-and-blew-16-million-dollars.
2. Zuraidah M. Sanusi, Mohd Nor Firdaus Rameli e Yusarina Mat Isa (13 aprile 2015), “Fraud schemes in the banking institutions: Prevention measures to avoid severe financial loss”, *Procedia Economics and Finance*, www.semanticscholar.org/paper/Fraud-Schemes-in-the-Banking-Institutions%3A-Measures-Sanusi-Rameli/681c06a647cfef1e90e52ccbf829438016966c44.
3. Joseph Cox (14 ottobre 2019), “Malware that spits cash out of ATMs has spread across the world”, *Vice Motherboard*, www.vice.com/en_us/article/7x5ddg/malware-that-spits-cash-out-of-atms-has-spread-across-the-world.
4. Dan Goodin (22 luglio 2020), “Thieves are emptying ATMs using a new form of jackpotting”, *Wired*, www.wired.com/story/thieves-are-emptying-atms-using-a-new-form-of-jackpotting.
5. Brian Krebs (27 gennaio 2018), “First ‘jackpotting’ attacks hit U.S. ATMs”, *Krebs on Security*, https://krebsonsecurity.com/2018/01/first-jackpotting-attacks-hit-u-s-atms.
6. Kim Zetter (28 luglio 2010), “Researcher demonstrates ATM ‘jackpotting’ at Black Hat conference”, *Wired*, www.wired.com/2010/07/atms-jackpotted.

CAPITOLO 7

L’hacking dei casinò

Richard Harris lavorava per il Nevada Gaming Control Board. Ispezionava le nuove slot machine prima che fossero installate nei casinò. Aveva accesso ai meccanismi interni delle slot e pertanto poteva sostituire i loro chip con i suoi. Il suo software modificato era programmato per far vincere il jackpot quando le monete venivano inserite in una determinata sequenza. Tra il 1993 e il 1995 modificò più di trenta macchine e vinse centinaia di migliaia di dollari tramite una serie di complici, fino a quando uno di loro non fece abbastanza attenzione e venne scoperto.[1]

Come un bancomat, anche una slot machine non è altro che un computer pieno di soldi. La slot è stata inventata nel 1895, e all’epoca era ovviamente meccanica, ma già dagli anni Ottanta è un computer a controllare i risultati. Le ruote che girano hanno solo una funzione psicologica. Su molte slot non ci sono nemmeno, vengono semplicemente simulate su uno schermo. Sin dagli albori le slot sono state hackerate. Alcuni modelli più vecchi venivano scossi fino a ottenere il risultato desiderato. Altri venivano ingannati inserendo monete legate a un filo. Molte slot contano con un sensore ottico le monete che elargiscono; oscurare il sensore inserendo un device dallo sportello delle vincite può consentire di ottenere più denaro.

Non c’è gioco del casinò che non sia stato hackerato. Alcuni di questi hack oggi sono normali. Non intendo che siano consentiti, ma che tutti ne abbiamo sentito parlare e non li consideriamo più innovativi o interessanti. Un tempo contare le carte a blackjack era considerato un hack: ora ci sono libri su come farlo e regole che lo impediscono.

Già dagli anni Cinquanta del Novecento si cerca di predire il risultato della roulette. La ruota gira a velocità costante, il croupier tende a lanciare la pallina sempre nello stesso modo, e con un computer puoi ipotizzare quali numeri avranno maggiori possibilità

di uscire.

Una tecnica degli anni Sessanta per barare prevedeva un computer portatile con un auricolare e comandi inseriti nelle scarpe.[2] Chi lo indossava inseriva i dati con le dita dei piedi: grazie a quelle informazioni, il computer avrebbe calcolato la velocità della ruota, la velocità alla quale il croupier in genere lanciava la pallina, e così via. Grazie all'auricolare, il giocatore avrebbe potuto conoscere i numeri con maggiori probabilità di uscire. I modelli successivi erano ancor più precisi nell'inserimento dei dati e nel calcolo della velocità, tanto che negli anni Settanta un gruppo di laureati della University of California, Santa Cruz, riuscirono a far soldi col loro computer da scarpa.

Il loro hack non era illegale. Solo nel 1985 il Nevada vietò l'utilizzo di dispositivi per prevedere l'esito dei giochi.[3] I casinò si difesero soprattutto cambiando le regole del gioco, ad esempio anticipando il momento in cui i croupier non accettavano più puntate.[4]

Contare le carte a blackjack è un hack difficile da attuare se non si è incredibilmente dotati. Per i giocatori è un vantaggio la presenza di molti dieci nel mazzo, mentre quando i dieci sono pochi, è favorito il banco. Chi riesce a contare le carte può capire se si trova in una situazione di vantaggio e se scommettere o meno. Il vantaggio è esiguo – solo l'1% rispetto al banco – ma effettivo. Richiede inoltre una forte concentrazione al giocatore.

I casinò hanno risposto in due modi. Il primo è rendere più difficile contare le carte. Molti casinò mescolano sei mazzi di carte assieme – utilizzando meccanismi automatici – e distribuiscono solo i primi due terzi del mazzo, per fare scendere il vantaggio probabilistico del giocatore. Oppure rimescolano il mazzo dopo ogni mano. A Las Vegas come ad Atlantic City, ci sono caposala che chiacchierano coi sospetti maghi del conteggio, per distrarli e intimidirli allo stesso tempo.

I casinò hanno cercato di fare dichiarare illegale il conteggio delle carte, ma non sono riusciti a far passare l'idea che servirsi di una strategia equivalga a barare (sono state invece approvate leggi che vietano l'uso di dispositivi per contare le carte).[5] I casinò devono pertanto limitarsi a beccare sul fatto i maghi del conteggio e a vietare

loro l'ingresso. Inizialmente l'hanno fatto ordinando ai dipendenti di stare in guardia per individuare comportamenti sospetti. Oggi le videocamere del casinò che tracciano il movimento di ogni carta lo fanno automaticamente. I casinò sono privati, e pertanto (anche se la cosa varia di Stato in Stato) possono negare l'ingresso a chiunque vogliano, a patto di non attuare discriminazioni illegali.[6]

L'altro sistema per fronteggiare chi conta le carte è accettarlo come una spesa inevitabile. Molte persone pensano di poter contare le carte e invece non ci riescono. I casinò possono sfruttare il luogo comune che a blackjack si possa sconfiggere il banco, e guadagnare dai sedicenti conta-carte più di quanto perdono da quelli reali. Alcuni casinò cercano perfino di tentare i giocatori, scrivendo nelle pubblicità che per il blackjack usano un solo mazzo per volta.

Ci sono però delle eccezioni. Negli anni Ottanta, un gruppo di studiosi di Harvard e del Mit ideò un innovativo hack per contare le carte.[7] I casinò sanno individuare i conta-carte: cercano persone che 1) vincono costantemente e 2) cambiano modo di puntare secondo una competenza strategica. Il gruppo del Mit suddivise i vari compiti di conteggio tra diversi giocatori, per evitare che venissero individuati. I conta-carte ai tavoli non cambiavano mai modo di puntare. E così facevano quelli tra loro che puntavano di più, che venivano però indirizzati ai "tavoli caldi" dai complici che ricevevano i segnali. Si stima che il gruppo sia riuscito a vincere circa 10 milioni di dollari prima di smettere.[8] Davvero un ottimo hack.

1. *Las Vegas Sun* (21 febbraio 1997), "Slot cheat, former casino regulator, reputed mob figure added to Black Book", https://lasvegassun.com/news/1997/feb/21/slot-cheat-former-casino-regulator-reputed-mob-fig.
2. Paul Halpern (23 maggio 2017), "Isaac Newton vs. Las Vegas: How physicists used science to beat the odds at roulette", *Forbes*, www.forbes.com/sites/startswithabang/2017/05/23/how-physicists-used-science-to-beat-the-odds-at-roulette.
3. Don Melanson (18 settembre 2013), "Gaming the system: Edward Thorp and the wearable computer that beat Vegas", *Engadget*, www.engadget.com/2013-09-18-edward-thorp-father-of-wearable-computing.html.
4. Grant Uline (1 ottobre 2016), "Card counting and the casino's reaction", *Gaming Law Review and Economics*, www.liebertpub.com/doi/10.1089/glre.2016.2088.
5. David W. Schnell-Davis (autunno 2012), "High-tech casino advantage play: Legislative approaches to the threat of predictive devices", *UNLV Gaming Law Journal* 3, https://scholars.law.unlv.edu/cgi/viewcontent.cgi?article=1045&context=glj.
6. Il New Jersey fa eccezione. I casinò di Atlantic City non possono vietare l'ingresso a chi conta le carte. Donald Janson (6 maggio 1982), "Court rules casinos cannot bar card counters", *New York Times*, www.nytimes.com/1982/05/06/nyregion/court-rules-casinos-may-not-bar-card-counters.html.
7. Ben Mezrich (2002), *Blackjack Club: la vera storia dei sei studenti di matematica che hanno sbancato Las Vegas*, Mondadori.
8. Janet Ball (26 maggio 2014), "How a team of students beat the casinos", *BBC World Service*, www.bbc.com/news/magazine-27519748.

CAPITOLO 8

L'hacking delle promozioni per i frequent flier

Nel 1999, David Phillips acquistò più di 12mila budini Healthy Choice. Perché mai? Per hackerare un programma *frequent flier*. Questi programmi divennero popolari nel 1981, quando American, United e Delta cominciarono a proporli. Oggi ogni compagnia aerea ne ha uno. Sono programmi fedeltà che ricompensano i clienti che viaggiano spesso sulle loro linee dando loro buoni motivi per non cambiare compagnia. Prima del Covid-19, anch'io volavo in continuazione. Conosco alla perfezione questi programmi. Sin dall'inizio sono stati hackerati. Uno dei primi hack si chiamava *mileage run*. I passeggeri, in base alle distanze percorse nei loro viaggi, guadagnano miglia, che diventano una sorta di valuta privata scambiabile coi biglietti. Un bravo hacker troverà sempre il modo migliore per sfruttare l'esistenza di due diverse valute: nel caso specifico, per ottenere molte miglia pagando poco. Ad esempio, un volo diretto da New York ad Amsterdam vale 3.630 miglia, mentre con scalo a Istanbul ne dà 6.370. Se i due biglietti hanno lo stesso prezzo, e non hai di meglio da fare, è un affarone.

Le mileage run erano senza dubbio una sovversione imprevista dei programmi frequent flier. Poi gli hack si sono complicati. I programmi prevedono anche ricompense: ad esempio, un viaggiatore che percorre almeno 50mila miglia l'anno otterrà un vantaggio supplementare. Ci sono pertanto clienti che percorrono itinerari complicati ma economici, con sei o più fermate, solo per accumulare miglia. Non escono nemmeno dagli aeroporti. Per anni le compagnie aeree non hanno badato a questi hack. Nel 2015 hanno però cominciato a cambiare i propri programmi per penalizzare il mileage run.[1] Hanno deciso che bisognava spendere almeno una determinata cifra per raggiungere lo status d'élite, al punto di associare la definizione di "frequent flier mile" non più alle miglia percorse ma ai soldi spesi.

Altri hack prevedevano l'accumulo di punti senza volare.[2] Da tempo le compagnie aeree sono collegate alle carte di credito, che offrono miglia con ogni acquisto, oltre a grandi bonus miglia al momento della sottoscrizione. In questo caso l'hack è scontato: sottoscrivere tante carte di credito e cancellarle prima di qualsiasi addebito. C'è chi ha sottoscritto una carta di credito e ha subito comprato 3.000 dollari di gift card su Amazon per ottenere un bonus supplementare, oppure chi ha riempito il garage di frullatori per sfruttare una promozione che offriva punti extra a chi comprava elettrodomestici. Una donna si è vantata di aver "sottoscritto quarantasei carte di credito in cinque anni, guadagnando 2,6 milioni di miglia solo con i bonus al momento della firma".

Il danno per le banche è trovarsi a pagare miliardi di dollari in voli e altre ricompense a clienti che non pagano commissioni e interessi sulle loro carte di credito, e questi costi ricadono inevitabilmente sui clienti che pagano i biglietti più cari. Alcune emittenti di carte di credito hanno cercato di fare qualcosa. Nel 2016, Chase ha stabilito che una persona che avesse già sottoscritto cinque o più carte di credito in varie banche negli ultimi ventiquattro mesi non avrebbe potuto diventare loro cliente.[3] American Express attualmente revoca le miglia a chi "ha abusato, usato in modo scorretto, o abbia adottato schemi per guadagnare o utilizzare i punti":[4] una regola molto penalizzante per i clienti sospettati di approfittarsi del sistema.

Torniamo dunque a "Mister Budino".[5] Già famigerato hacker delle miglia aeree, Phillips scovò una vulnerabilità non di un programma in particolare, ma di una promozione di Healty Choice del 1999. All'epoca, gran parte delle compagnie aeree avevano programmi affiliati: aziende di ogni tipo potevano comprare pacchetti di miglia per frequent flier e offrirli come premio ai propri clienti. In questo programma in particolare, i clienti potevano guadagnare miglia aeree della compagnia che volevano come premio per aver acquistato i prodotti Healthy Choice. Phillips si mise in cerca del prodotto più economico adatto all'impresa, e finì per comprare 12.150 budini in coppetta singola al prezzo di 25 centesimi l'uno. Così con solo 3.150 dollari accumulò 1,2 milioni di miglia e lo status a vita di frequent flier "Gold" sui voli American Airlines (in seguitò donò i budini in

beneficenza, ottenendo per giunta una detrazione fiscale di 815 dollari). Non era certo un esito che Healthy Choice si aspettasse, ma Phillips non aveva infranto alcuna regola e l'azienda accettò di pagare.

1. Josh Barro (12 settembre 2014), “The fadeout of the mileage run”, *New York Times*, www.nytimes.com/2014/09/14/upshot/the-fadeout-of-the-mileage-run.html.
2. Darius Rafieyan (23 settembre 2019), “How one man used miles to fulfill his dream to visit every country before turning 40”, *NPR*, www.npr.org/2019/09/23/762259297/meet-the-credit-card-obsessives-who-travel-the-world-on-points.
3. Gina Zakaria (25 febbraio 2020), “If you’re interested in a Chase card like the Sapphire Preferred you need to know about the 5/24 rule that affects whether you’ll be approved”, *Business Insider*, www.businessinsider.com/personal-finance/what-is-chase-524-rule.
4. Nicole Dieker (2 agosto 2019), “How to make sure you don’t lose your credit card rewards when you close the card”, *Life Hacker*, https://twocents.lifehacker.com/how-to-make-sure-you-dont-lose-your-credit-card-rewards-1836913367.
5. Carla Herreria Russo (3 ottobre 2016), “Meet David Phillips, the guy who earned 1.2 million airline miles with chocolate pudding”, *Huffington Post*, www.huffpost.com/entry/david-philipps-pudding-guy-travel-deals_n_577c9397e4b0a629c1ab35a7.

CAPITOLO 9

L'hacking dello sport

Gli sport vengono hackerati costantemente. Penso sia dovuto alla compresenza di una pressione molto intensa – e a livello professionale, di un sacco di soldi – e di regolamenti inevitabilmente incompleti. Eccovi qualche esempio:

Baseball, 1951. I St. Louis Browns mettono in squadra Ed Gaedel, un giocatore alto un metro e dieci.[1] Va alla battuta una volta sola. Ovviamente ottiene un *walk*, visto che la sua zona *strike* è troppo piccola per lanciare con precisione.[2] La Lega non prevedeva limiti di altezza, pertanto si trattò di un hack legale. Il giorno dopo, il presidente della Lega annullò comunque il contratto del giocatore.

Basket, 1976. Finali Nba, siamo al secondo supplementare. I Phoenix Suns sono sotto di uno, e hanno meno di un secondo a disposizione sul cronometro. Devono rimettere dal fondo, non hanno tempo per arrivare al tiro. Il giocatore dei Suns Paul Westphal hackera le regole. Chiama un time out, anche se alla sua squadra non ne restano più. Gli arbitri sono pertanto costretti a fischiare un fallo tecnico, assegnando un tiro libero ai Boston Celtics. Un punto in più per i Celtics non fa differenza. Per i Suns l'importante è poter rimettere la palla a metà campo dopo il tiro libero, per poter segnare un tiro da due e arrivare al terzo supplementare.[3] Ed è proprio così che va. L'anno seguente, la Nba cambiò le regole, impedendo alle squadre di rimettere la palla da metà campo dopo un fallo tecnico.

Nuoto, 1988. Sia l'americano David Berkoff sia il giapponese Daichi Suzuki hackerano il nuoto a dorso, nuotando sott'acqua per quasi tutta la lunghezza della vasca, ottenendo tempi incredibili.[4] Ben presto la tecnica viene ripresa da altri nuotatori di primo livello, fino a quando interviene la International Swimming Federation, e stabilisce dei limiti alla distanza che si può percorrere sott'acqua.

Football americano, 2015. I New England Patriots usano un nuovo hack contro i Baltimore Ravens, mescolando i giocatori sulla linea di

scrimmage per manipolare le complicate regole che permettono ai giocatori di poter ricevere.[5] Due mesi dopo, la Lega cambia le regole per rendere illegale questo hack.[6]

Non sempre va così. Molti hack non vengono dichiarati illegali, bensì incorporati nel gioco perché lo migliorano. Molti aspetti dello sport oggi normali un tempo erano hack. Nel football americano, un tempo il passaggio in avanti era un hack. Lo stesso dicasi per l'attacco *run-and-shoot* e il *fast snap* mentre l'altra squadra sta cambiando giocatori. Nel baseball, un tempo la "volata di sacrificio" e il walk intenzionale erano hack. Queste cose non erano contro le regole. Semplicemente, prima che fossero attuate, i giocatori e le squadre non ci avevano pensato. Una volta che qualcuno le trovò, divennero parte del gioco.

Non è un processo che fila sempre liscio. Nel basket, un tempo le schiacciate erano un hack.[7] Nessuno pensava che si potesse saltare tanto in alto da spingere la palla nel canestro. Nei primi decenni del basket, si trattava di un gesto al tempo stesso acclamato ed esecrato. Molte leghe cercarono di vietarlo, ma dagli anni Settanta è diventato una pietra miliare di questo sport, visto che piace tanto al pubblico.

Nel cricket, a differenza del baseball, il battitore può colpire la palla secondo un cerchio completo. Per più di un secolo, il battitore in genere ha colpito la palla indirizzandola verso il lanciatore, come nel baseball, o deviandola col bordo della mazza dietro di sé. Solo all'inizio degli anni Duemila, qualche giocatore di cricket si è reso conto di poter correre il rischio di "scucchiaiare" la palla sopra la propria testa.[8] Era qualcosa che rientrava perfettamente nelle regole, servivano solo un po' di coraggio e una mente hacker (un giocatore ha sostenuto di aver sviluppato questa tecnica negli angusti vicoli dello Sri Lanka). Alcune vittorie storiche sono state conquistate con questa tecnica, che ora è entrata tra i classici del gioco.

Nel baseball è permesso leggere i segnali che si lanciano gli avversari, con tutta una serie di restrizioni e puntualizzazioni per i numerosi hack di questo sistema. Il giocatore in seconda base e il coach in terza possono cercare di leggere i segnali del catcher, ma il battitore non può, e le videocamere in campo sono vietate. Nel 2017 e 2018 gli Houston Astros hanno intercettato i segnali con una

videocamera, e visto che la regola era già in vigore, di fatto non hanno hackerato il sistema, ma hanno barato.

Una volta usati, la maggior parte degli hack sportivi diventano palesi. Quando nuoti sott'acqua o tiri la palla da cricket verso l'alto, non puoi certo nasconderlo. Appena un giocatore o una squadra lo fanno, tutti lo vengono a sapere. Gli sport dove le cose possono essere nascoste fanno però eccezione. Due esempi sono le corse basate su mezzi meccanici (dalle auto ai motoscafi) e il doping (per esseri umani e animali).

Le corse di Formula Uno sono piene di hack. All'inizio i membri di una squadra trovano un loophole nei regolamenti e migliorano la propria auto di conseguenza. In una seconda fase, gli altri team lo scoprono, e copiano l'idea o fanno ricorso contro l'innovazione. Infine, la Fia, Fèdèration Internationale de l'Automobile, decide se vietare l'hack o incorporarlo nelle specifiche dell'anno dopo.

Ad esempio, nel 1975, la Tyrrell costruì un'auto a sei ruote, due dietro e quattro davanti.[9] Un hack che migliorava le prestazioni ma rendeva l'auto meno affidabile. In tutta risposta, altri team costruirono i loro prototipi. Nel 1983 però la Fia stabilì che tutte le auto dovessero avere non più – e non meno, per essere sicuri – di quattro ruote. Nel 1978, la Brabham sfidò la regola che imponeva alle auto di non avere parti aerodinamiche semoventi come le ventole:[10] ne mise una accanto al radiatore, sostenendo che si trattava di un sistema di raffreddamento. L'auto venne ritirata volontariamente dalla competizione, senza che nessuna regola venisse cambiata. Nel 1997, la McLaren sviluppò un'auto con due pedali del freno, col secondo che controllava solo le ruote posteriori.[11] Non capisco abbastanza di corse automobilistiche da comprendere i dettagli, ma pare che per il pilota fosse un grosso vantaggio. Inizialmente la modifica fu approvata, per essere poi ritirata dopo le proteste degli altri team. Nel 2010, la McLaren hackerò il divieto di avere parti aerodinamiche semoventi realizzando un foro nell'abitacolo che il pilota poteva coprire o meno con la gamba.[12] La McLaren sosteneva infatti che nessuna parte fosse semovente, e pertanto inizialmente il sistema fu consentito. Il fatto che il pilota potesse mettere o togliere la gamba portava però a ottenere lo stesso effetto, e così la tecnica

venne vietata. Nel 2014, Mercedes rinnovò il turbocompressore del proprio motore di Formula Uno,[13] dividendo turbina e compressore e posizionandoli su due lati diversi del motore. Questa trovata non venne mai dichiarata illegale, e permise alla Mercedes di dominare il proprio sport per i sei anni a venire. Nel 2020, Mercedes ha aggiunto una caratteristica al proprio volante:[14] spingendolo o tirandolo, il pilota poteva cambiare l'allineamento delle ruote anteriori. Aggiungere funzionalità al volante è contro le regole; la legalità di questo hack dipende da come si definisce il sistema di sterzata, e se si considera questo accorgimento come parte dello sterzo o delle sospensioni. La Fia ha chiuso questo loophole nel 2021.

Un ultimo esempio, sul quale ritorneremo in seguito. Un tempo le mazze da hockey erano dritte. Poi qualcuno ha scoperto che con una mazza ricurva era possibile colpire il disco a velocità prima impossibili. Ora le mazze ricurve sono la norma, e ci sono limiti precisi alla loro curvatura. È celebre il caso del giocatore dei Los Angeles Kings Marty McSorley, che nel 1993, durante una partita di campionato, venne beccato con una mazza dalla curvatura non consentita.[15]

1. Associated Press (20 agosto 1951), "Brownies hit all-time low; Use 3-foot 7-inch player", *Spokesman-Review*, https://news.google.com/newspapers?id=rS5WAAAAIBAJ&sjid=3uUDAAAAIBAJ&pg=4920%2C3803143.
2. Nel baseball un "walk" (o "base su ball") è la possibilità di aggiudicarsi la prima base senza correre. Si verifica quando il lanciatore compie quattro lanci fuori dall'area di strike, che è determinata in base all'altezza del battitore della squadra avversaria (*N.d.T.*).
3. Presh Talwalkar (6 giugno 2017), "Genius strategic thinking in the 1976 NBA Finals", *Mind Your Decisions*, https://mindyourdecisions.com/blog/2017/06/06/genius-strategic-thinking-in-the-1976-nba-finals-game-theory-tuesdays. Secret Base (5 febbraio 2019), "The infinite timeout loophole that almost broke the 1976 NBA Finals", *YouTube*, www.youtube.com/watch?v=Od2wgHLq69U.
4. John Lohn (24 settembre 2021), "Seoul Anniversary: When the backstroke went rogue: How David Berkoff and underwater power changed the event", *Swimming World*, www.swimmingworldmagazine.com/news/seoul-anniversary-when-the-backstroke-went-rogue-how-david-berkoff-and-underwater-power-changed-the-event.
5. Rodger Sherman (10 gennaio 2015), "The Patriots' trick play that got John Harbaugh mad", *SB Nation*, www.sbnation.com/nfl/2015/1/10/7526841/the-patriots-trick-play-that-got-john-harbaugh-mad-ravens.
6. Ben Volin (26 marzo 2015), "NFL passes rule aimed at Patriots' ineligible receiver tactic", *Boston Globe*, www.bostonglobe.com/sports/2015/03/25/nfl-passes-rule-change-aimed-patriots-ineligible-receiver-tactic/uBqPWS5dKYdMYMcIiJ3sKO/story.html.
7. La trama del film del 1997 *Air Bud – Campione a quattro zampe* è incentrata su un hack del basket professionistico. Nel mondo del film non esistono regole che vietino a un cane di giocare in una squadra di basket (nel caso ve lo stiate domandando, non è un gran film).
8. Manish Verma (7 gennaio 2016), "How Tillakaratne Dilshan invented the 'Dilscoop'", *SportsKeeda*, www.sportskeeda.com/cricket/how-tillakaratne-dilshan-invented-dilscoop.
9. Jordan Golson (17 dicembre 2014), "Well that didn't work: The crazy plan to bring 6-wheeled cars to F1", *Wired*, www.wired.com/2014/12/well-didnt-work-crazy-plan-bring-6-wheeled-cars-f1.
10. Gordon Murray (23 luglio 2019), "Gordon Murray looks back at the notorious Brabham fan car", *Motor Sport*, www.motorsportmagazine.com/articles/single-seaters/f1/gordon-murray-looks-back-notorious-brabham-fan-car.
11. McLaren (1° novembre 2017), "The search for the extra pedal", www.mclaren.com/racing/latest-news/mclarenracing/article/mclaren-extra-pedal-3153421/.
12. Matt Somerfield (20 aprile 2020), "Banned: The 2010 Formula 1 season's F-duct", *AutoSport*, www.autosport.com/f1/news/149090/banned-the-f1-2010-season-fduct.
13. Laurence Edmondson (6 febbraio 2016), "Mercedes F1 engine producing over 900bhp with more to come in 2016", ESPN, www.espn.com/f1/story/_/id/14724923/mercedes-f1-engine-producing-900bhp-more-come-2016.
14. Laurence Edmondson (21 febbraio 2020), "Mercedes' DAS system: What is it? And is it a 2020 game-changer?" ESPN, www.espn.com/f1/story/_/id/28749957/mercedes-das-device-and-2020-game-changer.
15. Dave Stubbs (2 giugno 2017), "Marty McSorley's illegal stick still part of Stanley Cup Final lore", *National Hockey League*, www.nhl.com/news/marty-mcsorleys-illegal-stick-still-part-of-stanley-cup-final-lore/c-289749406.

CAPITOLO 10

La natura parassitica degli hack

Un virione Sars-CoV-2 è largo circa 80 nanometri. Si aggancia a una proteina chiamata Ace2, presente sulla superficie di molte cellule del nostro corpo: nel cuore, nello stomaco, nei polmoni e nelle cavità nasali. Di norma, la proteina Ace2 contribuisce alla regolazione di pressione sanguigna e alla cura di infiammazioni e ferite. Il virus può però afferrarla e fondersi alle membrane cellulari, penetrando la cellula col suo Rna. Il virus procede quindi a sovvertire il sistema produttore di proteine della cellula-ospite, usandolo per moltiplicarsi e infettare altre cellule. Altre parti dell'Rna del virus creano proteine diverse che permangono nella cellula ospite. Ce n'è una che impedisce alla cellula ospite di segnalare al sistema immunitario di trovarsi sotto attacco. Un'altra spinge la cellula ospite a rilasciare nuovi virioni. Una terza aiuta il virus a resistere all'immunità innata della cellula-ospite. Il risultato è la malattia che a partire dal 2020 ha avuto un ruolo chiave nelle nostre vite: il Covid-19.

Il Covid-19 è un hacker. Come tutti i virus, il Sars-CoV-2 sfrutta in modo ingegnoso il nostro sistema immunitario, sovvertendo le consuete operazioni di sistema a spese della nostra salute e della vita di più di sei milioni di persone in tutto il mondo. L'Hiv è un altro hacker. Infetta i globuli bianchi T-helper, inserisce il suo Dna in quello di una normale cellula, e poi si moltiplica al suo interno. La cellula infetta rilascia ulteriore Hiv nel sangue, facendo proseguire il processo di moltiplicazione.

In generale, l'hacking si comporta da parassita. Hiv e Sars-CoV-2 sono parassiti: vengono ospitati da altre specie e ne approfittano, danneggiando chi ha aperto loro le porte. Lo scopo di un sistema è perseguire una serie di obiettivi, in genere stabiliti da chi l'ha progettato. Un hacker si impadronisce del medesimo sistema per perseguire obiettivi diversi, magari contrari a quelli originali.

Lo vediamo con chiarezza negli hack dei bancomat, dei giochi

d'azzardo dei casinò, dei programmi per ricompensare i clienti o dei piani tariffari per le chiamate a lunga distanza. Lo scopo di chiunque abbia progettato un bancomat è consentire ai clienti di prelevare denaro, scalando la cifra equivalente dal loro conto in banca. Lo scopo dell'hacker è ottenere contanti senza alcuna deduzione (e magari senza neanche avere un conto). Lo scopo di un casinò è comportarsi in modo equo (vale a dire offrire le stesse possibilità di vincere a tutti i clienti, non equiparare le possibilità di vincita del banco e dei giocatori). Lo scopo dell'hacker è invece quello di ottenere un vantaggio.

Quando si tratta di sport e giochi online la cosa è meno evidente. Lo scopo di una lega sportiva potrebbe essere quello di guadagnare denaro, divertire e far felice il pubblico, esaltare la competizione tra gli atleti e lo spirito sportivo, e in generale offrire "belle gare", qualunque cosa significhi. Lo scopo di un atleta hacker è vincere le gare alle quali partecipa, che siano individuali o di squadra, a discapito della correttezza, ricavandone magari del denaro.

Lo scopo di Club Penguin era quello di offrire un'esperienza sicura e divertente ai suoi giovani utenti, seguendo le leggi vigenti e arricchendo la Disney Corporation. I suoi hacker invece volevano comunicare più liberamente con gli altri giocatori, che si trattasse di seienni in cerca di quattro chiacchiere o di un pedofilo in cerca di vittime. Entrambi i tipi di hacker erano parassiti, seppure di tipo del tutto diverso.

Lo spam è un hack delle email. Al momento di stabilire i protocolli internet e il sistema che governa le email, nessuno ci aveva pensato (per quanto la posta indesiderata sia una storica tradizione americana). Mandare email invadenti, soprattutto di natura commerciale, era un'idea imprevista. La pratica iniziò negli anni Novanta, via email o attraverso il sistema di messaggistica Usenet, allora in gran voga, per poi diventare un grave problema nei primi anni Duemila. Secondo una stima, all'epoca il 90% delle email erano di spam. Si tratta di un hack parassitario di un sistema di comunicazione.

Non tutte le relazioni parassitarie danneggiano chi le ospita, così come non tutti gli hacker sono malvagi. In genere sono soggetti che si

comportano in modo razionale seguendo i propri interessi. Si può trattare di un interesse finanziario, come accade nella maggior parte degli esempi di questo libro. Ma gli interessi possono essere anche di natura emotiva, morale, etica o politica; un hacker potrebbe cercare di migliorare il mondo. A volte gli hacker non cercano altro che un'occasione. A volte, in caso di sistemi che li prendono di mira, devono reagire per necessità, perché ne va della loro sopravvivenza. Pensiamo a una persona che cerca di ottenere sussidi per comprare cibo per sé o per la propria famiglia.

Come ogni parassita, l'hacking non può sovvertire eccessivamente il sistema ospite: gli serve che il sistema sopravviva per poter funzionare. Hackerare i bancomat può far guadagnare molti soldi, ma perché sia possibile è necessario che esistano i bancomat. Se l'hacking dei bancomat fosse troppo efficace, le banche smetterebbero di offrire tale servizio. Se troppe persone, in barba alle leggi per la sicurezza dei bambini, avessero hackerato Club Penguin per parlare, Disney l'avrebbe chiuso molto prima. Senza i programmi anti-spam, lo spam avrebbe distrutto le email. Un hack troppo efficace può condannarsi all'obsolescenza distruggendo il sistema dal quale dipende.

CAPITOLO 11

Difendersi dagli hack

Spectre e Meltdown sono due vulnerabilità dell'hardware di Intel e altri microprocessori; sono state individuate nel 2017, ma la scoperta è stata annunciata l'anno seguente. Essenzialmente si tratta di vulnerabilità alla sicurezza dovute alle ottimizzazioni della performance attuate nel corso degli anni. Si trattava di vulnerabilità dalle quali era difficile difendersi, in quanto si trovavano non nel software ma nell'hardware. Per il software vengono spesso sviluppate patch, magari a discapito della performance, ma per l'hardware non è così semplice. La sostituzione dei sistemi vulnerabili non era un'opzione possibile: si tratta di chip presenti in circa cento milioni di computer. Certo, si possono progettare i nuovi microprocessori senza queste vulnerabilità, ma quelli già esistenti non possono essere riparati retroattivamente.

La miglior difesa era probabilmente il fatto che fosse difficile sfruttare quelle vulnerabilità. Molti computer erano vulnerabili, ma in modo non evidente agli hacker.

Talvolta è molto difficile difendersi dagli hack. Le contromisure vanno dalle patch fino alla progettazione di sistemi sicuri, come vedremo in seguito.

Ammetto di utilizzare una tassonomia poco rigorosa. Approvare una legge che vieta di contare le carte nel blackjack rende la tattica inefficace solo se ci si fa scoprire. È un rimedio che elimina la vulnerabilità o si limita a ridurre l'efficacia dell'hack? Un dispositivo anti-taccheggio che spruzza inchiostro sugli abiti rubati rende meno utilizzabile il capo in questione (rendendo il furto meno efficace) e al tempo stesso rende il furto meno probabile (disincentivando il ladro). Queste ambiguità mi stanno bene. Più che la precisione delle categorie, mi interessa far capire quali sono i sistemi di difesa attuabili contro gli hacker e i loro hack.

La prima difesa, la più scontata, è *sbarazzarsi della vulnerabilità*

in questione.

Nel mondo informatico, la difesa principale è costituita dalle patch. È una tecnica diretta: si aggiorna il computer e si elimina la vulnerabilità. Senza vulnerabilità, non c'è nulla da sfruttare, e se non lo si può fare, non può sussistere l'hacking.

Il buon funzionamento di una patch dipende soprattutto dal sistema. I sistemi che appartengono o sono gestiti da un'entità unica possono essere riparati in fretta con una patch, sempre che la cosa abbia senso dal punto di vista economico. La creazione di una patch è solo il primo passo del processo; in seguito la patch va installata su tutti i sistemi vulnerabili.

In genere tra le aziende che creano le patch e gli utenti che le installano c'è di mezzo il mare. Spesso chi si occupa di software diffonde le patch, ma gli utenti non le installano, oppure impiegano settimane o mesi per farlo. E i sistemi senza patch continuano a essere vulnerabili.

In questo scenario stabiliamo come assunto che esista una singola entità in grado di scrivere la patch e motivata a farlo, oltre al fatto che il sistema possa essere riparato con una patch. Le patch possono rivelarsi efficaci se l'azienda ha abbastanza ingegneri per scriverle e se diffonde in fretta a tutti i clienti un aggiornamento di sistema. Basta che una delle due cose venga a mancare e le patch perdono efficacia (come ricorderemo, molti device IoT hanno il codice in firmware, e pertanto non possono ricevere patch). Ecco perché il nostro computer e il nostro telefono ricevono costantemente patch, e in genere sono al sicuro malgrado i mille hack in agguato. Ed ecco anche perché il nostro router casalingo di rado riceve patch, malgrado la propria vulnerabilità.

Molti hack di alto profilo hanno sfruttato l'esistenza di sistemi senza patch. Nel 2017, la Cina hackerò Equifax grazie a una vulnerabilità del software per il web Apache Struts. Apache aveva diffuso la patch per la vulnerabilità a marzo; Equifax non aveva aggiornato subito il suo software, e pertanto a maggio non era riuscita a resistere all'attacco hacker.

Sempre nel 2017, il worm WannaCry raggiunse 200mila computer in tutto il mondo, causando 4 miliardi di dollari di danni ai network

che non avevano ancora installato la patch per la vulnerabilità di Microsoft Windows.

È evidente uno dei principali punti deboli delle patch: arrivano sempre dopo. La vulnerabilità è già presente nel sistema, e magari da tempo gli hacker la stanno sfruttando. E anche se non lo stanno già facendo, la creazione di una patch attira l'attenzione sulla vulnerabilità, rendendo ben visibili i sistemi ancora non aggiornati.

Per gran parte dei singoli utenti di computer e device mobili, il patching in genere avviene automaticamente. Il vostro computer Microsoft è presumibilmente configurato per aggiornarsi una volta al mese durante il "Patch Tuesday", che può installare patch per più di cento diverse vulnerabilità. Il vostro iPhone vi assillerà con annunci sempre più catastrofici se non installerete le vostre patch. (Ve lo ripeto in modo chiaro: attivate gli aggiornamenti automatici su computer e telefono. Non appena riceverete un aggiornamento, installate ogni patch. Sempre).

Le organizzazioni basate su grandi reti devono invece procedere con maggiore prudenza e lentezza. Una patch sbagliata può infatti causare problemi di ogni sorta nella sua interazione con altri software fondamentali, e pertanto le patch vengono in genere installate volontariamente, facendo molta attenzione. Per questo a volte vengono installate in ritardo, o non vengono installate affatto. Per quanto si possa dare a Equifax la colpa di non aver messo una patch ad Apache Struts, dobbiamo ricordare che le patch di quel software avevano una pessima reputazione, e spesso si erano rivelate incompatibili con altri software. Molte organizzazioni procedono coi piedi di piombo.

Il patching dei sistemi sociali è ben diverso da quello dei sistemi tecnologici. In quest'ultimo caso, la patch rende impossibile l'hack preso di mira. Lo vediamo nel software, ma anche in altri sistemi tecnologici. Chi fabbrica bancomat può creare patch per le proprie macchine, in modo che un hack basato sul jackpotting smetta di funzionare. Un casinò può usare per il blackjack sei mazzi mescolati in continuazione. I sistemi di scambio finanziario possono fissare intervalli di dieci secondi per il trading, rendendo impossibili hack come il trading ad alta frequenza. È possibile in quanto è la

tecnologia a determinare l'*affordance* del sistema.

Il processo non è così lineare nei sistemi sociali, economici e politici, che non utilizzano i computer in modo tanto diretto. Quando parliamo di "patching" del sistema fiscale o delle regole di un gioco, intendiamo un cambiamento delle leggi o delle regole con lo scopo di non consentire più un certo attacco. Sarà pertanto ancora possibile usare un computer per giocare alla roulette o una mazza da hockey con una curvatura superiore a tre quarti di pollice, ma nel caso si venisse scoperti, si incorrerà in sanzioni. La sola "installazione" necessaria è la formazione: assicurarsi che i controllori dei casinò e gli arbitri dell'hockey conoscano le regole e sappiano individuare i bari per poi punirli. Allo stesso modo, l'elusione fiscale può diventare evasione, che sarà punita se smascherata (o almeno speriamo).

Si presenta pertanto un altro problema: spesso è difficile individuare i bari. Come ricorderete, la roulette è stata vulnerabile fino a quando il sistema di scommesse è stato cambiato al fine di rendere inefficaci gli hack. È un problema che si presenta ripetutamente nei sistemi descritti in questo libro. Se aggiorniamo un computer, l'hack non è più possibile. Se aggiorniamo il sistema fiscale, l'hack è ancora possibile, ma smette di essere una soluzione legalmente lecita (e smette anche di essere un hack, secondo la mia definizione). Pertanto dovrete aggiornare anche il sistema di rilevazione delle infrazioni, per beccare i furbi, ora divenuti fuorilegge, e perseguirli.

Il patching è inoltre meno efficace quando l'organismo preposto al controllo funziona lentamente o non sa decidere nemmeno se una patch sia o meno necessaria. Pensiamo ai sistemi senza un obiettivo chiaro. Che cosa vuol dire, ad esempio, mettere una "patch" al sistema fiscale? Nella maggior parte dei casi, significa approvare una nuova legge che ripari le vulnerabilità della precedente. È un processo che può richiedere anni, in quanto il sistema fiscale viene creato in ambito politico, un contesto caratterizzato da visioni contrastanti sullo scopo delle politiche pubbliche. E chi sfrutta una data vulnerabilità, per continuare a farlo cercherà inoltre di hackerare anche il sistema legislativo. Pensate se a decidere le regole dei casinò fossero stati quelli che contano le carte a blackjack.

Contare le carte oggi verrebbe onorato come un metodo intelligente e onesto, proprio come ottenere vantaggi fiscali viene considerato un esempio di furbizia.

In mancanza di patch legislative, può essere un tribunale a occuparsi di una determinata patch. Nel mondo del computer, si parla di *hotfix*: un aggiornamento rapido per riparare un bug o una vulnerabilità. Il termine deriva dal fatto che tali aggiornamenti vengono applicati a sistemi attivi a pieno regime, e pertanto caldi, "hot". È più rischioso; il software può crashare, con le conseguenze del caso. Oggi le hotfix sono normali – i nostri sistemi operativi vengono aggiornati mentre sono attivi, e c'è un gran via vai nel cloud – ma il termine risale a quando questo non era certo una consuetudine.

CAPITOLO 12

Forme di difesa più raffinate

Un secondo modo di difendersi è *ridurre l'efficacia di un hack*. La *business email compromise* è un attacco basato sull'ingegneria sociale, in quanto non cerca di sfruttare una vulnerabilità tecnologica, bensì una vulnerabilità delle persone. In questa truffa, la vittima riceve una email da una fonte della quale si fida, e che le chiede di svolgere una cosa normale in modo inconsueto, spesso andando contro un ben preciso protocollo. Qualche esempio: un libraio riceve da un fornitore la richiesta di accreditargli la cifra stabilita su un nuovo conto in banca; l'acquirente di una casa riceve una email dall'agenzia immobiliare con nuove indicazioni per il pagamento; il direttore finanziario di un'azienda riceve una email dal Ceo che gli chiede un trasferimento urgente di milioni di dollari in un nuovo conto. Sono *scam*, truffe, che costano miliardi di dollari.

Per effettuarle, talvolta vengono hackerate le email di veri venditori. In tal modo il truffatore risulta più credibile e può conquistare facilmente la fiducia della vittima. È più facile però che vengano inviate email di scam da indirizzi che differiscono leggermente da quelli veri: ad esempio, person@c*o*mpanyname.com invece di person@c*o*mpanyname.com, con uno zero a sostituire la "o". In questo caso, la vulnerabilità è la disattenzione umana, o la fiducia mal riposta.

Ci possono essere molti motivi per i quali una vulnerabilità non può essere riparata con una patch. In politica, può accadere che il processo legislativo necessario non sia funzionale. O può mancare il corpo politico in grado di intervenire. Nel tipo di hack basato sull'ingegneria sociale che ho appena descritto, gli hack sfruttano il funzionamento della mente umana, una cosa sulla quale si può mettere una patch solo evolvendosi, e l'evoluzione richiede molto tempo.

Quando non possiamo mettere una patch su una vulnerabilità, ci

restano tre opzioni. La prima è riprogettare il sistema in modo che l'hack sia troppo difficile, troppo costoso, poco conveniente o in generale meno dannoso. Funziona anche quando non è sufficiente dichiarare fuorilegge un hack, ed è pertanto necessario rendere più arduo attuarlo.

La seconda è la lungimiranza. Insegnare alle persone come funziona la truffa del business email compromise consentirà loro di riconoscerlo e magari di non cascarci con tutte le scarpe. È così che ci difendiamo da truffe telefoniche e via email che non vengono bloccate dai filtri automatici, e da "hack" cognitivi che sfruttano pregiudizi quali la paura e il rispetto per l'autorità.

L'ultima opzione è l'uso di un sistema supplementare che riesca a mettere in sicurezza il sistema vulnerabile. Nel caso del business email compromise, un'azienda potrebbe richiedere che ogni trasferimento di grosse cifre di denaro venga approvato da almeno due persone. In tal modo, anche se l'hacker riesce a ingannare un impiegato, non avrà raggiunto il suo obiettivo.

Si parla spesso di questa opzione nel caso dei device IoT. Ma si teme che presto le nostre case e le nostre reti possano riempirsi di device IoT vulnerabili. Una soluzione è inserire tali device in una rete in grado di riscontrarne la presenza e limitarne i comportamenti in caso di minaccia hacker. Ad esempio: il router di casa nostra potrebbe riuscire a rilevare i device IoT e a bloccarli quando fanno cose impreviste (il frigorifero che invia email di spam, genera criptovalute o prende parte a un attacco DoS, *denial-of-service*).

Un terzo tipo di difesa è rilevare un hack e porvi riparo dopo che è avvenuto. Nel 2020, il servizio di intelligence russo Svr ha hackerato i server di aggiornamento di SolarWinds, uno sviluppatore di software per il management delle reti con più di 300mila clienti in tutto il mondo, comprese la quasi totalità degli appartenenti alla lista *Fortune 500* e buona parte del governo Usa. L'Svr ha installato una *backdoor* in uno degli aggiornamenti di Orion, un prodotto di SolarWind, e si è messo in attesa.

Fermiamoci un attimo. Qualche pagina fa ho spiegato come la prima difesa dell'industria informatica dall'hacking siano le patch. L'Svr ha hackerato il processo di patching dell'azienda, per poi

inserire una backdoor in uno degli aggiornamenti. Più di 17mila clienti di Orion hanno scaricato e installato l'aggiornamento hackerato, consentendo all'Svr l'accesso ai loro sistemi. L'Svr ha scardinato lo stesso processo di cui vorremmo che tutti si fidassero per migliorare la propria sicurezza. È come nascondere le truppe da combattimento nei mezzi della Croce Rossa in tempo di guerra, anche se non è così universalmente condannato (e proibito dal diritto internazionale). L'hack non è stato scoperto dall'Nsa o da qualsiasi altra agenzia governativa statunitense, bensì dalla società di sicurezza FireEye durante una dettagliata verifica dei propri sistemi.

Dopo essere entrati in tutti questi sistemi, gli agenti Svr sono stati in grado di stabilire nuovi canali di accesso non legati alla vulnerabilità di SolarWinds. Quindi, anche dopo che le società-target hanno installato le patch nei loro software e risolto i problemi dell'aggiornamento che ha permesso ai russi di inserire la vulnerabilità la prima volta, tutte le reti violate restavano ancora vulnerabili in diversi modi probabilmente sconosciuti. L'unico modo per riconquistare la sicurezza sarebbe stato quello di buttare via tutto l'hardware e il software e ricominciare da zero. Nessuna organizzazione lo ha fatto e scommetterei che queste reti potrebbero ancora essere manipolate da Mosca.

Da una cosa del genere possiamo imparare una serie di lezioni. Innanzitutto che la diagnostica può essere difficile. A volte gli hack possono essere colti sul fatto, ma in genere bisogna affrontarli a posteriori, dopo averli rilevati tramite una verifica. In secondo luogo, un hack può essere tanto devastante da rendere qualunque reazione insufficiente. Infine, ci sono hack dai quali è impossibile riprendersi, e non si può far altro che cercare di mettere in sicurezza il sistema in previsione dell'hack successivo.

Un ultimo tipo di difesa è quello di scovare le vulnerabilità prima che vengano sfruttate. *Red-teaming* significa hackerare i propri sistemi. Ci sono aziende specializzate in analisi del genere; lo può fare però anche un team di sviluppatori, come parte del controllo di qualità. Il red team affronta il sistema come se fosse un gruppo di hacker esterni. Scova una serie di vulnerabilità – nel mondo informatico è inevitabile – e ci mette le giuste patch prima di

diffondere il software. È un'idea ripresa dall'esercito. La community della cybersicurezza usa il termine in senso lato per indicare un gruppo di persone addestrate a pensare come il nemico e a trovare le vulnerabilità dei sistemi.[1] Questa definizione più ampia è a sua volta stata ripresa dagli strateghi militari ed è ora parte del pensiero tattico militare e della progettazione dei sistemi. Il dipartimento della Difesa americano – soprattutto per quanto riguarda la sicurezza nazionale – da tempo ha integrato il red teaming nei suoi processi di pianificazione strategica. Il Defense Science Board ha scritto:

> Riteniamo che il red teaming sia estremamente importante per il dipartimento della Difesa. [...] Abbiamo bisogno di red team aggressivi che mettano alla prova i nuovi piani operativi, per scoprirne le debolezze prima dei nostri avversari reali.[2]

Senza red team, ci si dovrà affidare al nemico per scoprire le vulnerabilità dei propri sistemi. Ma in tal caso, come fare in modo che tali vulnerabilità vengano eliminate e non sfruttate? Nel mondo informatico, significa trasformare l'hacking in un crimine, in modo che gli hacker evitino di sfruttare le proprie scoperte. Certo, un hacker che scova una vulnerabilità avrà sempre la tentazione di approfittarne, ma con la consapevolezza di rischiare la galera. C'è anche chi vende la scoperta ad altri criminali, sul mercato nero o grigio.

Un incentivo di segno opposto può essere costituito dai *bug bounties*: le aziende di software mettono una taglia sulle vulnerabilità, elargendo premi in denaro a chi sarà in grado di scovarle. Lo scopo è convincere gli hacker a segnalare i bug all'azienda e non a soggetti malintenzionati. Si tratta di un incentivo potenzialmente efficace, per quanto in genere un hacker guadagni molto di più rivolgendosi a fabbricanti di *cyberweapon* o a qualsivoglia criminale.

A ogni modo, più si conosce un sistema, più è semplice scovare nuove vulnerabilità, specialmente se si ha accesso al codice sorgente, decifrabile dagli esseri umani, e non solo all'object code, leggibile solo per i computer. Proprio come è più semplice scoprire le

vulnerabilità di un regolamento se se ne ha a disposizione una copia e non ci si limita ad avere qualche informazione sulla stesura di regolamenti.

1. University of Foreign Military and Cultural Studies Center for Applied Critical Thinking (5 ottobre 2018), *The Red Team Handbook: The Army's Guide to Making Better Decisions*, US Army Combined Arms Center, https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf.
2. Defense Science Board (settembre 2003), *Defense Science Board Task Force on the Role and Status of DoD Red Teaming Activities*, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, https://apps.dtic.mil/sti/pdfs/ADA430100.pdf.

CAPITOLO 13

Prevenire potenziali hack in fase di progettazione

AutoRun arrivò con Windows 95. Prima, quando si acquistava un software su CD-Rom, bisognava digitare manualmente uno script per installarlo. Con AutoRun, bastava inserire il disco nel computer, e il sistema avrebbe ricercato automaticamente lo script di installazione. In tal modo l'installazione di un software divenne molto più semplice per l'utente medio, a digiuno di tecnologia.

Sfortunatamente, questa caratteristica venne sfruttata anche dai creatori di virus per installare malware sui nostri sistemi. Il virus se ne stava in agguato su un CD-Rom apparentemente innocuo – e in seguito su una pen-drive Usb – e veniva eseguito automaticamente quando l'ignaro utente lo inseriva nel computer. Ecco perché i computer ci mettevano in guardia dal collegare pennette Usb sconosciute. In questo caso la vulnerabilità non derivava da un errore, ma dal tentativo di trovare un equilibrio tra sicurezza e usabilità. Il bilancio nel 1995 sicuramente sarà apparso positivo, ma già un decennio dopo non lo era più. In seguito a una valanga di segnalazioni di problemi di sistema dovuti all'AutoRun, nel 2011 Microsoft si decise a riprogettare il sistema: su Windows Vista disabilitò AutoRun per pennette, drive esterni e altri media, consentendolo solo per un media sempre più obsoleto quale il Dvd.

Tutto questo per dire che in fase di progettazione non ci si può difendere del tutto dagli hack, in quanto 1) l'ottimizzazione di un sistema ha anche altri obiettivi oltre alla sicurezza e 2) coi cambiamenti della società e della tecnologia cambiano anche tecniche, obiettivi e bersagli degli hacker. I progettisti devono riconsiderare i propri assiomi di partenza su come un sistema va organizzato e fatto funzionare. Quella che oggi è un'ottima architettura presto potrebbe rivelarsi deleteria e facile da sfruttare per gli hacker.

Cercare di creare sistemi con meno vulnerabilità è meglio che

andare a caccia di vulnerabilità in un sistema prima che vengano hackerate. Ovvero, *bisogna assicurarsi in primo luogo che le vulnerabilità non esistano*. Nel gergo della sicurezza informatica, si parla di design sicuro, o *security by design*. Più facile a dirsi che a farsi. Il codice informatico è una questione complessa, ed è impossibile trovare tutte le vulnerabilità in agguato. I comuni mortali non possono produrre software privi di bug o perfino di vulnerabilità. Non disponiamo di una teoria della security by design, e ancor meno di una metodologia. Il motivo principale di questi difetti sta però nel fatto che la scrittura di un codice sicuro e affidabile è di per sé lenta, ardua e costosa, e mancano gli incentivi economici per intraprendere un'impresa simile. Con eccezioni rilevanti come quelle che riguardano aerei e shuttle, i software vengono scritti in fretta e furia.

Ci sono comunque principi di progettazione che riescono a minimizzare il numero di vulnerabilità e la possibilità di sfruttarle.

Semplicità: più un sistema è complesso, più è vulnerabile. Questo accade per moltissime ragioni, ma soprattutto perché in un sistema complesso ci sono più cose che possono andare storte. Un grattacielo offre più vulnerabilità di una villetta. L'antidoto in questo caso è la semplicità. Certo, molti sistemi sono complessi per natura, ma tendere alla semplicità favorirà senz'altro la sicurezza.

Protezione profonda: fare in modo che una singola vulnerabilità non permetta di distruggere l'intero sistema. Nei sistemi informatici, lo vediamo in genere nella autentificazione multifattore. I sistemi migliori non si limitano a chiedere solo un nome e una password – creando un unico punto vulnerabile – ma richiedono di autentificarsi in più modi. La mia email, ad esempio, sfrutta la sicurezza supplementare offerta da Google Authenticator. Si tratta di una app collegata a qualcosa che porto sempre con me: il mio smartphone. Per accedere al mio account, devo sbloccare il telefono, aprire la app e digitare un codice supplementare temporizzato. Altri sistemi multifattore possono includere elementi biometrici come l'impronta

digitale o un piccolo device Usb da inserire nel computer.

Fuori dall'ambito informatico, la difesa in profondità è qualcosa in grado di impedire a una sola vulnerabilità di dare il via libera a un hack distruttivo. Pensiamo a chi aggiunge una serratura blindata alla porta di casa o ai doppi sbarramenti di filo spinato fuori dalle basi militari, o alla richiesta di approvazione da parte di due persone per le transazioni finanziarie che superano un certo ammontare. Anche se un hack supera una delle due difese, difficilmente potrà aggirare anche l'altra.

Compartimentazione (isolare/separare le mansioni): le più efficienti organizzazioni terroristiche si suddividono in piccole cellule. Nessuna sa tutto delle altre, pertanto, nel caso venga compromessa, le altre restano al sicuro. È un esempio di compartimentazione, in grado di limitare gli effetti dei singoli attacchi. Per lo stesso motivo, uffici diversi hanno chiavi diverse, e vari account hanno differenti password. La compartimentazione viene definita talvolta anche come "principio del minimo privilegio": attribuire solo accessi e privilegi necessari al completamento di un lavoro. Per questo non abbiamo la chiave di tutti gli uffici del nostro posto di lavoro: non ci serve. Nelle reti informatiche si parla di "segmentazione": le singole parti di una rete vengono separate dalle altre, in modo che l'hack contro una di esse non si traduca in un hack contro l'intero network. È l'identico *modus operandi* delle cellule terroristiche. Una volta entrato in un network, un aggressore cercherà per prima cosa di violarne la segmentazione. Una buona segmentazione avrebbe impedito all'Svr russo di sfruttare il proprio accesso a SolarWinds per infiltrarsi in altre parti del network e installare altri malware e backdoor.

Un concetto del genere lo si può applicare facilmente anche alle reti sociali. Si riflette nell'idea che chi ha ruoli governativi non debba avere interessi finanziari nel settore industriale che supervisiona (negli Usa questo principio viene costantemente violato, governo e industria sono contigui). Oppure nell'idea che a creare i collegi elettorali non dovrebbero essere figure elette in grado di trarre vantaggio dalla manipolazione dei collegi stessi.

Fail-safe / fail-secure: tutti i sistemi si guastano, per caso, per un errore o in seguito a un attacco. Ci interessa però che lo facciano in modo più sicuro e senza conseguenze possibili. A volte è semplice, pensiamo al dispositivo vigilante sui treni, detto anche "uomo morto": se il conducente perde i sensi, il treno smette di accelerare e rallenta fino a fermarsi. A volte è più complesso: le rampe di lancio dei missili nucleari sono dotate di ogni sorta di meccanismo fail-safe, per evitare il lancio accidentale di una testata nucleare.

Anche i sistemi sociali possono prevedere meccanismi fail-safe. Pensiamo a molte delle nostre leggi. A prescindere dal sistema usato, anche se si escogita un hack ingegnoso per attuarlo, l'omicidio è sempre illegale. La Alternative Minimum Tax, in vigore negli Stati Uniti, è stata ideata come fail-safe: una tassa minima da pagare a prescindere da qualunque scappatoia si potesse scoprire (non ha funzionato, a dimostrazione di come sia difficile attuare meccanismi del genere).

Queste contromisure sono in grado ovviamente anche di ridurre l'efficacia di un hack. In questi capitoli non sto dicendo niente di nuovo, si tratta di cose delle quali mi sono già occupato nel mio libro del 2000 *Secrets and Lies*[1] e delle quali hanno scritto molti altri prima e dopo di me. Comprendere le basi di una progettazione sicura è però fondamentale per limitare l'efficacia dell'hacking. Più riusciamo a incorporare i principi fondamentali della sicurezza in fase di progettazione, più saremo al sicuro dall'hacking. Le aziende usano o meno queste tecniche a seconda dell'economia del loro settore. Possiamo immaginare che Apple e Microsoft per la sicurezza del loro software spendano più di quanto spende lo sviluppatore di un gioco, e chi crea il software di aerei, auto e attrezzature mediche investa di più di chi crea il software di giocattoli programmabili. È intuitivo, e in genere corrisponde al vero.

1. Bruce Schneier (2000), *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons.

CAPITOLO 14

Difendersi dagli hacker: gli aspetti economici

Nel 1971, una persona che aveva acquistato un biglietto a nome "Dan Cooper" hackerò un Boeing 727. Si servì della scaletta per l'imbarco in un modo ingegnoso che non era stato previsto dai progettisti: dirottò l'aereo, si fece consegnare 200.000 dollari, e mentre l'aereo era in volo, aprì la scaletta e si lanciò col paracadute. Non lo trovarono mai. In tanti cercarono di imitarlo, finché Boeing modificò il 727, togliendo la scaletta sotto la coda, e rendendo così impossibile lanciarsi da un aereo commerciale in volo. Si trattò di una patch efficace ma costosa. Ma per quale motivo quegli aerei presentavano una simile vulnerabilità? Forse Boeing non aveva previsto quel tipo di rischio, o aveva pensato che fosse troppo improbabile da doversene difendere.

Nella progettazione dei sistemi si parla di *threat modeling* quando si elencano tutte le potenziali minacce che possono colpire un sistema.[1] Immaginiamo che il sistema sia casa nostra, e proviamo a elencare tutti gli oggetti di valore che possediamo: dispositivi elettronici di lusso, cimeli di famiglia, un Picasso originale, le persone che vivono con noi. Possiamo poi fare un elenco di tutti i modi in cui qualcuno potrebbe entrare: una porta lasciata aperta, una finestra spalancata, una finestra chiusa. Pensiamo inoltre a tutte le persone che potrebbero cercare di entrare: un topo d'appartamento, il figlio dei vicini, uno stalker, un serial killer. E poi ci sono i rischi dovuti a chi non deve nemmeno trovare un sistema per entrare, come un partner violento. Usando tutte queste informazioni, potremmo immaginare un modello di casa che tenga conto delle minacce rischiose e di quelle che si potrebbero ignorare, dell'impegno necessario per affrontare tali minacce e così via. Nel caso si possieda un Picasso, bisognerà inoltre immaginare un sistema di sicurezza domestico specifico per il mondo dei furti d'arte. Nel caso fossimo un capo di Stato sarà necessaria una diversa sicurezza,

così come se ci trovassimo a vivere in una zona di guerra.

Bisogna tenere conto di questi aspetti economici per capire come difendersi dagli hacker. Ipotizzare il costo di un hack, e il costo e l'efficacia di una determinata difesa, prima di effettuare un'analisi costi-benefici e decidere se ne vale la pena. In alcuni casi, è meglio evitare. Ci sono meccanismi di sicurezza per i bancomat che potrebbero ridurre hacking e truffe, ma che non vengono implementati per non infastidire i normali clienti. Si potrebbe richiedere lo scan delle impronte digitali o il riconoscimento facciale, ma in tanti la considererebbero una precauzione eccessiva. Se quelle persone reagissero smettendo di usare il bancomat, il danno economico sarebbe ancor maggiore.

Per capire gli hack e come difendersene, bisogna avere ben chiaro anche il concetto di "esternalità". In economia, una esternalità è l'effetto di un'azione che non ricade sul soggetto che l'ha messa in atto. Pensiamo al proprietario di una fabbrica che inquina un fiume. Anche se le persone a valle si ammalano, l'industriale può infischiarsene. La cosa non è però del tutto vera. A valle potrebbero vivere impiegati e clienti del proprietario della fabbrica. Gli ambientalisti potrebbero denunciarlo, la stampa potrebbe criticarlo, e l'opinione pubblica rivoltarsi contro di lui. Per chi si occupa di sistemi, l'inquinamento del fiume va visto comunque come un'esternalità.

L'hacking provoca esternalità. Ha un costo, che ricade però sul resto della società. Un po' come il taccheggio: gli altri clienti devono pagare un po' di più per pareggiare le perdite dei negozi e le loro spese per i dispositivi antifurto. Sappiamo già come risolvere i problemi causati dalle esternalità: trasformarli in problemi per il detentore del sistema che ha preso una determinata decisione. Ad esempio stabilendo regole che facciano ricadere i costi sul sistema. In un mondo ideale questa tecnica funzionerebbe a meraviglia, ma in realtà la sua efficacia dipende da come la legge viene applicata e da come vengono comminate le sanzioni. Dipende dagli avvocati e e dall'esito dei processi. Dipende dall'azione delle istituzioni, a sua volta determinata da chi è al potere, dai lobbisti che cercano di annacquare le regole, da chi finanzia le campagne elettorali e dalle

loro priorità. Dipende dai risultati di ricerche finanziate dall'industria e dall'università, che a loro volta possono influire sulle politiche da attuare. Dipende da quanto i cittadini sono consapevoli di stare pagando un costo, di chi ne è il colpevole e di come si potrebbe far ricadere tali costi su di lui.

I sistemi tecnici diventano meno sicuri quando cambia il tipo di minaccia. Fondamentalmente, un sistema viene progettato secondo le contingenze dell'epoca. Prima o poi le cose cambiano. Per un motivo o per l'altro, crollano le certezze di un tempo, e il sistema scivola verso l'insicurezza. Vulnerabilità un tempo di poco conto divengono cruciali, e viceversa. Gli hack diventano più o meno semplici, più o meno convenienti, più o meno diffusi.

Probabilmente l'esempio migliore è proprio internet. Potrà sembrare assurdo, ma internet non è stato progettato pensando alla sicurezza. A fine anni Settanta e nei primi anni Ottanta, non veniva *mai* usato per cose importanti, e per potervi accedere bisognava appartenere a un'istituzione di ricerca. I computer *mainframe* usati da più utenti e connessi a internet disponevano inoltre dei loro meccanismi di sicurezza. Per tali motivi, chi progettò internet si disinteressò alla sicurezza e preferì un protocollo più semplice. Ci sarebbe stato modo in seguito di pensare alla sicurezza.

Sappiamo tutti come è andata a finire. Le cose cambiano. La rete si è aperta a personal computer senza sicurezza, anche se i progettisti della rete presumevano che disponessero delle stesse difese dei vecchi mainframe. Il modo di utilizzare internet è del tutto mutato. Sono cambiate la sua velocità e la sua portata. La sua centralità. Hack un tempo insignificanti sono diventati decisivi. È cambiato il modello per valutare le minacce. Tutte le analisi di costi e benefici sono saltate.

Nel mondo della sicurezza, conosciamo bene i contesti dinamici. A quanto pare, ogni tot di anni, le cose cambiano, costringendo anche la sicurezza a tenersi al passo. Lo spam via email è più problematico di quello materiale per una mera questione economica: mandare una email costa molto meno che mandare una lettera.

Per mantenere la sicurezza in un contesto dinamico bisogna stare un passo avanti agli hacker, ed è per questo che ci dedichiamo alla

ricerca sulla sicurezza informatica: conferenze, riviste, programmi accademici, gare tra hacker. Ci scambiamo informazioni su quel che fanno gli hacker e sui modi migliori per difenderci. Cerchiamo di anticipare la comparsa delle vulnerabilità e i modi in cui gli hacker cercheranno di sfruttarle. Perché le leggi stiano al passo degli hacker, sono necessarie regole generali che consentano al governo di essere abbastanza flessibile da vietare nuovi hack e punire nuovi hacker. Nel 1986 venne approvato il Computer Fraud and Abuse Act, scaturito dalla preoccupazione che le leggi vigenti non riuscissero a coprire tutti i crimini informatici. Ad esempio stabiliva che fosse un crimine, tra le altre cose, accedere a un altro sistema senza autorizzazione, o restarvi oltre i limiti stabiliti da un accesso autorizzato. Una scelta di termini tanto vaga copre una grossa fetta degli hack informatici, al punto che la Corte Suprema degli Stati Uniti nel 2021 si è trovata a ridurne la portata. L'obiettivo generale di questa legge resta comunque quello di consentire alla giustizia di dire: "Ok, il sistema ti ha permesso di fare questa cosa, ma non prendiamoci in giro: è evidente che lo scopo del sistema non fosse questo, e lo sapevi bene. E pertanto quello che hai fatto è illegale".

Molti sistemi sociali sono in grado di mettere patch ai sistemi e alle regole generali. La questione è aperta: come gestire il ciclo di vita di un sistema non informatico? Con quale frequenza dobbiamo revisionare, ad esempio, le istituzioni democratiche e controllare se servono ancora al loro scopo? E nel caso non lo siano, che cosa fare?

Ogni qualche anno compriamo un laptop e uno smartphone nuovi, device sempre più sicuri. Come fare lo stesso con le istituzioni sociali?

1. Adam Shostack (2014), *Threat Modeling: Designing for Security*, John Wiley & Sons.

CAPITOLO 15

Resilienza

I sistemi di norme sociali sono diversi dai sistemi di regole. Il fatto che tu non debba hackerare una norma sociale fa parte della sua natura e se la hackeri la stai violando. Le norme sociali sono però informali e non codificate, e lasciano dunque maggiore spazio all'interpretazione. Chi vuole può pertanto sfidarne i limiti al fine di ottenere un certo esito. I sistemi di norme hanno bisogno di persone che rispondano agli attacchi e di conseguenza, evolvendosi, le norme sono sempre più a rischio di venire hackerate.

Pensiamo alla politica degli ultimi anni: Donald Trump è riuscito a piegare ai suoi voleri alcune norme sociali e politiche. In genere evito di usarlo come esempio, per non dare connotazioni politiche, in questo caso è però talmente calzante che non posso esimermi. La società dispone di meccanismi – in genere efficaci – per porre riparo alle violazioni lievi delle sue norme: la condanna dell'opinione pubblica, le bocciature politiche, la stampa, la trasparenza. Trump ha schiacciato tutti questi meccanismi. Sono scoppiati troppi scandali contemporaneamente. I meccanismi volti a rafforzare le norme di comportamento di chi è chiamato a servire il popolo hanno alzato bandiera bianca di fronte a un candidato come Trump. Le norme funzionano solo se sono previste conseguenze per chi le viola, ma la società non si è dimostrata in grado di tenere il ritmo degli attacchi. Trump ha superato ogni limite in mille direzioni allo stesso momento. In molti casi, ha demolito le norme preesistenti.

Può però anche succedere che un sistema di norme divenga più resiliente dopo essere stato sfidato. Le norme sociali sono implicite e flessibili; non c'è sistema che sia più aperto al cambiamento. Per sfidare e cambiare un sistema di norme sociali non servono soldi, competenze giuridiche o chissà quali tecnologie, anche se possono essere d'aiuto. Chiunque voglia farsi avanti e disponga della giusta piattaforma può contestare le nostre norme sociali e le aspettative

implicite che ne conseguono. Sfide del genere impongono alle norme non di infrangersi, ma di piegarsi ed evolversi.

Il concetto di resilienza è importante, e vale per tutto, dal corpo umano all'ecosistema planetario, dai sistemi organizzativi a quelli informatici. È l'abilità di un sistema di riprendersi dopo essere stato messo alla prova da un elemento di disturbo, come può essere anche un hack. Per favorire la resilienza, nella costruzione dei ponti non si punta sulla rigidità assoluta: una trave fissa si romperà in modo improvviso e devastante, mentre dei cavi sospesi lo faranno lentamente e dando avvisaglie sonore. Per lo stesso motivo le nostre menti e i nostri corpi trovano vari modi di adattarsi alle circostanze: i bravi tassisti conoscono almeno quattro modi per andare da un punto importante a un altro di una città; e la contea di Orange, in California, ora ha un governo funzionante anche dopo aver dovuto dichiarare bancarotta nel 1994.

Anche nella sicurezza si sta cominciando a badare alla resilienza, cercando di ottenere sistemi che presentino proprietà quali impenetrabilità, omeostasi, ridondanza, agilità, capacità di ridurre i danni e di riprendersi. I sistemi resilienti sono più sicuri di quelli fragili. Molti accorgimenti di sicurezza che abbiamo già incontrato nei capitoli precedenti riguardano la capacità di rendere un sistema sempre più resiliente agli attacchi hacker.

Vorrei soffermarmi su un'ulteriore cosa. Abbiamo parlato di difese dagli hacker soprattutto in forma astratta; non dobbiamo però dimenticare un interrogativo sempre presente: chi si sta difendendo da chi? Chi decide se un hack è benefico o meno? Chi si occupa della difesa? Fino a quando vale la pena di spendere soldi e darsi da fare per difendersi?

Finora vi ho presentato esempi relativamente diretti, nei quali la persona o l'organizzazione responsabili di un sistema si occupano anche della sua difesa. Ad esempio, il management di Microsoft deciderà se un particolare hack di Windows è un problema, e che cosa fare per limitare i danni. In genere, applicherà una patch. Se la patch non è facile da applicare, si troverà costretto a convivere per un po' con la vulnerabilità (come abbiamo visto nel caso di AutoRun). In alcuni casi, le patch per gli hack vengono applicate in men che non si

dica, in altri non accade mai. Ci sono inoltre hack ai quali viene consentito di sopravvivere solo perché combatterli sarebbe troppo costoso. Una azienda di carte di credito non fermerà una frode se stimerà che le perdite saranno meno dannose del costo della patch. Spesso i negozi decidono di non fermare i taccheggiatori che se la svignano con qualche prodotto rubato: i ladri potrebbero fare del male al personale, oppure una persona accusata per sbaglio potrebbe dare il via a beghe legali molto costose.

Costruire sistemi sociali e politici in grado di difendersi da soli dagli hack significa anche pensare all'equilibrio tra chi scrive le leggi e chi è chiamato ad applicarle tramite regole operative. Questi ultimi non sono direttamente responsabili del proprio operato verso i cittadini quanto i legislatori. D'altro canto, non sarebbe possibile chiedere al legislatore di considerare ogni dettaglio dell'applicazione di una legge prima di approvarla. Più il legislativo può delegare l'implementazione delle leggi all'esecutivo, più otterremo un sistema agile e resiliente agli attacchi degli hacker.

La difesa della società dall'hacking non riguarda solo chi ha progettato un determinato sistema. Riguarda la società intera, e in particolar modo chi tiene al suo progresso.

PARTE TERZA
L'HACKING DEI SISTEMI FINANZIARI

CAPITOLO 16

Hackerare il paradiso

Pentimento e redenzione erano pilastri del cattolicesimo medievale. Se peccavi, potevi fare ammenda e venire perdonato. Ma per l'espiazione dei peccati più gravi, spesso erano necessarie azioni impossibili. Quasi nessuno, dopo una vita di peccati, poteva guadagnarsi l'assoluzione andando in pellegrinaggio a Gerusalemme. Era possibile invece donare una bella sommetta perché qualcuno facesse il lavoro al posto tuo: un compromesso ragionevole e molto conveniente per la Chiesa. E così, se una cattedrale aveva bisogno di un nuovo tetto, un ricco peccatore avrebbe potuto far penitenza finanziandolo. In cambio avrebbe ricevuto una "indulgenza", un documento che al cospetto degli uomini e di Dio attestava che il peccato tal dei tali era stato rimesso. E fin qui ci siamo.

Uno schema del genere presentava però una vulnerabilità: le indulgenze erano un bene illimitato, e la chiesa lo sfruttò (exploit) utilizzandolo come valuta. L'intero sistema era regolato in modo molto lasco, pertanto nessuno poteva davvero limitare i sistemi di vendita delle indulgenze. La chiesa poteva stamparne a volontà, e i ricchi potevano comprarne tutte quelle che volevano. Entrarono in scena anche intermediari che corrompevano i vescovi per ottenere il diritto di rivendere le indulgenze. Fu così che un sistema nato per redimere le persone mise al centro profitto e potere.[1] Nel 1517, la vendita delle indulgenze spinse Martin Lutero a inchiodare le sue "Novantacinque tesi", ovvero la *Disputa sulle indulgenze*, sul portone della chiesa del castello di Wittenberg, in Germania, dando il via alla riforma protestante e a più di un secolo di guerre di religione.

Dovunque ci si possa arricchire, l'hacking non manca mai. E chi scova un hack remunerativo può riempirsi le tasche. Per questo i sistemi finanziari, come nessun altro sistema, si prestano tanto bene a essere hackerati (per farci soldi).

Johann Tetzel, un frate domenicano degli inizi del Sedicesimo

secolo, inventò due tipi di indulgenze molto innovativi:[2] indulgenze per gli amici morti, per "migliorare" il loro status nell'aldilà e farli passare dal purgatorio al paradiso,[3] e indulgenze che assolvevano dai peccati futuri, e non solo da quelli già commessi. Una sorta di carta "esci gratis dall'inferno".[4]

Malgrado le vibranti proteste dei teologi cattolici e di riformisti come Martin Lutero, la Chiesa non riuscì a bloccare queste pratiche perché era ormai dipendente dagli enormi profitti dovuti al commercio delle indulgenze: era paralizzata, incapace di reagire. Ad esempio le indulgenze vendute da Tetzel furono fondamentali per finanziare la costruzione della Basilica di San Pietro.

Tra gli hack che abbiamo già visto, molti sono stati disinnescati da chiunque fosse il responsabile del sistema in questione. Le compagnie aeree hanno aggiornato i regolamenti dei loro piani per i frequent flier. Le federazioni sportive hanno cambiato le regole del gioco. Di tanto in tanto accade però che un hack venga consentito, o perfino dichiarato legale. Un bastone da hockey ricurvo rende le partite più emozionanti. I casinò possono approfittare dei clienti che si illudono di poter contare le carte pur non essendone capaci.

Nel mondo finanziario, la normalizzazione di un hack è cosa molto comune. Chi gestisce le regole del gioco talvolta blocca i nuovi hack, ma è più probabile che li consenta, e magari li codifichi giuridicamente a posteriori. Questo è uno dei meccanismi mediante i quali i sistemi finanziari si rinnovano. I cambiamenti non vengono dai regolatori in forma di concessione, ma dagli utenti in forma di hack. La soluzione più scontata sarebbe quella di mettere una patch al sistema, ma spesso non è politicamente possibile. Le lobby dispongono di forza e potere sufficienti a cambiare le carte in tavola. Non significa che le patch non vengano mai messe, ma spesso ci vuole tempo. Solo nel 1567 papa Pio V revocò il permesso di concedere indulgenze che prevedessero transazioni finanziarie; in tal modo mise una patch al sistema ed eliminò l'hack.

I ricchi sono hacker potenti e il profitto è una buona motivazione per hackerare, oltre che per normalizzare un hacking.

1. Robert N. Swanson (2011), *Indulgences in Late Medieval England: Passports to Paradise?*, Cambridge University Press.
2. Ray Cavanaugh (31 ottobre 2017), "Peddling purgatory relief: Johann Tetzel", *National Catholic Reporter*, www.ncronline.org/news/people/peddling-purgatory-relief-johann-tetzel
3. Aveva perfino una sorta di slogan pubblicitario: "Quando cade il soldin nella cassetta, l'anima vola in cielo benedetta".
4. Off topic: la carta "Esci gratis di prigione" nel gioco del Monopoly può essere usata per hackerare la regola che non consente ai giocatori di prestarsi soldi a vicenda. Non vale molto, ma può essere venduta a un altro giocatore per qualunque somma, diventando un utile sistema per il trasferimento di valuta. Jay Walker e Jeff Lehman (1975), *1000 Ways to Win Monopoly Games*, Dell Publishing, www.lehman-intl.com/jeffreylehman/1000-ways-to-win-monopoly.html.

CAPITOLO 17

L'hacking bancario

Molte procedure del sistema bancario che oggi ci sembrano scontate sono nate come hack. Sono state infatti ideate da qualche soggetto potente per aggirare regolamenti limitanti e guadagnare di più. Non lo dico come una critica: l'hacking è un sistema per convincere chi governa a rivedere e aggiornare le regole.

Per gran parte del Ventesimo secolo, la Federal Reserve ha governato il sistema bancario statunitense tramite la Regulation Q. Emanata nel 1933, dopo la Grande Depressione, la Regulation Q si occupava di cose come i tassi di interesse per i diversi conti o i tassi per singoli clienti e aziende.

La Regulation Q è una misura di sicurezza.[1] Prima che venisse attuata, le banche erano in competizione l'una con l'altra per offrire i tassi di interesse più alti sui depositi. Tale competizione spingeva le banche a comportamenti rischiosi, pur di poter offrire il tasso migliore. I limiti della Regulation Q miravano pertanto a ridurre un rischio sistemico. La cosa ha funzionato per più di quarant'anni. Negli anni Settanta i tassi d'interesse si gonfiarono, e le banche cercarono disperatamente di aggirare la Regulation Q e di offrire tassi più alti per competere con altri tipi di investimento. Uno degli hack dei primi anni Settanta era il conto corrente Now, che stava per *Negotiable Order of Withdrawal* (ordine di prelievo negoziabile), e mirava a sfruttare la differenza tra conti in cui si poteva ritirare il denaro a piacimento (*demand deposit account*) e altri nei quali il denaro veniva depositato dal cliente per un periodo predeterminato (*term deposit account*). I conti Now avevano le sembianze del primo tipo, ma tecnicamente appartenevano alla seconda categoria. L'hacker che inventò il conto Now ha un nome: Ronald Haselton, presidente e Ceo della Consumer Savings Bank di Worcester, in Massachusetts. A quanto pare, Haselton ascoltò per caso una cliente che si chiedeva perché non potesse accedere ai suoi risparmi per

pagare tramite assegno. Haselton si pose la stessa domanda e hackerò la Regulation Q per creare il primo *checking account* che pagava interessi al cliente.

Un altro esempio di hacking bancario innovativo sono i certificati di deposito, o CD. Per questo hack fu necessario l'impiego di un intermediario mobiliare per creare un mercato secondario di CD, che potesse pertanto attrarre i conti aziendali. A immaginarlo furono alcuni impiegati della First National City Bank, oggi Citicorp. Nel 1961, la banca introdusse i certificati di deposito negoziabili, che pagavano un tasso di interesse più alto di quello consentito per i conti bancari, e cinque anni dopo li fece esordire nel mercato londinese. Poco dopo, la First National City Bank si riorganizzò come holding company per evitare che i regolamenti bancari le impedissero l'emissione di CD a tassi più alti.

Il congresso pose riparo a questo hack con un emendamento al Bank Holding Company Act del 1956, che assegnò al consiglio della Federal Reserve il compito di supervisionare e regolare le holding company delle banche.

Tra gli altri hack bancari di metà Ventesimo secolo ci sono i fondi del mercato monetario e i conti in eurodollari, pensati entrambi per aggirare le limitazioni normative dei tassi d'interesse per i conti tradizionali.

Si tratta di una serie di hack poi normalizzati, o dalla decisione del regolatore di non chiudere i loophole che li rendevano possibili, oppure dal Congresso, che – sopraffatto dalle richieste dei regolatori – si è deciso a legalizzarli. Ad esempio, i conti Now sono stati legalizzati inizialmente in Massachusetts e nel New Hampshire, poi nel New England, e infine a livello nazionale nel 1980.[2] Molte altre limitazioni imposte dal Bank Holding Company Act sono state abrogate dall'approvazione del Riegle-Neal Interstate Banking and Branching Efficiency Act del 1994. Era tutto parte di una grande ondata di deregulation del settore bancario proseguita anche all'inizio del nuovo millennio. Questo è lo schema base, e come vedremo, tende a ripetersi.[3]

Il governo, imponendo regole, limita i danni che i banchieri possono arrecare all'economia. Queste regole riducono i profitti delle

banche, che mettono in atto le loro contromosse: hackerano le regole con espedienti non previsti e non esplicitamente proibiti dai regolatori, e sfruttano tali hack per arricchirsi ulteriormente. Poi fanno il possibile per spingere i regolatori – e il governo stesso – sia a non mettere patch sia a normalizzare i loro hack. Un effetto collaterale sono le costose crisi finanziarie che colpiscono l'intera popolazione.

L'hacking continua ancora oggi. Il Dodd-Frank Wall Street Reform and Consumer Protection Act è stato approvato subito dopo la crisi finanziaria globale del 2008, con l'intenzione di ristrutturare radicalmente il sistema regolatorio finanziario. Il Dodd-Frank comprendeva una serie di regole per le banche volte ad aumentare la trasparenza, ridurre i rischi sistemici ed evitare un altro disastro finanziario. La legge regolamentava in particolare i derivati, dei quali spesso si era abusato e che erano stati un fattore decisivo per la crisi del 2008.

Il Dodd-Frank Act era pieno di vulnerabilità. Le banche scatenarono immediatamente i propri avvocati in cerca di hack per aggirare l'intento della legge, alla faccia dei rischi per l'economia. Per prima cosa si soffermarono su un passaggio che esentava le attività estere, a meno che non avessero "un collegamento diretto significativo con attività negli Stati Uniti o col commercio con essi". Quella vulnerabilità venne riparata, ma subito cavillarono sulla definizione di *branch* all'estero, diversa da quella di *affiliate*. Anche questo tentativo durò ben poco. Infine si tuffarono sulla parola *guarantee* (garanzia). In sintesi, tutti i derivati stranieri venivano garantiti dalla casa madre statunitense, che avrebbe coperto le perdite nel caso fosse accaduto qualcosa alle affiliate all'estero. Eliminando la parola "garanzia" e altri termini equivalenti dai loro contratti, le banche avrebbero aggirato tale regolamentazione.

Alla fine del 2014, con l'ennesimo hack per sfuggire al Dodd-Frank, le banche avevano già spostato off-shore il 95% del loro *swap trade*, in cerca di giurisdizioni meno severe.[4] Nel 2016, la Commodities Futures Trading Commission cercò di chiudere questo loophole. Stabilì che gli swap non potessero essere mandati all'estero per evadere il Dodd-Frank Act, e che sia gli swap garantiti sia quelli non

garantiti dovevano essere coperti dalla casa madre. La nuova regola non è stata però varata prima dell'insediamento del presidente Trump, e il presidente della commissione da lui nominato non si è mai premurato di farlo.

Altri hack prendevano di mira la Volcker Rule, un'altra parte del Dodd-Frank che impedisce alle banche di portare all'estero certi investimenti coi propri conti e allo stesso tempo limita le loro interazioni con hedge fund e private equity fund. Le banche si resero conto che avrebbero potuto aggirare la Volcker nel caso il denaro non fosse provenuto dai loro conti. Bastava stabilire varie partnership attraverso le quali investire. Questa regola venne abrogata durante l'amministrazione Trump, rendendo inutili molti degli hack. Infine le banche capirono di poter aggirare tutte le regole sui conti di trading previste dal Dodd-Frank affermando che fossero finalizzati alla cosiddetta "gestione della liquidità".

Gli hack bancari sono un perfetto esempio di una cosa sulla quale torneremo più volte. Banche e regolatori giocano incessantemente come il gatto col topo. I regolatori devono porre un freno a comportamenti irresponsabili, aggressivi e corrotti. Le banche cercano di guadagnare quanto più possibile. I loro obiettivi sono contrastanti, per questo le banche cercano di hackerare il sistema non appena possibile. Una banca che non cercasse di farlo verrebbe schiacciata dalle altre. La possibile applicazione di patch – l'intervento più scontato – viene intralciata dal tentativo estremamente aggressivo da parte delle banche di normalizzare le nuove situazioni che si vengono a creare. È un tentativo messo in atto tramite le lobby e la *regulatory capture*: un organismo di regolamentazione diviene preda del settore che sta cercando di regolare e finisce per servire le aziende invece che l'interesse pubblico. Il settore bancario arriva perfino a hackerare lo stesso processo legislativo. Il settore dei servizi finanziari, tra il 1998 e il 2016, ha speso 7,4 miliardi di dollari in attività di lobbying, 1,2 miliardi dei quali provenienti dalle sole banche.[5]

Se non è possibile mettere patch, bisogna scovare le vulnerabilità prima che vengano hackerate, e soprattutto prima che vengano inglobate dal sistema e che le lobby facciano pressioni per

normalizzarle. Nei sistemi finanziari, le agenzie governative possono attuare il red teaming, reclutando esperti di finanza e di diritto in grado di studiare l'evoluzione dei sistemi, per migliorare le nuove regole mentre sono ancora delle bozze.

Ci sono alcuni paesi – Stati Uniti compresi, almeno per quanto riguarda alcune agenzie e alcuni casi specifici – che già lo fanno, e analizzano le nuove proposte normative tramite un *comment process*, un processo di valutazione pubblico:[6] lo scopo è capire come le regole potrebbero essere hackerate o come i progressi tecnologici a breve termine potrebbero permettere nuovi hack, per mettere patch preventive. Certo, così non si risolve del tutto il problema della regulatory capture, né tanto meno quello delle pressioni delle lobby sul legislatore, ma in tal modo questi potenti hacker possono limitare i danni che deriverebbero da una successiva chiusura dei loophole. I lobbisti possono inserirsi però anche nel comment process per fare in modo che i loophole non vengano chiusi, o addirittura ne vengano creati di nuovi. È però possibile che con l'adozione del comment process i lobbisti non debbano fare altro che spostare la mira dal proprio bersaglio al sistema che lo governa. Tale sistema deve pertanto dimostrarsi al contempo rapido e prudente per non diventare facile preda di chi lo vuole attaccare.

1. R. Alton Gilbert (Feb 1986), "Requiem for Regulation Q: What it did and why it passed away", Federal Reserve Bank of St. Louis, https://files.stlouisfed.org/files/htdocs/publications/review/86/02/Requiem_Feb1986.pdf.

2. Joanna H. Frodin e Richart Startz (giugno 1982), "The NOW account experiment and the demand for money", *Journal of Banking and Finance* 6, n. 2, www.sciencedirect.com/science/article/abs/pii/0378426682900322; Paul Watro (10 agosto 1981), "The battle for NOWs", Federal Reserve Bank of Cleveland, www.clevelandfed.org/en/newsroom-and-events/publications/economic-commentary/economic-commentary-archives/1981-economic-commentaries/ec-19810810-the-battle-for-nows.aspx.

3. Ne ha parlato Hyman Minsky, pur non usando mai la parola "hacking": Hyman Minsky (maggio 1992), "The financial instability hypothesis", Working Paper n. 74, The Jerome Levy Economics Institute of Bard College, www.levyinstitute.org/pubs/wp74.pdf.

4. Charles Levinson (21 agosto 2015), "U.S. banks moved billions of dollars in trades beyond Washington's reach", *Reuters*, www.reuters.com/investigates/special-report/usa-swaps; Marcus Baram (29 giugno 2018), "Big banks are exploiting a risky Dodd-Frank loophole that could cause a repeat of 2008", *Fast Company*, www.fastcompany.com/90178556/big-banks-are-exploiting-a-risky-dodd-frank-loophole-that-could-cause-a-repeat-of-2008.

5. Deniz O. Igan e Thomas Lambert (9 agosto 2019), "Bank lobbying: Regulatory capture and beyond", *IMF Working Paper* n. 19/171, International Monetary Fund, www.imf.org/en/Publications/WP/Issues/2019/08/09/Bank-Lobbying-Regulatory-Capture-and-Beyond-45735.

6. Molte istituzioni normative del settore bancario in alcune occasioni consentono di esprimere la propria opinione al riguardo: si vedano l'Office of the Comptroller of the Currency, www.occ.treas.gov/about/connect-with-us/public-comments/index-public-comments.html, e il Consumer Financial Protection Bureau (ultimo aggiornamento 7 aprile 2022), "Notice and opportunities to comment", www.consumerfinance.gov/rules-policy/notice-opportunities-comment.

CAPITOLO 18

L’hacking degli scambi finanziari

Anche i mercati azionari, quelli delle commodity e gli altri sistemi di trading finanziario si prestano a essere hackerati. Questo sin dalla loro invenzione, e ancor di più dopo che tali sistemi sono stati computerizzati e automatizzati.

In quest’ambito, gli hacker mettono nel loro mirino l’informazione. Quando uno scambio finanziario funziona a modo, i trader che dispongono delle migliori informazioni ottengono risultati migliori, riuscendo a comprare a meno e a vendere quando le quotazioni salgono. Gli hack sovvertono tale meccanismo fondamentalmente in due modi. In primo luogo, sfruttano informazioni ancora non diffuse per fare affari prima degli altri. In secondo luogo, diffondono false informazioni e riescono a guadagnare prima che gli altri si accorgano di essere stati turlupinati. Sono due hack che minano l’equità del mercato: il concetto che l’accesso alle informazioni sul mercato sia uguale per tutti gli investitori.

L’hack del primo tipo più diffuso è l’insider trading, illegale da talmente tanto tempo da non poter nemmeno più essere considerato un hack. In genere si fa insider trading acquistando o vendendo titoli sulla base di informazioni non note al pubblico. L’insider può essere un direttore finanziario (Cfo) a conoscenza dei dati sulle vendite della sua azienda prima che vengano diffuse, il PR che si occupa di stilare il rapporto finanziario o addirittura lo stampatore che legge il rapporto prima di pubblicarlo. L’insider trading fa due tipi di danni: 1) penalizza chi non dispone delle stesse informazioni e 2) crea sfiducia nei confronti del mercato.

Negli Usa, l’insider trading è stato messo fuorilegge dal Securities Exchange Act del 1934, poi ribadito e corretto nel corso degli anni dalle sentenze della Corte Suprema. Nel 2021, tre persone sono state accusate di insider trading[1] per l’acquisto di azioni della Long Island Iced Tec Co. prima che cambiasse il nome in Long Blockchain Co.

semplicemente per seguire la moda delle blockchain, che impazzava in quel periodo. Una norma tanto duratura è un perfetto esempio di patch efficace.

È davvero sorprendente che tale divieto sia sopravvissuto a novant'anni di hack e di inerzia dei regolamenti. La lezione è che una norma ampia genera un sistema solido, adattabile e resiliente. La semplicità di una regola minimizza le vulnerabilità di progettazione (abbiamo visto quanto invece sia vulnerabile una legge come il Dodd-Frank Act). Secondo Arthur Levitt, ex presidente della Securities and Exchange Commission (Sec), "una maggiore specificità consentirebbe agli avvocati di trovare più sistemi per aggirarla. [La Sec e il dipartimento della Giustizia] hanno volutamente fatto in modo che queste leggi fossero vaghe, per poterle applicare ad ampio raggio".[2] Le regole sull'insider trading sono pertanto volutamente generiche per prevenire ulteriori tentativi di hacking.

Un altro tipo di hacking basato sull'accesso a informazioni segrete è il *front running*. Se sei un broker, e sei a conoscenza di un grosso scambio imminente, prima che avvenga puoi approfittarne per scambiare qualche azione per conto tuo. Solo in seguito effettuerai la transazione per il cliente. Il mercato si muove e tu ne ricaverai un profitto immediato. Come l'insider trading, anche il front running è stato dichiarato illegale.

Alcuni hacking dei network e dei mercati finanziari prendono di mira i loro sistemi informativi. Ad esempio, nel 2015, la Sec ha incriminato due hacker ucraini che erano entrati nelle reti di Business Wire e PRNewswire,[3] rubando più di 100mila comunicati stampa di società quotate sul mercato che non erano ancora stati diffusi. Gli hacker li avevano poi distribuiti a una rete di trader, che aveva sfruttato le informazioni per puntare o meno sulle azioni di quelle società, in una sorta di insider trading.

Il secondo tipo di hack si basa sulla diffusione di informazioni false. Un vecchio esempio ci è dato dal *pump-and-dump*: si comprano azioni, in genere di un'azienda poco nota (il mercato delle cosiddette *penny stock*, le azioni di piccole società con quotazione inferiore 5 dollari, è celebre per il pump-and-dumping); poi si consigliano le stesse azioni ad altre persone, millantando possibili

profitti. Se qualcuno ci casca, il prezzo sale ed è possibile vendere le proprie azioni. Una volta questo sistema prevedeva una serie di telefonate ai potenziali investitori. Oggi si svolge invece sui forum online, sui social media e tramite spam. Dagli agitatori del forum finanziario di Reddit r/WallStreetBets, che hanno fatto arrivare "alle stelle" il prezzo di GameStop, fino a Elon Musk, che ha raccontato ai suoi milioni di follower su Twitter di aver comprato bitcoin, gli investitori possono usare internet per manipolare le aspettative altrui e produrre bolle molto remunerative per loro (e dannose per gli altri), con numeri e rapidità senza precedenti. L'avvento del trading online ha reso particolarmente vantaggioso questo tipo di hack. Il pump-and-dump è generalmente illegale, con grosse multe per chi viene beccato, ma perseguirne i colpevoli può essere molto difficile. Non ci sono state conseguenze né per Elon Musk né per le persone coinvolte con l'affare GameStop del 2021.

Un altro tipo di hack basato sulla disinformazione è lo *spoofing*, nel quale un trader fa ordini per milioni di dollari e poi li cancella subito dopo che gli altri trader se ne sono accorti e hanno reagito di conseguenza. Anche lo spoofing è illegale, ma allo stesso modo ben poche persone hanno dovuto risponderne legalmente.

Tra gli hack basati sulla disinformazione, si diffonde sempre più anche il metodo delle fake news, notizie volutamente fuorvianti camuffate da giornalismo. È un hack spesso usato per dire il falso sul valore di un'azienda, e permettere agli hacker di sfruttare le fluttuazioni dei suoi prezzi azionari. Nel 2015, ad esempio, una falsa versione di Bloomberg.com venne usata per diffondere la notizia di un'offerta di 31 miliardi di dollari per l'acquisto di Twitter. Mentre la notizia si diffondeva, il prezzo delle azioni di Twitter salì alle stelle, permettendo agli hacker di vendere le proprie quote a prezzi gonfiati artificialmente. Il sito fake ricalcava il reale Bloomberg.com, e usava un url molto simile.

Per gli stessi scopi sono stati usati falsi comunicati stampa, falsi giornalisti, falsi tweet e perfino falsi rapporti della Sec. La Sec considera tutte queste cose illegali.

Pensandoci bene, la disinformazione non hackera tanto i mercati finanziari quanto gli altri trader. È un tentativo di influenzarne i

comportamenti. Sono tutti esempi di hack al nostro sistema cognitivo.

Tra gli altri hack al sistema finanziario c'è l'uso di nuovi sistemi per la riduzione del rischio, basati in genere su loophole nei regolamenti finanziari. Lo vediamo negli hedge fund, che hanno questa funzione sin da quando sono stati lanciati negli anni Sessanta, prima attraverso la "copertura", o la compensazione, di rischi contrapposti, poi tramite l'impiego di varie strategie di investimento e infine tramite il trading informatico. L'esistenza stessa degli hedge fund si basa su un hacking del sistema che regola la finanza. Gli hedge fund sono stati storicamente protetti da una serie di loophole legislativi che li mettevano al riparo dalla supervisione della Sec. Gli hedge fund accettano come clienti solo investitori istituzionali o particolarmente ricchi, e sono pertanto esclusi dalla supervisione prevista dal Securities Act del 1933, volta a proteggere i piccoli risparmiatori che si muovono sul mercato. Gli hedge fund rientrano nei criteri stabiliti dall'Investment Company Act del 1940, e pertanto non sottostanno ai divieti su tecniche – quali lo *shorting* – vietate invece alle società d'investimento registrate. Il Dodd-Frank Act nel 2010 ha sottoposto gli hedge fund alla supervisione della Sec, ma continuano comunque a essere per larga parte non regolati. Gli hedge fund sono diventati una parte accettata del sistema finanziario. Nel corso dei decenni, hanno sfruttato un loophole giuridico dopo l'altro, che a volte vengono chiusi solo dopo che chi li aveva scoperti era riuscito a guadagnare un sacco di soldi. A volte si cambiano le regole per legittimare un determinato hack. La cosa più frequente è che un hack venga semplicemente usato e poi accettato come una cosa normale. Non è detto che chi sfrutta gli hedge fund sia più furbo degli altri. Semplicemente capisce meglio il sistema ed è più bravo a individuarne le vulnerabilità, trovando anche il modo per sfruttarle. Visto che i maggiori esperti del sistema sono quelli che approfittano degli hack, è difficile aspettarsi delle patch nel breve termine.

Si tratta di un hacking relativamente complesso, diretto a più sistemi a diversi livelli di generalità. Ci sono hack che avvengono a livello tecnico: spoofing e front running sfruttano l'automazione e la

velocità dei computer. Altri hack avvengono al livello dei mercati finanziari. Altri ancora a livello legislativo: pensiamo alle vulnerabilità delle leggi sugli investimenti in Borsa. È un microcosmo di hack che vedremo meglio nei capitoli seguenti.

1. US Securities and Exchange Commission (9 luglio 2021), “SEC charges three individuals with insider trading”, www.sec.gov/news/press-release/2021-121.
2. Redazione di Knowledge at Wharton (11 maggio 2011), “Insider trading 2011: How technology and social networks have ‘friended’ access to confidential information”, *Knowledge at Wharton*, https://knowledge.wharton.upenn.edu/article/insider-trading-2011-how-technology-and-social-networks-have-friended-access-to-confidential-information.
3. US Securities and Exchange Commission (11 agosto 2015), “SEC charges 32 defendants in scheme to trade on hacked news releases”, www.sec.gov/news/pressrelease/2015-163.html.

CAPITOLO 19

L'hacking degli scambi finanziari computerizzati

Ormai tutti gli scambi finanziari sono computerizzati, consentendo innumerevoli nuovi hack.[1] Ad esempio oggi è molto più facile mettere in atto il front running, così come è molto più difficile individuarlo. Collegare il trading automatizzato alla *sentiment analysis* – al punto che i programmi di trading comprano quando un'azione diviene un meme, o vendono quando una cattiva notizia diventa virale – permette di fare più soldi col pump-and-dump e la diffamazione. Il più devastante degli hack moderni è però l'*high-frequency trading*, o Hft. L'Hft non sfrutta informazioni segrete né diffonde informazioni false, e si serve invece di informazioni pubbliche alla velocità della luce. Si tratta infatti di un tipo di trading algoritmico che sfrutta i differenziali di prezzo dovuti a forti ordinazioni, in genere effettuate dai fondi pensionistici o dalle compagnie assicurative (grossi ordini che possono influenzare notevolmente i prezzi delle azioni). Gli algoritmi Hft individuano questi ordini e altri eventi in grado di influenzare i prezzi, e ne approfittano. Si chiamano scambi "ad alta frequenza" in quanto cercano di "comprare a poco e vendere a tanto" alla velocità della luce, sulla base di minuscole fluttuazioni dei prezzi. Spesso gli scambi avvengono nel giro di millisecondi o microsecondi, tanto che le società cercano di ottenere server fisicamente vicini a dove avvengono, per massimizzare la velocità di internet. Proprio come i cani sono in grado di sentire frequenze troppo alte per l'orecchio umano, gli algoritmi Hft riescono a riconoscere pattern impercettibili per una persona reale.

È un perfetto esempio di hack. Se presumiamo che lo scopo del mercato sia lo scambio di denaro e beni tra compratori e venditori a un prezzo che entrambi considerano vantaggioso, gli Hft costituiscono un hack. Un Hft si serve infatti di riflessi inumani per racimolare soldi dal rumore di fondo del sistema. È un artefatto dei sistemi informatici usati per semplificare il trading. È qualcosa che

chi ha progettato il mercato non ha voluto e non ha previsto. Sovverte gli obiettivi del sistema per scopi privati. Si comporta in modo indubbiamente parassitico.

Un Hft non solo è sleale, ma crea anche nuovi rischi e nuove vulnerabilità all'interno del sistema. Nel 2010, il mercato azionario degli Usa crollò in un lampo, perdendo più di mille miliardi di dollari in trentasei minuti, prima di risalire. La causa non è stata mai scoperta, ma le proporzioni del crollo furono senza dubbio ampliate dagli Hft. Nel 2012, il Knight Capital Group perse 440 milioni di dollari per via di un difetto in un nuovo software che controllava gli Hft. Come dimostrano questi esempi, Hft e trading automatizzato, proprio per la loro velocità e la mole di denaro che spostano, possono rivelarsi più rischiosi del consueto trading umano. Inoltre gli Hft mettono in una posizione di evidente svantaggio chi non ha accesso ai sistemi di trading algoritmici.

A differenza di altri hack dei quali ci stiamo occupando, e malgrado la loro evidente scorrettezza, gli Hft sono stati normalizzati. Negli Usa, la Financial Industry Regulatory Authority ha stabilito alcune regole fondamentali per aumentare la trasparenza dei metodi alla base dei sistemi di trading algoritmico; l'Unione Europea ha adottato regole simili. Ma nessuno è riuscito a rallentare davvero l'uso di questa pratica.

Nel 2009-2010, al culmine della sua adozione, dal 60 al 70% degli scambi negli Usa veniva attribuito agli Hft. Un singolo cittadino può servirsi di un broker Hft per accedere a questi algoritmi, ma i trader Hft professionisti saranno sempre più bravi e più rapidi. Le società Hft possono pagare un extra per conoscere gli ordini in entrata una frazione di secondo prima del resto del mercato, ottenendo un ulteriore vantaggio sleale.

Un altro hack ad alta velocità è quello che sfrutta gli errori di battitura, piuttosto frequenti nel trading computerizzato. Gli errori più grossi fanno notizia, come quella volta che l'azienda giapponese Mizuho Securities Co. perse 225 milioni di dollari sul mercato azionario perché un dipendente, invece di scrivere che un'azione costava 610.000 yen, aveva messo sul listino 610mila azioni a uno yen l'una. Oppure quando un junior trader della Deutsche Bank per

sbaglio inviò 6 miliardi di dollari a un hedge fund per *fat-finger error*, un errore di digitazione. O ancora quando un trader della borsa di Tokyo perse 617 miliardi di dollari in azioni per aver premuto il tasto sbagliato, cancellando quarantadue diverse transazioni nello stesso istante: un altro problema di "dita tozze".

Questi non sono hack, sono errori. È però un hack fare ordinazioni pazze sperando che gli altri combinino pasticci. Fare un'offerta non costa niente, perciò è possibile hackerare il sistema inondandolo di offerte assurde. In genere scadranno senza essere evase, ma ci sono rarissimi casi nei quali un errore umano permetterà a queste offerte di generare profitti giganteschi.

Come difendersi in casi del genere? La flessibilità delle regole finanziarie rende possibile applicare le patch: si tratta infatti di regole volutamente ampie, pensate per offrire spazio alla discrezione di chi le applica. Tribunali e regolatori, in breve tempo e senza troppe difficoltà, possono vietare o stabilire nuove pratiche semplicemente interpretando o chiarendo le leggi già in vigore. L'efficacia delle patch viene però limitata dalla capacità degli hacker di normalizzare le proprie pratiche.

In quest'ambito è consigliabile il *secure systems design*. Possiamo progettare i nostri sistemi finanziari cercando di ridurre la volatilità dovuta all'high-frequency trading. In molti mercati ci sono dei "fusibili" che interrompono automaticamente il trading se i prezzi azionari cambiano oltre una determinata percentuale. Ma si può fare di più. Ad esempio, possiamo imporre che gli scambi vengano attuati una volta al secondo – oppure ogni dieci secondi – e in contemporanea. Possiamo inoltre costruire sistemi che rilevino automaticamente scambi Hft pericolosi per ritardarne l'esecuzione o cancellarli del tutto. Questi cambiamenti hanno però bisogno di regolatori che non temano di contrapporsi a potenti investitori. Dopo le tesi di Martin Lutero, il papa ha impiegato cinquant'anni per mettere mano alle indulgenze; speriamo di non dover pazientare altrettanto.

1. Atlantic Re:think (21 aprile 2015), “The day social media schooled Wall Street”, *Atlantic*, www.theatlantic.com/sponsored/etrade-social-stocks/the-day-social-media-schooled-wall-street/327; Jon Bateman (8 luglio 2020), “Deepfakes and synthetic media in the financial system: Assessing threat scenarios”, *Carnegie Endowment*, https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237.

CAPITOLO 20

Il mercato immobiliare di lusso

A Londra, New York, Vancouver e in molte altre grandi città, il mercato degli immobili di lusso è cambiato. Al centro non ci sono più i ricchi che si comprano case. È diventato una macchina per lavare i soldi sporchi. L'hack è questo: avete milioni di dollari (o rubli) che scottano, e che non potete depositare in banca o in un fondo di investimento; su richiesta del governo, queste istituzioni vi riempirebbero di domande da ficcanaso, col rischio di finire in un Rapporto per le attività sospette. Il sistema immobiliare vi offre però una vulnerabilità. In molti Paesi, i regolamenti per gli acquisti immobiliari non sono paragonabili neanche lontanamente alla rigidità di quelli delle banche e dei mercati finanziari. Le banche devono filtrare i clienti per evitare truffe e riciclaggio di denaro sporco, ma lo stesso non vale per le società di facciata straniere che si occupano di compravendite immobiliari. Visto che il governo non lo richiede, broker e venditori non fanno domande sul vostro contante dalla provenienza discutibile. Non appena vi rendete conto della vulnerabilità, l'hack è presto fatto.

Per prima cosa, acquistate un appartamento costosissimo in una città dove non avete intenzione di vivere. Effettuate l'acquisto tramite una società di facciata per celare il vostro coinvolgimento (tecnicamente sarete "beneficiari effettivi"). In seguito userete la proprietà come garanzia per ottenere un prestito bancario. Il denaro che otterrete in prestito sarà pulito, e potrete investirlo in modo più convenzionale, sul mercato azionario o da qualche altra parte, senza preoccuparvi delle regole di tali sistemi. Non importa se l'appartamento salirà o meno di valore: non è per questo che l'avete acquistato. Se il prezzo sale è comunque un plus, che vi permetterà di chiedere più soldi in prestito. Non lo affitterete, in quanto farlo svaluterebbe la proprietà, a prescindere dal comportamento degli affittuari.

Per questo Andrei Borodin, fuggito dalla Russia perché accusato di aver defraudato la propria banca, ha comprato un appartamento da 140 milioni di sterline a Londra. Non è l'unico ad aver fatto una cosa simile. Secondo un rapporto del 2015 di Transparency International, centosessanta proprietà in Gran Bretagna, dal valore complessivo di 4,4 miliardi di dollari, sono di proprietà di soggetti definiti "ad alto rischio di corruzione".[1] Città come New York e Miami sono piene di condomini di lusso senza affittuari. Nel 2014, il New York Times ha scoperto che in un palazzo di lusso l'80% degli appartamenti era di proprietà di società di comodo.[2]

Lo stesso trucchetto funziona, anche se non altrettanto bene, pure se non state cercando di riciclare i vostri soldi. Gli immobili sono comunque un buon sistema per parcheggiare denaro e acquisire garanzie, oltre che di far crescere il proprio potere di contrattazione grazie all'ascesa del mercato immobiliare.

È così che si spiega un'apparente stranezza di questo mercato: molti venditori preferiscono non vendere le proprie proprietà piuttosto che far scendere i prezzi a livelli sostenibili. Un asset non si svaluta finché non viene effettivamente venduto a un prezzo più basso. Quasi chiunque nel mercato degli immobili di lusso preferisce questa soluzione.

Questo crea un danno diretto a chi vuole semplicemente vivere nei quartieri interessati da questi fenomeni, che finiscono per svuotarsi. In zone come Mayfair a Londra, il 30% delle case sono vuote per colpa di chi le usa per riciclare denaro, con conseguenze nefaste per i negozi locali.

I modi per combattere questa deriva sono tanto evidenti quanto la vulnerabilità: servono cambiamenti regolatori che equiparino il mercato immobiliare agli altri sistemi finanziari. Nel 2016, il dipartimento del Tesoro degli Stati Uniti ha implementato un programma pilota in dodici città (noto come *geographic targeting order*) per imporre alle Llc, le aziende a responsabilità limitata, di rivelare, al momento della loro creazione, i nomi dei loro beneficiari effettivi. La quota di acquisti in contanti effettuata dalle Llc è così calata del 70%. La stessa imposizione può essere resa permanente e vigente a livello nazionale; nel frattempo i geographic targeting order

sono stati rinnovati ed espansi, per includere anche nuovi mercati immobiliari.[3] Il governo federale potrebbe ampliare la regola bancaria "conosci il tuo cliente" includendo anche i beneficiari effettivi delle società fittizie; potrebbe inoltre eliminare[4] l'esenzione "temporanea" – ma ormai praticamente permanente – imposta dai lobbisti nel Patriot Act del 2001, che non consente indagini approfondite nel settore immobiliare.

I politici non sembrano però poi tanto ansiosi di cambiare le regole – per quanto la Gran Bretagna potrebbe ripensarci dopo l'invasione russa dell'Ucraina. Tale inerzia è dovuta a questioni di potere. Ci sono interi settori – immobiliare, edilizio ecc. – che traggono beneficio dalla mancanza di regole. E tra le persone al potere, ben poche si gioverebbero di un cambiamento. Aumentare il gettito fiscale, rendere le case più a buon mercato e impedire di riciclare denaro sporco sono cose che interessano alla gente comune.

Il riciclaggio tramite il mercato immobiliare è oggi una tale consuetudine che è quasi un'esagerazione definirlo un hack. Lo stesso si potrebbe dire del business delle opere d'arte. È possibile, ad esempio, comprare un'opera d'arte a poco prezzo, farla valutare a una cifra molto alta e poi donarla a un museo per scaricarla fiscalmente, pagando così meno tasse a danno della collettività.

1. Matteo de Simone *et al.* (marzo 2015), “Corruption on your doorstep: How corrupt capital is used to buy property in the U.K.”, *Transparency International*, www.transparency.org.uk/sites/default/files/pdf/publications/2016CorruptionOnYourDoorstepWeb.pdf.
2. Louise Story e Stephanie Saul (7 febbraio 2015), “Stream of foreign wealth flows to elite New York real estate”, *New York Times*, www.nytimes.com/2015/02/08/nyregion/stream-of-foreign-wealth-flows-to-time-warner-condos.html.
3. Michael T. Gershberg, Janice Mac Avoy e Gregory Bernstein (2 maggio 2022), “FinCEN renews and expands geographic targeting orders for residential real estate deals”, *Lexology*, www.lexology.com/library/detail.aspx?g=065ffb4d-f737-42dc-b759-ef5c4d010404.
4. Max de Haldevang (22 giugno 2019), “The surprisingly effective pilot program stopping real estate money laundering in the US”, *Quartz*, https://qz.com/1635394/how-the-us-can-stop-real-estate-money-laundering.

CAPITOLO 21

La normalizzazione degli hack sociali

Quando pensiamo agli hack, supponiamo che vengano bloccati in fretta – con una patch – dai progettisti del sistema. E con gli hack informatici in genere va così. Sto scrivendo questo paragrafo nel maggio 2022, e negli ultimi tempi sono uscite queste notizie:

– Cisco ha dichiarato[1] di aver individuato una serie di vulnerabilità nel proprio software Enterprise Nfv Infrastructure, tra le quali una che può consentire a un hacker di passare da una macchina virtuale guest alla macchina host, compromettendo l'intera rete host.

– F5, azienda di sicurezza in cloud, ha segnalato[2] ai propri clienti quarantatré vulnerabilità presenti nei propri prodotti, tra le quali una "che potrebbe permettere a un hacker non autenticato con accesso di rete al sistema Big_IP tramite il management port e/o indirizzi self IP di eseguire comandi di sistema arbitrari, creare o cancellare file o disattivare servizi".

– Avg Corporation ha chiarito[3] i dettagli di due gravissime vulnerabilità nei suoi prodotti antivirus, annidate nel codice sin dal 2012. Entrambe consentirebbero a un hacker malevolo di disabilitare il software di sicurezza o manomettere il sistema operativo del cliente.

In tutti questi casi, la vulnerabilità è stata scoperta da ricercatori o dai realizzatori stessi, comunicata privatamente ai progettisti e solo in seguito resa pubblica, sottolineando però che a quel punto il sistema non era più vulnerabile.

Nel gergo della sicurezza informatica si parla di *divulgazione responsabile*. Il suo contrario è la *zero day vulnerability*. In questo caso la vulnerabilità viene scoperta in segreto da criminali, governi o da hacker che la rivendono a criminali o governi; l'organizzazione che gestisce il sistema lo viene a sapere solo dopo che la vulnerabilità è stata sfruttata. In questi casi, nessuno viene preavvisato. Nei casi

visti negli ultimi capitoli, e in molti altri esempi di questo libro, non sussiste alcuna divulgazione responsabile.

Nei sistemi non informatici, la cosa è più normale. Quando un manager di hedge fund scopre un hack particolarmente remunerativo per sfruttare il sistema finanziario, non avvisa il regolatore perché possa porvi rimedio. Lo adopera invece a proprio vantaggio fino a quando un organismo governativo lo costringerà a smettere.

Il processo è generalmente strutturato così: in primo luogo, viene scoperta una vulnerabilità, che viene poi usata per hackerare il sistema. In seguito, l'hack si diffonde. Può accadere in poco tempo o molto lentamente, a seconda del funzionamento dell'hack e di quanto è conveniente, della diffusione del sistema hackerato, della velocità di propagazione delle informazioni ecc. A un certo punto, l'organismo pubblico preposto al controllo del sistema scopre l'hack e si trova davanti due strade: può modificare le regole del sistema per prevenire l'hack, usando una patch, oppure può incorporare l'hack nel sistema normalizzandolo. Dopo la normalizzazione, l'hack spesso muore di morte naturale: se tutti lo attuano, smette infatti di offrire un vantaggio competitivo.

La storia degli hack finanziari è nel segno della normalizzazione.[4] Qualcuno inventa un hack e ci si arricchisce. Altri lo copiano e si accodano. I regolatori se ne accorgono e cercano di intervenire. A volte dichiarano illegale l'hack in questione, mettendo in prigione gli hacker. La maggior parte delle volte, invece, approvano l'hack retroattivamente. L'hack smette così di essere un hack per diventare un comune elemento della finanza. Il processo di normalizzazione non è sempre deliberato. Come nel caso degli hedge fund, ci sono hack che vengono ignorati, fino a quando è l'inazione a normalizzarli. La cosa può essere positiva – ci sono hack come i conti Now e i trasferimenti di rischio di credito che hanno innovato la finanza – ma c'è sempre un prezzo da pagare. Molti degli hack appena visti mandano all'aria l'equità del mercato, prendendo di mira l'informazione, la scelta o le azioni di chi vi opera. Non sono innovativi, sono sovversivi. La loro normalizzazione ci fa capire quanto possano essere potenti certe persone ricche, in grado di

imporre il proprio volere a discapito di tutti gli altri.

La normalizzazione non è una novità,[5] come non lo è il tira-e-molla tra hacker e regolatori. Nel medioevo, sia la chiesa cattolica sia le autorità secolari limitavano fortemente la possibilità di elargire prestiti con interessi, attività considerata peccato. Il mestiere del bancario però divenne sempre più professionale, e i più ricchi del settore riuscirono ad aggirare le restrizioni con metodi particolarmente raffinati. Ad esempio falsificavano i registri e classificavano i prestiti a usura come leciti, mascherando gli interessi da regali ricevuti dal debitore. Un tipo di hack era spacciare un prestito a tasso di usura per un caso di *pecunia traiecticia*, associandolo a un viaggio in mare fittizio.[6]

Questi hack medievali riecheggiano in tutti i casi visti in questo capitolo. Tra il Dodicesimo e il Tredicesimo secolo, la chiesa cattolica rinnovò i regolamenti sull'usura per combattere innovazioni quali la falsa pecunia traiecticia, creò meccanismi più sofisticati per applicare le leggi e cominciò a punire in modo più severo chi veniva condannato per usura. I ricchi sanno però scovare sempre nuovi sistemi per proteggere i propri guadagni. Le potenti gilde disponevano di risorse e competenze per creare prodotti finanziari in grado di sfuggire alle maglie della chiesa. Si stabilì inoltre una sorta di regulatory capture, in quanto la chiesa accettava donazioni e restituzioni da chi violava le regole sull'usura, che divenne così di fatto tollerata.

Si può dire che le banche moderne nascano nel 1517, con il Concilio Lateranense V, un perfetto esempio di come un hack benefico possa essere normalizzato. Chiunque abbia mai fatto un mutuo per comprare casa, mandare i figli a scuola o aprire un'attività deve ringraziare proprio questa normalizzazione (il Concilio legalizzò anche i banchi dei pegni, dei quali pure potreste esservi serviti).

Oggi la normalizzazione sembra una cosa comune. Sono certo che gran parte degli hack ad alta frequenza sul trading sarebbero stati dichiarati illegali se fossero stati inventati cent'anni fa. E sono altrettanto sicuro che, se l'insider trading fosse stato inventato negli ultimi decenni, oggi sarebbe legale.

1. Michael Cooney (5 maggio 2022), "Cisco warns of critical vulnerability in virtualized network software", *Network World*, www.networkworld.com/article/3659872/cisco-warns-of-critical-vulnerability-in-virtualized-network-software.html.
2. Harold Bell (5 maggio 2022), "F5 warns of BIG-IP iControl REST vulnerability", *Security Boulevard*, https://securityboulevard.com/2022/05/f5-warns-of-big-ip-icontrol-rest-vulnerability.
3. Charlie Osborne (5 maggio 2022), "Decade-old bugs discovered in Avast, AVG antivirus software", *ZD Net*, www.zdnet.com/article/decade-old-bugs-discovered-in-avast-avg-antivirus-software.
4. Avrei potuto scrivere lo stesso dei fondi indicizzati. Annie Lowrey (aprile 2021), "Could index funds be 'worse than Marxism'?", *Atlantic*, www.theatlantic.com/ideas/archive/2021/04/the-autopilot-economy/618497.
5. La normalizzazione non è certo una novità: Robert Sabatino Lopez e Irving W. Raymond (2001), *Medieval Trade in the Mediterranean World: Illustrative Documents*, Columbia University Press.
6. La *pecunia traiecticia*, o *foenus nauticum*, era un prestito per una spedizione marittima: visto il rischio d'impresa, in questo caso i tassi più alti erano consentiti (*N.d.T.*).

CAPITOLO 22

L'hacking del mercato

Dal 2010 al 2014, la Goldman Sachs è stata proprietaria di un'azienda per lo stoccaggio dell'alluminio, con ventisette magazzini nella zona di Detroit. Ogni giorno, i camion spostavano da un capannone all'altro un carico dopo l'altro di sbarre d'alluminio da sette quintali l'una.[1] Ogni singolo giorno.

Naturalmente si trattava di un hack. Il prezzo spot dell'alluminio viene calcolato anche in base al tempo di attesa per il cliente tra acquisto e consegna. Spostare le sbarre d'alluminio da un magazzino all'altro ne influenzava il prezzo e, visto che in quei ventisette capannoni c'era un quarto delle riserve d'alluminio del Paese, il giochetto permetteva a Goldman Sachs di trarne vantaggio.

Un hack del genere è impossibile per chi non è ricco come la Goldman Sachs. È il denaro a consentire di hackerare l'economia di mercato, per questo solo i più ricchi possono farlo.

Gli hack di mercato sfruttano le vulnerabilità nel processo di compravendita di merci e servizi: elementi quali la logica della domanda e dell'offerta, la scelta dei consumatori, l'ingresso e l'uscita dal mercato di un'azienda, e soprattutto il tipo di prodotti offerti.

Il capitalismo – il libero mercato – è un sistema economico che presenta alcuni vantaggi rispetto a quello che l'ha preceduto, il sistema mercantile. A differenza di sistemi a pianificazione centrale come il comunismo, il capitalismo non viene controllato da una singola entità. I singoli soggetti compiono scelte individuali per il proprio interesse, il capitale va dove può essere impiegato con maggior profitto e in mezzo a tutto questo caos emerge un mercato efficiente, o almeno così accadrebbe in un mondo perfetto.

Il meccanismo di base per far funzionare il tutto è che gli acquirenti prendano per il proprio interesse decisioni intelligenti, scegliendo tra venditori in competizione tra loro. Le regole di mercato servono a preservare il funzionamento di questo

meccanismo di base, impedendo che si verifichino ulteriori danni. Tra queste regole ci sono leggi facili da immaginare, come quelle contro le truffe e la mancata sicurezza sul lavoro, oltre a leggi meno scontate, come quelle che governano il rispetto dei contratti, le valute nazionali, la risoluzione delle dispute in sede civile eccetera.

Ai mercati interessa che tre cose funzionino al meglio: l'informazione, la scelta, e l'agency, ovvero il modo di agire dei soggetti interessati. Gli acquirenti devono essere informati su prodotti e servizi per poter decidere i propri acquisti in modo intelligente: devono conoscerne pregi e difetti, caratteristiche ecc. Devono poi poter scegliere tra vari venditori, perché senza concorrenza i prezzi non scendono e l'innovazione ristagna. Infine devono poter agire, in modo da usare la propria conoscenza per scegliere. Tutti e tre questi elementi del mercato sono stati hackerati:

– Ci sono prodotti complessi che non danno un'informazione chiara. Pensiamo ad esempio a quando dobbiamo confrontare i prezzi di diversi cellulari, pacchetti di investimento o carte di credito. Un cliente che non capisce si confonde e ha più difficoltà a fare una scelta intelligente. Certo, è una conseguenza inevitabile del nostro mondo tecnologico, ma spesso si tratta anche di un hack voluto, per impedire agli utenti di accedere a informazioni accurate.

– I monopoli tolgono la libertà di scelta. I monopoli non sono certo una novità, e prima del capitalismo non erano un hack. Se un sistema di libero mercato implica che i venditori siano in competizione tra loro per arrivare agli acquirenti, i monopoli sovvertono i meccanismi di base di tale sistema. Nel 1776, Adam Smith ha spiegato come spesso gli interessi degli uomini d'affari non concordino con l'interesse pubblico.[2] Lo scopo degli affaristi, e ovviamente delle imprese, è massimizzare i profitti. Lo scopo del pubblico è (più o meno) massimizzare quantità, qualità, varietà e innovazione dei prodotti, minimizzando i prezzi. Se viene a mancare la concorrenza, i venditori non temono più di perdere acquirenti, e non sono incentivati a offrire al pubblico ciò che vuole.

– Il *lock-in*, la difficoltà di muoversi e cambiare, riduce la nostra agency, la nostra possibilità di scegliere liberamente tra vari prodotti. Se oggi beviamo una Coca-Cola e non ci piace, domani possiamo bere

una Pepsi. Ma se oggi non ci troviamo bene con il piano tariffario del nostro telefono, col nostro provider di posta elettronica o con la nostra carta di credito, probabilmente domani useremo comunque lo stesso piano, lo stesso provider e la stessa carta. C'è un prezzo troppo alto da pagare per cambiare: è questione di costi, tempo, comodità, difficoltà di imparare nuove cose. È questo che si intende con lock-in. Può essere un hack in quanto ci sono diversi modi per costringere un consumatore al lock-in: software proprietari che rendono più costoso cambiare il device col quale ascoltiamo la musica o leggiamo ebook; social network che non ci fanno più accedere agli account dei nostri amici se cancelliamo il nostro; app che non ci consentono di trasferire i nostri dati se le abbandoniamo.

La conseguenza di tutte queste cose è che a nostre spese le aziende hackerano il mercato e guadagnano di più. Per impedirlo si può ricorrere a una regolamentazione del mercato. La deregulation, per sua natura, elimina gli ostacoli. Permette più hack, e lo fa essenzialmente dando loro un'approvazione preventiva, prima ancora che se ne possano conoscere gli effetti. Ovviamente la deregulation ha lati positivi e negativi. Tra quelli positivi c'è la possibilità di implementare rapidamente un'innovazione. Tra quelli negativi il fatto che una sovversione del sistema possa venir attuata in tempi altrettanto rapidi.

Negli Usa abbiamo storicamente privilegiato l'innovazione tramite una struttura normativa minima. In genere ha funzionato, visto che sono stati limitati i danni dei peggiori hack. Oggi non è più così, a causa della maggior forza della tecnologia e della natura globale delle nostre economie. Un sistema economico basato su avidità ed egoismo funziona solo quando queste caratteristiche non rappresentano un rischio sistemico. Il celebre motto coniato da Mark Zuckerberg per Facebook, "muoviti in fretta e rompi tutto", è accettabile solo se mette a rischio cose che ti appartengono. Se c'è di mezzo la roba degli altri, meglio magari pensarci bene, o essere costretti a riparare i danni fatti.

1. David Kocieniewski (20 giugno 2013), “A shuffle of aluminum, but to banks, pure gold”, *New York Times*, www.nytimes.com/2013/07/21/business/a-shuffle-of-aluminum-but-to-banks-pure-gold.html.
2. Adam Smith (1776), *La ricchezza delle nazioni*, UTET (2017), a cura di Anna e Tullio Biagiotti. Nei capitoli “Diseguaglianze derivanti dalla natura stessa degli impieghi” e “Digressioni sulle variazioni del valore dell’argento negli ultimi quattro secoli”.

CAPITOLO 23

"Too big to fail"

L'espressione *too big to fail*, troppo grande per fallire, racchiude una vulnerabilità molto importante della nostra economia di mercato. Quando sei così grosso che un tuo fallimento metterebbe a rischio la sopravvivenza dell'intero sistema, puoi permetterti di rischiare, tanto nessuno ti consentirà di fallire. Lo dice bene un vecchio adagio attribuito a J. Paul Getty (anche se probabilmente lo disse prima John Maynard Keynes): "Se devi 100 dollari a una banca è un tuo problema, se devi 100 milioni di dollari a una banca il problema è della banca". Ecco il concetto di "too big to fail" in sintesi.

Ma addentriamoci nei dettagli. Ci sono aziende necessarie al funzionamento della nostra economia, al punto che non possiamo permettere che falliscano. Sono troppo grandi, troppo centrali e, nel caso smettano di creare profitti, per lo Stato sarebbe più economico salvarle che lasciarle al loro destino. Il meccanismo base del mercato è che i venditori siano in competizione tra loro per trovare acquirenti; chi sa vendere riesce a prosperare, chi non è capace viene sconfitto.

Immaginiamo un uomo d'affari o un'azienda qualunque alle prese con una decisione rischiosa. Devono soppesare i vantaggi di un esito positivo e i rischi di uno negativo, tenendo conto di entrambi. Chi invece è a capo di un'azienda troppo importante per fallire saprà che i costi inevitabili di una decisione sbagliata ricadranno sui contribuenti: saranno un problema della società nel suo complesso. Si viene così a creare un *moral hazard*, un rischio morale, e vengono favorite decisioni pericolose. Nel caso vadano a buon fine, tanto meglio; in caso contrario, non ci sarà nulla da temere. Essere "too big to fail" significa disporre di un'assicurazione contro le scommesse perse. Per il nostro sistema di mercato è un elemento fortemente perturbante, una distorsione alimentata da soldi e potere. Ed è anche un hack.

Dopo la crisi finanziaria del 2008, il governo statunitense salvò molte grandi banche e istituzioni finanziarie di Wall Street, malgrado i loro manager fossero colpevoli di anni di gestioni dissennate. Venne attuato il Troubled Asset Relief Program, che consentiva al governo di acquistare beni e azioni di aziende allo sbando, compresi i titoli basati sui mutui, con la convinzione che quel bailout da 700 miliardi di dollari fosse necessario per salvare l'economia americana. Si temeva la recessione, con un crollo del sistema molto più oneroso di quei 700 miliardi di dollari. (Nei periodi di recessione economica, i governi incassano di meno, visto che le persone guadagnano meno e pagano meno tasse; al contempo i governi spendono di più, ad esempio per i sussidi di disoccupazione. In sintesi, più una recessione è grave, più è costosa).

Non è stata la prima volta che il governo Usa ha salvato le aziende "troppo grandi per fallire". Negli anni Trenta, dopo una serie di fallimenti bancari, venne creata la Federal Deposit Insurance Corporation per monitorare le banche e proteggere i depositi dei consumatori. Nel 1979, il governo salvò la Chrysler Corporation. Fu un bailout di entità minore, solo 1,5 miliardi di dollari, ma le motivazioni date non furono molto diverse. Si parlò di sicurezza nazionale in quanto, all'apice della Guerra Fredda, l'azienda stava costruendo i carri armati M1 Abrams. Si tirò in ballo il sistema economico. Si disse che bisognava salvare 700mila posti di lavoro a Detroit e non solo. Inoltre gli Usa erano in piena guerra commerciale col Giappone per il dominio del mercato automobilistico. Il salvataggio fu un successo: Chrysler ripagò il prestito in breve tempo, e con gli interessi.

L'hack "too big to fail" è reso possibile da un cambiamento del *threat model*. Quando vennero inventati i meccanismi dell'economia di mercato, non esisteva alcuna impresa tanto importante da rendere necessario l'intervento del governo nel caso rischiasse il fallimento. Questo non solo per una questione di dimensioni: anche le privatizzazioni dei servizi sociali fondamentali non si erano spinte ai livelli odierni. Era ovviamente possibile che un'azienda crescesse, ma non a tal punto. Per una crescita del genere ci vogliono le tecnologie moderne.

I rari tentativi di regolare queste imprese gigantesche sono in genere piuttosto fiacchi, schiacciati dalle loro attività di lobby, volte a schivare ogni supervisione. Le riforme bancarie introdotte dal Dodd-Frank Act del 2010 riducevano la minaccia delle istituzioni "too big too fail", ma una volta passate al vaglio del Congresso vennero rese inefficaci, o comunque furono azzoppate dalle successive riforme fiscali.

Un modo di difendersi dall'hack del "too big to fail" è non salvare direttamente le mega-corporation. Nel 2008, il governo Usa avrebbe potuto seguire almeno due strade alternative. Avrebbe potuto collegare i salvataggi a una ristrutturazione dei mutui volta a eliminare un'ondata di default. Oppure avrebbe potuto salvare le banche a patto che queste trasferissero poi il denaro ai loro debitori. Entrambe le opzioni vennero bocciate da Larry Summers, all'epoca direttore del National Economic Council. Il bailout del 2008 è un ulteriore esempio di come i ricchi proteggano gli hack sfruttati dai ricchi stessi.

Il modo migliore per difendere un sistema economico da aziende troppo grandi per fallire è fare in modo che non ce ne siano. Nel 2009, il sociologo Duncan Watts scrisse il saggio *Too Big to Fail? How About Too Big to Exist?*, sostenendo che certe aziende sono talmente grosse e potenti da poter usare il governo come assicurazione contro le proprie decisioni avventate, servendosi liberamente del denaro dei contribuenti. Hack come questi sono un perfetto esempio di tre caratteristiche che ritroveremo nel corso del libro.

In primo luogo, il concetto di "too big to fail" è generalizzabile. Non appena i colossi bancari, immobiliari e di altri settori "essenziali" dell'economia si rendono conto di poter mettere in atto l'hack del "too big to fail", l'intera economia di mercato diviene vulnerabile a imprese che si espandono in modo non sostenibile.

In secondo luogo, gli hack possono essere sistematizzati e influire sui processi decisionali: i salvataggi del 2008 di fatto trasformarono il concetto di "too big to fail" in norma di legge. Il Congresso dimostrò che il governo federale era disposto a salvare settore bancario, immobiliare e automobilistico, normalizzando l'hack come

parte effettiva dell'alta finanza.

In terzo luogo, il concetto stesso di "too big to fail" cambia il modo di comportarsi dei dirigenti delle aziende più grandi, e di conseguenza le loro stesse organizzazioni. Sono sicuro che oggi alcune aziende considerino il bailout da "too big to fail" come una sorta di polizza assicurativa d'emergenza.

Senza dubbio, le poche organizzazioni che ottennero un esplicito bailout con il Dodd-Frank – Citigroup, JP Morgan Chase, Bank of America e Goldman Sachs – sanno bene che il governo, in caso d'emergenza, sarebbe pronto a salvarle ancora.[1] Può sembrare incredibile, ma per quanto sia dannoso per la nostra economia di mercato, questo tipo di hack è stato normalizzato.

1. Michael Greenberger (giugno 2018), “Too big to fail U.S. banks’ regulatory alchemy: Converting an obscure agency footnote into an ‘at will’ nullification of Dodd-Frank’s regulation of the multi-trillion dollar financial swaps market”, Institute for New Economic Thinking, www.ineteconomics.org/uploads/papers/WP_74.pdf.

CAPITOLO 24

Venture capital e private equity

Le app di food delivery si basano su un business model insostenibile. Nel 2020, anno di pandemia nel quale molti di noi erano costretti a stare chiusi in casa, DoorDash ha perso 139 milioni di dollari e Grubhub 156 milioni di dollari. Non abbiamo le cifre per Uber Eats, ma Uber in generale ha perso 6,8 miliardi di dollari: sempre meglio degli 8,5 miliardi di dollari persi nel 2019. Si tratta di un modello insostenibile anche per i singoli investitori: il food delivery non funziona per nessuno. I fattorini – *gig worker* senza assicurazione o contributi – vengono pagati poco. I servizi danneggiano i ristoranti: non generano profitti per una serie di motivi, non fanno crescere le vendite e danneggiano la reputazione di un ristorante se il servizio di consegna fa un errore. E non se ne avvantaggiano neanche i clienti: sono costretti a pagare prezzi più alti per la merce e per il servizio, e spesso nel delivery si presentano problemi di ogni sorta. Il solo motivo per l'esistenza di un mercato del genere è che società di venture capital come Soft Bank sono disposte a investirci decine di miliardi di dollari, con la speranza di poter intercettare abbastanza profitti dell'industria della ristorazione da poterne ricavare un guadagno. Questa strategia di investimento è un hack: nell'economia di mercato, la razionalità collettiva non coordinata degli acquirenti dovrebbe influenzare i venditori. I soldi investiti nel venture capital impediscono che questo accada, bloccando l'agency degli acquirenti.

Il venture capital (VC) come modello di finanziamento ha origine centinaia di anni fa, ma ha preso piede solo negli anni Ottanta del Novecento. È stato decisivo nell'ascesa delle prime aziende tecnologiche, oltre che nell'inflazione e nello scoppio della bolla dot-com nel 2001. Da allora, questo modello non ha fatto che crescere: nel 2010, il mercato globale del venture capital era di 50 miliardi di dollari; nel 2019, era già arrivato a 295 miliardi di dollari. Io stesso ne ho approfittato: nel 2006 ho venduto a BT la mia prima azienda,

finanziata dal venture capital, e nel 2016 ho venduto la seconda a Ibm. Il venture capital in sé non è un hack. L'hack viene attuato quando aziende che non generano profitti usano i soldi del VC per ignorare le dinamiche dell'economia di mercato.

Non auspichiamo certo che un ente per la pianificazione centrale decida quali aziende possano operare e quali debbano chiudere.[1] Ma quando ci sono di mezzo le società di venture capital, è proprio quello che accade. Grazie ai soldi del VC, le aziende non sono più in competizione l'una con l'altra secondo il modello tradizionale, né devono più preoccuparsi della legge della domanda e dell'offerta. Possono fare cose pazze – regalare i propri prodotti, pagare stipendi folli, accettare perdite finanziarie enormi, offrire servizi che fanno male alla gente – tutto questo grazie a quei finanziamenti esterni. Si tratta di una pianificazione centrale decisa da investitori d'élite. Se lo facesse il governo, qualcuno potrebbe parlare di comunismo.

Da quando è stata fondata nel 2009, Uber ha ricevuto 25,5 miliardi di dollari dal VC. Non c'è stato un singolo anno in cui abbia generato profitti. Nel 2019, le sue perdite a livello mondiale sono state di 8,5 miliardi di dollari, pari a una perdita di 58 centesimi per ogni dollaro dei 5,2 miliardi di corse effettuate. L'unico motivo per l'esistenza di Uber è che ci sono ancora investitori disposti a versare capitale in un simile pozzo, probabilmente in attesa che la tecnologia per le auto senza guidatore consenta all'azienda di licenziare tutti i suoi conducenti e operare con una flotta del tutto automatizzata.

Anche WeWork, gruppo statunitense che fornisce locali e servizi di coworking, non ha mai generato profitti, perdendo più di 10 miliardi di dollari negli ultimi tre anni. Nel 2019 ha cercato, fallendo, di quotarsi sul mercato, e la sua bolla alimentata dal VC è esplosa. Il lavoro a distanza imposto dal Covid-19 ha danneggiato ulteriormente le speranze di successo di WeWork, al punto che il cofondatore dell'azienda è stato rimosso dal ruolo di Ceo e presidente del board. Il solo motivo per la crescita di WeWork è stato la raccolta di 12,8 di miliardi provenienti dal VC tra il 2010, anno della sua fondazione, e l'estate del 2019; da allora sono arrivati altri miliardi per appianare i debiti.

Questi esempi non vanno equiparati ai cattivi investimenti, e

nemmeno a quelli di natura fraudolenta. Quibi era un'azienda basata sul venture capital che si era accaparrata più di 1,75 miliardi di finanziamenti prima ancora del suo lancio. Il suo concept era l'offerta di contenuti video della durata di dieci minuti o meno. Dopo aver raccolto pochissimi abbonamenti, è stata chiusa nel giro di sei mesi. Elizabeth Holmes ha fondato Theranos sfruttando il venture capital e senza proporre nemmeno un prodotto di successo, ed è riuscita a spennare gli investitori per anni per il totale di un miliardo di dollari. Si tratta di due esempi di normale funzionamento del mercato: semplicemente gli acquirenti – nel caso, gli investitori – hanno fatto un acquisto sbagliato. Nell'esempio della Theranos si è trattato di una vera e propria frode.

In generale, il sistema del venture capital sovverte l'economia di mercato sotto diversi aspetti. Distorce i mercati, permettendo alle aziende di richiedere prezzi che non riflettono il costo o il valore di quel che vendono. Permette a imprese che non generano profitti e a business model insostenibili di diffondersi e prosperare. Distorce anche il mercato del lavoro, soprattutto nel settore tecnologico. E infine incide negativamente su intere categorie di mercato, come trasporti, settore immobiliare e media. Ad esempio, Uber e Lyft hanno creato un mercato insostenibile per i trasporti, richiedendo prezzi artificialmente bassi che non riflettono il valore reale del lavoro del conducente.

Il VC hackera anche l'innovazione. Favorisce i ricavi finanziari a discapito di reali miglioramenti del prodotto, dando così la priorità ad alcuni tipi di innovazione e penalizzandone altri. A un'azienda finanziata dal VC interessa solo che si possa rientrare degli investimenti. Il VC fa mancare pertanto uno degli obiettivi di un'economia di mercato, ovvero che l'innovazione venga incentivata. Gli investitori del VC vogliono rientrare dei propri investimenti nel giro di dieci anni o anche meno, con conseguenze sul comportamento delle aziende.

Allo stesso modo, la cultura del VC ricompensa solo chi porta ricavi molto alti. Gli investitori sono pertanto pronti a finanziare centinaia di aziende con idee e business model di vario tipo, pur sapendo che saranno in gran parte destinate al fallimento, perché confidano che le

poche aziende di successo sulle quali avranno scommesso porteranno risultati trionfali. Cercano "il colpaccio", invece di costruire imprese sostenibili a lungo termine. Per questo le aziende finanziate dal VC spesso perdono tanti soldi e danneggiano la società. Sono perdite ripagate dai trionfi, definiti "unicorni" nel gergo del VC.

La private equity consente un diverso tipo di hack: il finanziamento del debito. Quando una società di private equity acquisisce un'azienda rilevandone la maggior parte delle quote, può usare una parte minore del proprio capitale e affidarsi invece al debito. Può cioè acquisire l'azienda tramite il debito, estrarne tutto il denaro possibile, lasciarla ancor più indebitata e venderla a una cifra più alta, il tutto mentre i debitori se ne restano a mani vuote. Pensiamo al caso di Greensill Capital, che nel 2021 è andata incontro a un disastro memorabile.[2] Per dieci anni si è espansa in modo insostenibile, passando da startup finanziaria per la supply-chain a intermediaria multinazionale con un carico debitorio di 4,6 milioni di dollari, fino all'insolvenza, un processo accelerato dagli investimenti di SoftBank, che ha guadagnato milioni grazie a fondi che restavano disponibili malgrado i bilanci sempre più sospetti.

Non si tratta di pratiche illegali. Venture capital e private equity sono parti integranti della nostra economia, al punto che sembra perfino strano chiamarli hack. E invece è quel che sono. Sono hack di tutto ciò che dovrebbe essere il mercato. Nessuno parla di hack, ma solo di pratiche "dirompenti" e "innovative". Il fatto che una cosa sia legale e accettata non cambia però che siano soldi e potere a decidere quali siano i comportamenti consentiti e chi può sedersi al tavolo da gioco.

1. Eric Levitz (3 dicembre 2020), “America has central planners. We just call them ‘venture capitalists’”, Intelligencer – *New York Magazine*, https://nymag.com/intelligencer/2020/12/wework-venture-capital-central-planning.html.
2. Eshe Nelson, Jack Ewing e Liz Alderman (28 marzo 2021), “The swift collapse of a company built on debt”, *New York Times*, www.nytimes.com/2021/03/28/business/greensill-capital-collapse.html.

CAPITOLO 25

Hacking e ricchezza

Nello sport professionistico i tetti retributivi mantengono competitivi i campionati, riducendo il vantaggio delle squadre più ricche. Le squadre di una lega si accordano per non superare una somma complessiva per gli ingaggi dei loro giocatori. Questi accordi vengono però hackerati. A seconda dello sport e delle regole, i team possono nascondere i compensi nei bonus assegnati alla firma dei contratti, spalmando i compensi nel corso degli anni, chiedendo agli sponsor amici di ingaggiare i loro giocatori, assumendo il partner o la partner di un giocatore o spostando gli stipendi dei giocatori nel budget di una squadra associata appartenente a una categoria inferiore. Lo sport professionistico è un gran giro di soldi, e le squadre fanno di tutto per aggirare le regole.

Gli hack che abbiamo visto finora nei sistemi finanziari e bancari sono in genere messi in atto da persone ricche col fine di arricchirsi ancor di più. È un totale ribaltamento dei preconcetti sull'hacking. In genere pensiamo che l'hacking abbia una valenza controculturale: che sia uno strumento usato dai più deboli per superare gli ostacoli messi dai potenti sulla loro strada. Pensiamo ad esempio al gruppo di hacker Anonymous. È però più facile che siano i ricchi a hackerare un sistema a proprio vantaggio, per diventare ancora più ricchi o potenti.

Quando si tratta di hacking, i ricchi sono privilegiati. Innanzitutto non devono per forza essere grandi hacker in prima persona. Hanno abbastanza risorse per ingaggiare esperti in grado di trovare le vulnerabilità e i modi di sfruttarle, per poi mettere in atto gli hack. Inoltre, il denaro è tanto importante in politica che i ricchi riescono meglio degli altri a normalizzare i propri hack. Usano il proprio potere per fare in modo che i loro hack vengano approvati dalla legge.

Nel 2009, General Motors dichiarò bancarotta, stabilendo che le

proprie azioni non avevano più valore, per poi creare un nuovo stock da vendere per raccogliere capitale. I dirigenti e i maggiori azionisti ne approfittarono, mentre i comuni shareholder – in gran parte dipendenti e pensionati dell'azienda – rimasero fregati. Si trattò di un hack molto remunerativo, ma solo per chi era già ricco. Ennesimo esempio di come i ricchi siano maestri dell'hacking. Gli individui e le organizzazioni con più risorse riescono meglio a scovare e implementare gli hack, oltre che a fare in modo che vengano legittimati e normalizzati.

Nel 2020, si è parlato tanto di un nuovo hack del sistema fiscale che riguarda la compravendita di azioni: il *cum-ex trading* (dal latino "con-senza").[1] Il *New York Times* l'ha descritto così: "Facendo grande attenzione alla tempistica, e coordinando una dozzina di diverse transazioni, gli scambi *cum-ex* danno origine a due rimborsi sulla tassa sui dividendi versata per un singolo paniere azionario". Il primo rimborso era legittimo, il secondo no.

È ovvio che si tratti di un hack; non era né previsto né voluto che un singolo o un'organizzazione ricevessero due rimborsi fiscali per un singolo pagamento. Il sistema però lo permetteva, e dal 2006 al 2011, banche, avvocati e investitori che hanno usato questo hack hanno alleggerito di 60 miliardi di dollari i Paesi dell'Unione Europea.

Di recente, in seguito a questo scandalo, la Germania ha condannato a dieci anni di prigione il banchiere Christian S.[2] Ma non è detta l'ultima parola: il caso di Christian S. andrà in appello. Nel 2020, due banchieri londinesi hanno ottenuto la sospensione della pena e una multa di 14 milioni di sterline per il cum-ex trading.[3] Una banca privata tedesca è stata condannata a pagare 176,6 milioni di euro alle autorità fiscali della Germania. Un ex ispettore fiscale tedesco,[4] fuggito in Svizzera nel 2012 quando si sono diffuse le prime voci sullo scandalo cum-ex, è stato estradato e accusato di aver dato consigli fraudolenti e di aver aiutato alcuni banchieri coinvolti in questa macchinazione. Di recente, gli offici di Francoforte della banca Morgan Stanley sono stati perquisiti nell'ambito di un'indagine sul metodo cum-ex,[5] e altri procedimenti sono in sospeso. Nella sola Germania, sono sotto indagine più di mille

avvocati e banchieri coinvolti negli scambi cum-ex.

Possiamo vedere come si intreccino hacking, legalità e moralità. Quando hanno chiesto conto a Donald Trump della sua elusione fiscale, come è noto ha risposto: “Vuol dire che sono furbo”.[6] Non vuol dire però che quel che fa sia eticamente accettabile. Potrebbe esserlo, se sfruttasse solo loophole legali, ma non significa che quei loophole fiscali non debbano essere chiusi.[7] Il cum-ex trading è costato agli Stati europei e ai loro cittadini almeno 60 miliardi di dollari, gran parte dei quali non sarà mai recuperata. L’hacking è parassitico, viene messo in atto soprattutto da ricchi e potenti, mentre tutti gli altri ne fanno le spese.

1. David Segal (23 gennaio 2020), "It may be the biggest tax heist ever. And Europe wants justice", *New York Times*, www.nytimes.com/2020/01/23/business/cum-ex.html.
2. Karin Matussek (1 giugno 2021), "A banker's long prison sentence puts industry on alert", *Bloomberg*, www.bloomberg.com/news/articles/2021-06-01/prosecutors-seek-10-years-for-banker-in-398-million-cum-ex-case.
3. Olaf Storbeck (19 marzo 2020), "Two former London bankers convicted in first cum-ex scandal trial", *Financial Times*, www.ft.com/content/550121de-69b3-11ea-800d-da70cff6e4d3.
4. Olaf Storbeck (4 aprile 2022), "Former German tax inspector charged with €279mn tax fraud", *Financial Times*, www.ft.com/content/e123a255-bc52-48c4-9022-ac9c4be06daa.
5. Agence France-Presse (3 maggio 2022), "German prosecutors raid Morgan Stanley in cum-ex probe", *Barron's*, www.barrons.com/news/german-prosecutors-raid-morgan-stanley-in-cum-ex-probe-01651575308.
6. Daniella Diaz (27 settembre 2016), "Trump: 'I'm smart' for not paying taxes", *CNN*, www.cnn.com/2016/09/26/politics/donald-trump-federal-income-taxes-smart-debate/index.html.
7. Come confermato nel 1935 da una sentenza della Corte Suprema degli Stati Uniti: "Chiunque potrà disporre dei propri affari in modo che le sue tasse siano quanto più basse possibile; non sarà obbligato a scegliere le soluzioni più vantaggiose per il Tesoro; non sussiste alcun dovere patriottico per il quale un individuo debba pagare più tasse" – Corte Suprema degli Stati Uniti (7 gennaio 1935), Gregory *vs* Helvering, 293 US 465, www.courtlistener.com/opinion/102356/gregory-v-helvering.

PARTE QUARTA
L'HACKING DEI SISTEMI GIURIDICI

CAPITOLO 26

L'hacking delle leggi

Per quanto possa sorprenderci, spesso l'edilizia si presta agli hack fiscali. Nella Francia del periodo napoleonico si diffuse la mansarda, che consentiva di ottenere un ulteriore piano abitabile senza pagare altre tasse, visto che veniva considerato parte del tetto. Anche il tetto a falde permetteva di avere un piano in più, aggirando così la legge fiscale federale americana del 1798. In Perù e in alcuni altri Paesi, dalle pareti e dai tetti delle case sbucano tondini d'acciaio, mentre nei paraggi ci sono pile di ghiaia: questo perché gli edifici ancora in costruzione pagano meno tasse di proprietà.

Colgo l'occasione per ricordare al lettore che cosa è un hack e che cosa non lo è. Dal 1696 al 1851, in Gran Bretagna, una tassa sulle finestre domestiche spinse molti proprietari a oscurarle. Era un hack, in quanto il numero delle finestre veniva utilizzato per calcolare la grandezza della casa, e oscurarle dava la possibilità di barare. Se si fosse misurata direttamente la grandezza delle case, e per non pagare le tasse i proprietari avessero demolito casa propria, non sarebbe stato un hack. Abbandonare o distruggere un sistema per evitarne i costi non è un esempio di hacking. L'hacking prevede che vengano scovate e sfruttate le regole di un sistema, volgendole a proprio vantaggio mentre si continua a prendere parte a tale sistema.

Gli Stati agiscono utilizzando il linguaggio e le parole possono cambiare il mondo. Negli Usa il Congresso approva le leggi, il Presidente firma i decreti, le agenzie scrivono i regolamenti. Si tratta solo di parole associate al potere di attuarle. In un certo senso, tali parole sono un codice. E come un codice informatico, presentano bug e vulnerabilità. Gli autori di qualunque testo giuridico sono imperfetti e fallibili, proprio come sono influenzabili. Per questo le leggi possono essere hackerate. I loro autori possono – per errore o volutamente – lasciare qualche vulnerabilità nelle leggi, ed è inevitabile che prima o poi gli hacker la scovino. Le "leggi suntuarie"

(pensate alla parola “sontuoso”) regolavano il lusso e lo sfarzo. Un tempo servivano a evitare che i nobili facessero a gara a chi spendeva di più in feste, banchetti, lussi e bagordi. A volte sono state approvate per impedire che le persone delle classi inferiori cercassero di imitare gli aristocratici. In entrambi i casi, chi veniva limitato da queste leggi ha cercato di hackerarle.

Spesso, ad esempio, è stato imposto un limite al numero di portate o alla varietà di carni che si potevano servire. Una legge fiorentina del 1356 imponeva di non superare le tre portate in un pranzo di nozze. Dalla definizione di “portata” erano però esclusi formaggio, frutta e verdura: un perfetto loophole per servire altro cibo. Un solo “arrosto” poteva inoltre presentare una portata riempita con uno o più tipi di carne diversa: a quanto pare il *turducken*[1] è nato proprio per hackerare una legge suntuaria. È l’ennesima dimostrazione di come i ricchi possano rispettare tecnicamente una legge e al tempo stesso sovvertirne lo spirito.

I sistemi giuridici sono sistemi di regole e in quanto tali vulnerabili all’hacking. In un certo senso, sono progettati per essere hackerati. In genere viene attuata la lettera della legge, è raro che ne venga attuato lo spirito. Ammettiamo che tu scopra un hack, vale a dire un modo per obbedire alla lettera della legge violandone lo spirito: non sarà colpa tua se la legge non è stata ben scritta. Chi cerca di aggirare il sistema fiscale usa costantemente questo tipo di argomentazione.

Le leggi vengono hackerate ovunque. Nel 2020, la Federal Reserve ha attuato un programma di prestiti d’emergenza per le aziende colpite dalla pandemia di coronavirus.[2] Per quanto ufficialmente solo le aziende americane potessero beneficiarne, alcune aziende straniere hanno trovato il modo per trasformarsi in aziende americane e hackerare questa regola. La Pacific Investment Management Company, con sede a Newport Beach, in California, gestisce un hedge fund registrato nelle Isole Cayman per non pagare le tasse negli Usa. Investendo in una corporation del Delaware e collegandola all’azienda madre in California, l’hedge fund è riuscito però a chiedere denaro in prestito per acquistare titoli, a ottenere 13,1 milioni di dollari dal programma di sussidi governativi e a usare la cifra del sussidio per ripagare il prestito per l’acquisto di titoli. Un

profitto istantaneo, perfettamente legale e a spese dei cittadini americani. Forse si sono comportati da sociopatici, ma non posso fare a meno di ammirare la loro creatività.

Quando parlo di hackerare le leggi non mi riferisco solo all'ambito legislativo. Qualsiasi regola può essere hackerata. La chiesa cattolica, nel corso dei secoli, ha stabilito varie regole per l'astinenza, che in genere prevedevano di non mangiare carne in determinati giorni: un digiuno, seppur parziale se confrontato con lo Yom Kippur o il Ramadan. Ma sapete com'è fatta la gente: nel medioevo in tanti si sono scervellati per definire bene i concetti di "carne" e "non carne", soprattutto quando si trattava di periodi lunghi come la quaresima e l'avvento. Così il pesce non veniva considerato carne, proprio come l'oca facciabianca, in quanto (si dice) deponeva le uova in acqua e aveva le zampe squamose. E i castori? Non contavano come carne nemmeno loro. (E non si tratta di una mera curiosità storica. Ancora oggi, a Detroit, i cattolici possono mangiare topi muschiati nei giorni di digiuno, in base a una regola missionaria del Settecento). In alcuni monasteri francesi venivano serviti feti di coniglio, non considerati carne in quanto nuotavano nel fluido amniotico (giuro che non mi sto inventando niente). San Tommaso d'Aquino dichiarò che i polli erano di origine acquatica – qualunque cosa significhi – e pertanto non erano da considerarsi carne. Alcuni vescovi si spinsero ancora oltre, dichiarando che la regola vale per tutto il pollame, visto che non si tratta di quadrupedi.

Un hack più moderno delle regole sul digiuno viene attuato da alcune ricche famiglie saudite, che considerano il Ramadan una sorta di festa lunga un mese, dove si può stare svegli la notte e dormire di giorno.

Non c'è legge che non si presti all'hacking. Fino a quando ci saranno persone desiderose di sovvertire l'intento di una legge, gli hacking non mancheranno mai.

1. Si tratta di un tacchino ripieno di un'anatra ripiena di pollo. La versione moderna è una fantasiosa creazione dello chef Paul Prudhomme. Una volta ho provato a prepararlo ma non ne vale la pena.
2. Jeanna Smialek (30 luglio 2020), "How Pimco's Cayman-based hedge fund can profit from the Fed's rescue", *New York Times*, www.nytimes.com/2020/07/30/business/economy/fed-talf-wall-street.html.

CAPITOLO 27

Loophole giuridici

La “zona della morte” è una strana vulnerabilità della costituzione degli Stati Uniti.[1] Deriva dalla contraddizione tra alcune regole giurisdizionali statali e locali. La Venue Clause dell’articolo III, sezione 2 della Costituzione stabilisce che: “Il processo per tutti i reati, tranne i casi di impeachment, avverrà mediante giuria; e tale processo sarà tenuto *nello Stato* dove i detti reati sono stati commessi”. La Vicinage Clause del sesto emendamento sostiene che: “In ogni processo penale, l’accusato avrà il diritto a un procedimento pronto e pubblico, con una giuria imparziale di persone *dello Stato e del Distretto* in cui il delitto sia stato commesso”. La Corte distrettuale[2] del Wyoming ha la giurisdizione sul parco nazionale di Yellowstone, che si estende leggermente anche in Idaho e Montana. Supponiamo che uccidiate qualcuno nella parte del parco di Yellowstone che si trova in Idaho. Non vi potranno processare in Wyoming – la giurisdizione dove vi hanno arrestato – perché l’articolo III impone che siate processati in Idaho. Il sesto emendamento richiede invece che la vostra giuria risieda sia nello Stato (l’Idaho) sia nel distretto (Wyoming) dove è stato commesso il crimine. Significa che la vostra giuria dovrà essere composta da persone residenti nella parte del parco di Yellowstone che appartiene all’Idaho… dove però non ci sono residenti. Non esiste dunque un sistema costituzionale per condannarvi per omicidio. Nessuno ha ancora sfruttato questo hack per uccidere qualcuno impunemente, ma è stato usato dalla difesa in un caso di bracconaggio. Nel 2007, un uomo, nella parte del parco di Yellowstone appartenente al Montana, ha sparato illegalmente a un alce. I suoi avvocati hanno sfruttato proprio questo hack,[3] respinto però dal tribunale, in quanto avrebbe rafforzato il loophole della “zona della morte”. Così facendo, invece, ha neutralizzato l’hack attraverso una sentenza.

Sulle terre dei nativi americani viene spesso messa in atto una

versione ben più inquietante di questo hack.[4] Le *tribal court*, i tribunali dei nativi americani che hanno giurisdizione all'interno delle loro comunità, non possono processare i non nativi che commettono crimini sulle terre dei nativi; possono farlo solo le autorità federali, che però in un numero preoccupante di casi non agiscono. In tal modo i non nativi possono violentare le donne native sulle terre delle loro tribù quasi senza rischiare di subirne le conseguenze. Secondo i dati, l'80% delle donne native americane che subiscono violenza sessuale sono vittime di uomini non nativi.

Ancora un altro hack. Le enclavi federali sono porzioni di uno Stato appartenenti al governo federale, e da sempre rappresentano una vulnerabilità del sistema giuridico degli Stati Uniti. Tra le enclavi federali ci sono le basi militari, i tribunali, le prigioni e altri edifici federali, le foreste e i parchi nazionali. Hanno una denominazione diversa in quanto gli Stati di fatto ne cedono la proprietà al governo federale; per questo in tali enclavi non valgono più leggi statali e locali. Col tempo, il sistema legale ha cercato di applicare delle patch a questa vulnerabilità. Nel 1937, una sentenza della Corte Suprema stabilì che nelle enclavi federali si pagassero le tasse dei relativi Stati.[5] Nel 1970, nella sentenza per il caso Evans vs Cornman, la Corte Suprema sancì che i residenti delle enclavi federali[6] (ad esempio chi risiedeva in una abitazione privata sul territorio di un parco nazionale) potevano votare nelle elezioni del loro Stato. I tribunali hanno applicato altre patch, ma le enclavi federali hanno continuato a eludere un gran numero di leggi statali, comprese leggi penali, contro la discriminazione e a difesa dei lavoratori.

Chi risiede in un'enclave federale può inoltre aggirare le regole che vietano il *foie gras*. Il foie gras è il fegato di un'anatra o un'oca che ha subito il processo di *gavage*: l'animale viene soggetto ad alimentazione forzata due volte al giorno per un paio di settimane, fin quando il suo fegato raggiunge un volume dieci volte superiore al normale. Gli animalisti lo combattono da tempo e nel 2004 la California ha vietato la vendita e la produzione di foie gras. Negli anni a venire, questo divieto è stato più volte contestato in sede giuridica. Nel 2014, i proprietari del Presidio Social Club, un ristorante di San Francisco situato in un'enclave federale, hanno

obiettato che per loro il divieto della California non fosse valido.[7] Prima ancora che un tribunale potesse pronunciarsi, i proprietari si sono arresi alle proteste degli animalisti che manifestavano fuori dal ristorante. Non è stata pertanto detta l'ultima parola su questo hack.

In tutti questi aneddoti, il patch migliore è rivedere la legge per riparare la falla. È il Congresso che deve decidere di assegnare la zona della morte al distretto dell'Idaho. È il Congresso che deve dare alle nazioni indiane la giurisdizione e le infrastrutture necessarie a proteggere le donne e le ragazze native sui loro territori. Il Violence Against Women Act del 2013 ha posto parzialmente riparo a questa vulnerabilità, ma nel 2019 il rinnovo dell'autorizzazione è stato mandato all'aria dalla lobby delle armi,[8] per motivi che non hanno niente a che fare con questo particolare provvedimento.

1. Brian C. Kalt (2005), "The perfect crime", *Georgetown Law Journal* 93, n. 2, https://fliphtml5.com/ukos/hbsu/basic.
2. Le tredici corti distrettuali Usa sono tribunali federali di primo grado che hanno competenza territoriale su più Stati contigui (N.d.T.).
3. Clark Corbin (3 febbraio 2022), "Idaho legislator asks U.S. Congress to close Yellowstone's 'zone of death' loophole", *Idaho Capital Sun*, https://idahocapitalsun.com/2022/02/03/idaho-legislator-asks-u-s-congress-to-close-yellowstones-zone-of-death-loophole.
4. Louise Erdrich (26 febbraio 2013), "Rape on the reservation", *New York Times*, www.nytimes.com/2013/02/27/opinion/native-americans-and-the-violence-against-women-act.html.
5. Corte Suprema degli Stati Uniti (6 dicembre 1937), James *vs* Dravo Contracting Co. (Case No. 190), 302 U.S. 134, https://tile.loc.gov/storage-services/service/ll/usrep/usrep302/usrep302134/usrep302134.pdf.
6. Corte Suprema degli Stati Uniti (15 giugno 1970), Evans *vs* Cornman (Case No. 236), 398 U.S. 419, www.justice.gov/sites/default/files/osg/briefs/2000/01/01/1999-2062.resp.pdf.
7. Andrew Lu (16 luglio 2012), "Foie gras ban doesn't apply to SF Social Club?", *Law and Daily Life*, *FindLaw*, www.findlaw.com/legalblogs/small-business/foie-gras-ban-doesnt-apply-to-sf-social-club.
8. Indian Law Resource Center (aprile 2019), "VAWA reauthorization bill with strengthened tribal provisions advances out of the House", https://indianlaw.org/swsn/VAWA_Bill_2019. Indian Law Resource Center (2019), "Ending violence against Native women", https://indianlaw.org/issue/ending-violence-against-native-women.

CAPITOLO 28

L'hacking della burocrazia

Quando progettiamo una serie di regole, chi è chiamato a rispettarle[1] sovente ottimizza le proprie azioni perché rientrino in tali regole, anche se questo significa andare contro il loro obiettivo esplicito. Pensiamo a un disinfestatore che libera uno sciame di insetti per procurarsi più lavoro, o a un professore che insegna solo come superare i test, in modo che i suoi studenti ottengano punteggi più alti. Gli economisti la chiamano legge di Goodhart: quando è il rimedio stesso a diventare un obiettivo, significa che non è più un buon rimedio. Le regole burocratiche vengono pertanto hackerate costantemente da chi non vuole rispettarle.

I sistemi burocratici vengono hackerati dal basso, da chi vi è sottoposto, con lo scopo di ottenere qualcosa a discapito delle regole. Negli anni Ottanta, il dirigente Daniel Goldin hackerò la stagnante burocrazia della Nasa, scovando loophole normativi che gli consentirono di lanciare più sonde spaziali, e a un prezzo minore,[2] come la missione Pathfinder. Agenzie per l'innovazione come la 18F e lo US Digital Service hanno hackerato una serie di procedure d'appalto governative per implementare i progressi tecnologici alla velocità di internet. Gli esperti di tecnologia dei governi di Gran Bretagna e Canada hanno fatto lo stesso nei propri Paesi.

I sistemi burocratici vengono hackerati anche dai loro nemici. Pensiamo alla tecnica dello sciopero bianco, che permette di fare il proprio dovere in modo strategico, seguendo i regolamenti alla lettera, fino a un'inevitabile situazione di stallo. Alcuni esempi di sciopero bianco sono intuitivi: prendersi tutte le pause concesse, smettere di lavorare nel momento esatto in cui finisce l'orario. Un infermiere può rifiutarsi di rispondere al telefono perché non fa parte di quanto previsto dal suo contratto. È una tattica utilizzata da decenni, che ispirò la trama del romanzo satirico incompiuto di Jaroslav Hašek *Il buon soldato Švejk*, scritto negli anni Venti. Alcuni

tipi di sciopero bianco sono indubbiamente esempi di hack: ostinarsi a rispettare ogni formalità, richiedere un'infinità di scartoffie, seguire a menadito ogni indicazione. L'idea di base è quella di sabotare il sistema con le sue stesse regole.

Negli anni Ottanta, in Malesia esisteva un tipo di mezzadria chiamato *sewa padi*. In sostanza, l'affitto veniva richiesto dopo il raccolto, in base alla sua qualità.[3] Ovviamente i contadini effettuavano il raccolto di notte, di nascosto, prima che cominciasse il raccolto ufficiale; se i supervisori chiudevano un occhio, si sbarazzavano di un po' delle granaglie, oppure facevano una pessima trebbiatura, raccogliendo solo in seguito il riso rimasto sugli steli. Per giustificarsi, spargevano la voce che il raccolto era stato pessimo. Un comportamento in gran parte truffaldino, che per alcuni aspetti possiamo però considerare hacking. Il governo pose rimedio a questa vulnerabilità istituendo un nuovo sistema, il *sewa tunai*, basato su quote fisse da pagare prima della semina.

Un altro tipo di hack molto diffuso: nel 1902, il governo di Hanoi cercò di sterminare i topi offrendo ai cittadini una ricompensa per ogni coda consegnata.[4] In tanti pensarono che la cosa migliore da fare fosse intrappolare i ratti, tagliar loro la coda, e rimetterli in libertà in modo che potessero riprodursi, aumentando il numero di ratti da catturare. Nel 1989, a Città del Messico, per combattere l'inquinamento, venne decisa la circolazione a targhe alterne.[5] Molti cittadini decisero di comprarsi una seconda macchina, spesso vecchia e molto inquinante.

Più di recente, gli autisti Uber di Nairobi hanno trovato un hack per non pagare la percentuale all'azienda.[6] I passeggeri contattano gli autisti tramite la app di Uber, che stabilisce la tariffa. Quando l'autista arriva da chi l'ha contattato, i due si accordano per usare il metodo *karura*: la chiamata viene annullata sulla app e la corsa viene pagata in contanti.

Il fiasco del Boeing 737 Max è un tragico esempio delle negligenze normative che possono derivare dall'eccessiva vicinanza tra chi fa le regole e chi le deve rispettare. I regolatori della Faa, la Federal Aviation Administration, non esaminarono abbastanza nel dettaglio le modifiche apportate al Maneuvering Characteristics Augmentation

System (Mcas). Per colpa di questa leggerezza, due 737 Max si schiantarono in Indonesia (2018) e in Etiopia (2019), causando la morte di 346 persone.

Chiariamo bene qual è l'hack in questo caso. Gli esperti degli organismi di regolazione dovrebbero fare l'interesse dei cittadini. Una persona qualunque come me non se ne intende di sicurezza aerea (o automobilistica, o di adulterazioni alimentari, efficacia dei farmaci, contabilità bancaria). Tramite queste agenzie, il governo ci dovrebbe offrire le giuste competenze e stabilire regole che ci proteggano. È proprio questo meccanismo di supervisione che viene sovvertito.

Le inchieste sui disastri aerei stabilirono che c'era stato un problema normativo. Non c'era stata infatti alcuna valutazione indipendente del Mcas da parte della Faa, che si era affidata invece all'autovalutazione di Boeing. La Faa non disponeva delle giuste competenze, e il suo ufficio per la supervisione della sicurezza aerea aveva delegato gran parte del lavoro a Boeing. Agli ingegneri che avevano progettato gli aerei era stato pertanto assegnato il compito di certificare il proprio lavoro. In alcuni casi, i dirigenti della Faa si schierarono addirittura con Boeing,[7] e contro gli ingegneri che richiedevano cambiamenti in nome della sicurezza. La Faa cassò perfino alcune regole[8] per consentire alla Boeing di avvalersi di un sistema rapido di certificazione e vendere più in fretta i propri aerei. Nel complesso, il processo normativo della Faa venne hackerato da un'industria capace di creare un contesto all'insegna della regulatory capture, di incentivi perniciosi, di dilemmi etici e pericolosi buchi nella sicurezza.

Nel 2001, il Dipartimento di Giustizia si è accordato con la Boeing, stimando i danni degli incidenti per 2,5 miliardi di dollari. Potrà sembrare tanto, ma nei fatti non è stato così. Solo 243,3 milioni di dollari di multa sono stati pagati alla Faa, senza che Boeing dovesse ammettere alcuna colpa o incorrere in ulteriori accuse penali, malgrado fosse stata confermata una negligenza sistemica nel valutare la sicurezza.

Il rapporto molto stretto tra Boeing e i regolatori dimostra quanto sia necessario rivedere la divisione dei compiti tra chi fa le regole e le

aziende che le dovrebbero rispettare. L'onere di imporre una condotta responsabile spetta alle agenzie normative, e nel lungo periodo affidarsi eccessivamente alle autocertificazioni crea conflitti di interesse e atrofizza la supervisione pubblica. Cosa ancor più importante, bisogna fare in modo che chi si occupa di scrivere le leggi, prima di passare a lavorare per il settore che ha regolamentato, debba far passare un lungo periodo di "raffreddamento". Se i regolatori non si considerano servitori dei cittadini, ma futuri dipendenti delle aziende che dovrebbero tenere a bada, difficilmente verranno stabilite linee guida che fanno l'interesse generale.

1. Charles A.E. Goodhart (1984), *Monetary Theory and Practice: The UK Experience*, Springer, https://link.springer.com/book/10.1007/978-1-349-17295-5.
2. Howard E. McCurdy (2001), *Faster, Better, Cheaper: Low-Cost Innovation in the U.S. Space Program*, Johns Hopkins University Press.
3. James C. Scott (1985), *Weapons of the Weak: Everyday Forms of Peasant Resistance*, Yale University Press.
4. Michael G. Vann (2003), "Of rats, rice e race: The Great Hanoi Rat Massacre, an episode in French colonial history", *French Colonial History* 4, https://muse.jhu.edu/article/42110/pdf.
5. Lucas W. Davis (2 febbraio 2017), "Saturday driving restrictions fail to improve air quality in Mexico City", *Scientific Reports* 7, articolo 41652, www.nature.com/articles/srep41652.
6. Sean Cole (7 agosto 2020), "Made to be broken", *This American Life*, www.thisamericanlife.org/713/made-to-be-broken; Gianluca Iazzolino (19 giugno 2019), "Going Karura. Labour subjectivities and contestation in Nairobi's gig economy", *Development Studies Association*, Open University, Milton Keynes, www.devstud.org.uk/past-conferences/2019-opening-up-development-conference.
7. Natalie Kitroeff, David Gelles e Jack Nicas (27 giugno 2019), "The roots of Boeing's 737 Max crisis: A regulator relaxes its oversight", *New York Times*, www.nytimes.com/2019/07/27/business/boeing-737-max-faa.html.
8. Gary Coglianese, Gabriel Scheffler e Daniel E. Walters (30 ottobre 2020), "The government's hidden superpower: 'Unrules'", *Fortune*, https://fortune.com/2020/10/30/federal-law-regulations-loopholes-waivers-unrules.

CAPITOLO 29

Hacking e potere

L'hacking è un esercizio di potere. Un hack rafforza il potere di chi lo attua a discapito di qualcun altro all'interno del sistema, spesso a discapito di tutti gli altri. Viene attuato per gli scopi dell'hacker, con evidente sprezzo delle regole. (Vale anche per i tipici hacking informatici attuati dai ragazzi, dovuti solo alla curiosità: per quanto la curiosità spesso non faccia danni, non dobbiamo sottovalutare il valore della privacy).

Chi non ha potere si dedica all'hacking per sovvertire le strutture di potere. Lo fa per aggirare la burocrazia o per guadagno personale. Ben poche persone hanno voce in capitolo sui sistemi globali che influenzano le loro vite; spesso hackerarli è l'unica possibilità, e ovunque ci sia un sistema problematico ci sarà qualcuno che cercherà di hackerarlo. L'hacking può essere pertanto una reazione comprensibile a hack attuati dallo Stato o dalle élite, come ad esempio i gravami burocratici.

Per quanto però si possa pensare all'hacking come a un'azione dal basso contro il potere, in genere sono i potenti a usare gli hack per trarne ulteriore vantaggio. Come ho già detto, le più grandi banche americane hanno sguinzagliato i loro migliori avvocati per trovare i loophole nel Dodd-Frank Act, e hanno dato vita a una campagna di lobby multimilionaria, durata tre anni, perché i propri hack venissero normalizzati. Le banche sono tanto ricche e grandi da sfruttare le vulnerabilità del sistema. La ricchezza significa potere, e dal potere deriva la possibilità di fare legalizzare i loophole.

Gli hack di chi ha potere sono diversi da quelli di chi non ce l'ha. Criminali, dissidenti o singoli cittadini rappresentano delle anomalie, e possono agire in modo più agile. Possono hackerare più rapidamente i nuovi sistemi, ed è per questo che il loro potere può sembrare maggiore di quanto non sia. Sono però le istituzioni a poter hackerare i sistemi in modo più efficace, anche se riescono a capire

come farlo solo in un secondo tempo. Governi e grandi aziende, già potenti in partenza, sapranno sfruttare i loro hack meglio di un singolo individuo.

Le dinamiche di potere sono presenti tanto negli hack quanto nella loro normalizzazione.

I potenti (e per potenti intendo in genere i ricchi) dispongono di strumenti migliori per rendere duraturi i propri hack, al punto da non farli sembrare più sospetti, ma parte del modo normale di fare le cose. Probabilmente è così che ci appaiono gli hedge fund, i finanziamenti del venture capital e tutte le strategie per pagare meno tasse.

Questo è dovuto a motivi strutturali. Innanzitutto per sfruttare i loophole fiscali servono onerosi avvocati e commercialisti. Inoltre chi è più ricco ha più denaro da nascondere, ed è pertanto più motivato alla ricerca di loophole da sfruttare. In terzo luogo, i loophole fiscali occupano una zona grigia; i meno abbienti non dispongono di risorse finanziarie sufficienti a combattere le autorità del settore. Infine, le leggi non vengono fatte rispettare in modo rigoroso, ed è più difficile che venga chiesto ai ricchi di rendere conto dei propri espedienti per aggirarle.

Quanto vale per le tasse, è vero anche in contesti diversi. Per un hack riuscito in genere ci sarà bisogno di esperti specializzati, oppure delle risorse per ingaggiarli, o delle risorse per strutturare un sistema in modo che possa essere hackerato da quegli esperti. In tutti e tre i casi, chi è ricco e potente si troverà in vantaggio, e avrà gioco più facile nell'attuare hack su vasta scala.

Chi non appartiene alla maggioranza, chi è marginalizzato, le persone di generi ed etnie meno potenti, avranno meno opportunità di hackerare così come di farla franca. I loro eventuali crimini hanno un valore diverso. Alle donne viene insegnato che devono rispettare le regole, agli uomini bianchi che se vogliono le possono infrangere. Bisogna tenerlo a mente quando parliamo di hacking e potere.

I potenti sono anche in grado di mettere un freno agli hack di chi potente non è. Strategie sindacali come lo sciopero bianco hanno perso sempre più potere, soprattutto perché i sindacati sono stati progressivamente indeboliti. Il management è in genere ostile ai

sindacati e da sempre cerca di contrastarli facendo pressioni sul legislatore e sulla giustizia. Accade pertanto che molti dipendenti vengano licenziati senza giusta causa. Lo sciopero bianco viene sempre meno utilizzato, in quanto richiede che i partecipanti siano sindacalizzati, o comunque protetti da leggi sui licenziamenti.

Julie Cohen, professoressa di diritto a Georgetown, ha scritto che "nell'interpretazione del potere, le regole sono un danno, una cosa da aggirare".[1] Intende dire che chi è potente ha i mezzi per evitare i limiti imposti dalle regole. Una volta capito che era possibile hackerare i sistemi – in primo luogo i processi normativi che impedivano loro di fare come volevano – i potenti hanno sviluppato le competenze necessarie. Lo abbiamo visto nel caso delle banche, dei mercati finanziari e degli immobili di lusso.

Pensiamo a come nel 2016 il Senato degli Stati Uniti si sia rifiutato anche solo di prendere in considerazione la nomina di Merrick Garland alla Corte Suprema. È un hack: una sovversione del processo di nomina del Senato. Trovo molto interessante che non sia possibile stabilire o meno se questo hack sia stato normalizzato. Sappiamo che quattro anni dopo, quando è stata nominata Amy Coney Barrett, i repubblicani non sono stati puniti per la loro ipocrisia. Tutto sarà più chiaro la prossima volta che ci sarà un seggio vacante alla Corte Suprema, e uno dei partiti controllerà la presidenza e l'altro il Senato. Un Senato repubblicano si comporterà allo stesso modo? I democratici, sfrutteranno l'occasione, se si presenterà? Se la risposta a una di queste domande sarà sì, allora in futuro ci saranno nomine alla Corte Suprema solo quando Senato e presidenza saranno sotto il controllo dello stesso partito, visto che il Senato ha in tal modo il potere di hackerare il sistema.

Ecco perché è raro che a effettuare un hack siano persone svantaggiate, povere, o i dissidenti in un Paese autoritario. I loro hack vengono dichiarati illegali. I loophole fiscali dei poveri vengono bloccati dall'Irs. I sit-in e gli scioperi basati sul rallentamento del lavoro negli anni Trenta del Novecento erano molto diffusi, ma oggi non sono più protetti dalle leggi federali degli Stati Uniti. Non li consideriamo neanche più degli hack. Questo non significa che chi non ha il potere sia meno capace di hackerare il sistema, ma solo che

incontrerà maggiori difficoltà nel tentativo di normalizzare i propri hack. Quando esaminiamo un sistema, chiediamoci a chi serve e a chi non serve. Chi non viene servito a dovere da quel sistema, che si tratti di un potente o meno, cercherà di hackerarlo. Tutti proveranno a superare i limiti imposti dal sistema, ma è più probabile che siano i ricchi a riuscirci, evitandone anche le conseguenze.

1 Julie Cohen e Chris Bavitz (21 novembre 2019), “Between truth and power: The legal constructions of informational capitalism”, Berkman Klein Center for Internet and Society at Harvard University, https://cyber.harvard.edu/sites/default/files/2019-12/2019_11_21_Berkman_Julie_Cohen_NS.pdf.

CAPITOLO 30

Contro le regole

Per gli utenti, Uber è un servizio di taxi.[1] Sembra proprio un servizio di taxi. Funge da servizio di taxi. Ma se provi a chiederlo a Uber – o alla concorrenza – ti risponderà che non è un'azienda di taxi o di autonoleggio con conducente. Ti dirà che è un servizio internet che collega persone che guidano la macchina con persone che devono andare da qualche parte, e che gli autisti sono appaltatori indipendenti e non impiegati dell'azienda. Uber sostiene di non controllarli in alcun modo. Stabilisce le loro tabelle di marcia e gestisce i loro compensi, ma si tratta solo di una gentilezza. Stando a quanto sostiene Uber, l'azienda non ha nulla a che fare con le automobili, almeno per quanto riguarda i regolamenti governativi.

Le app di car sharing sono un hack dei servizi di taxi[2] o, in senso lato, di come la società cerca di gestire il trasporto su brevi distanze. Il loro business model consente di ignorare decine di leggi che regolano il settore di taxi e limousine, come quelle a protezione dei lavoratori e dei consumatori, le leggi sulla sicurezza sul lavoro, le leggi sulle licenze e sulle tariffe, e quelle che riguardano l'interesse pubblico. L'esperienza dei tassisti viene messa sotto esame, a differenza di quella degli autisti di Uber e Lyft (per quanto ora le cose, *obtorto collo*, stiano cambiando). Le aziende di taxi hanno l'obbligo di un minimo retributivo e di un massimo di auto circolanti contemporaneamente in ogni città. Lo stesso non si può dire di Uber e Lyft. L'elenco potrebbe continuare.

Tutto è iniziato nel 2012 circa, e da allora Uber ha sfruttato il proprio vantaggio competitivo su taxi e limousine per imporsi sul mercato.[3] Secondo le cifre del 2021, è operativa in diecimile città di settantadue diversi Paesi, con un totale di diciannove milioni di corse al giorno. Tre milioni e mezzo di autisti lavorano per Uber,[4] al servizio di novantatré milioni di clienti al mese. Eppure Uber non riesce ancora a ricavarne dei profitti.

Le amministrazioni cittadine di tutto il mondo hanno cercato di porre riparo alle vulnerabilità sfruttate da Uber per hackerare il mercato dei taxi, con risultati contrastanti. Nel 2017, il tribunale competente dell'Unione Europea ha stabilito che Uber è un servizio di trasporti, e non, come dichiarava per aggirare le leggi in materia, un'azienda tecnologica. Nel 2017, la Corte d'appello della Gran Bretagna ha stabilito che gli autisti di Uber sono dipendenti della società, e non, come sostenuto da Uber, appaltatori indipendenti. La Corte di cassazione francese nel 2020 ha preso una decisione simile. Negli Stati Uniti, in California, nel 2019 è stata approvata una legge che impone ad aziende come Uber di trattare i propri lavoratori come dipendenti; Uber ha fatto ricorso, e il dibattito prosegue. Altre città e Stati stanno cercando di fare lo stesso, anche se la maggior parte degli Stati ha già emanato sue proprie norme sul tema.

In modo molto simile, Airbnb hackera il settore alberghiero.[5] Offre pernottamenti a breve termine, diversi però da quelli degli hotel. Non essendo un'azienda di hotel, Airbnb ritiene di non dover sottostare alle loro stesse leggi, regole e tasse di soggiorno. Airbnb non possiede alcuna proprietà, e si pone come azienda tecnologica. I proprietari degli alloggi sono contractor indipendenti, responsabili del pagamento delle tasse e del rispetto delle norme locali. Naturalmente, spesso non lo fanno. Le amministrazioni locali possono scegliere di farla passare liscia ad Airbnb oppure di contrattaccare. Alcune amministrazioni hanno cercato di limitarne l'espansione, ma Airbnb ha fatto loro causa (senza smettere di essere operativa): il risultato sono state lunghe battaglie in tribunale. Airbnb ha inoltre spesso utilizzato i proprietari degli immobili come lobbisti sul territorio, avvisandoli che l'amministrazione cittadina era intenzionata a mettere le mani sui loro soldi, dando anche indicazioni sulle assemblee alle quali partecipare.

Queste due aziende sono solo due esempi della *gig economy*, caratterizzata da tentativi di hackerare le leggi sul lavoro, le leggi a tutela dei consumatori e altre norme e regole. TaskRabbit, Handy e DoorDash usano gli stessi hack, proprio come Amazon, che di fatto per le consegne gestisce un sistema privato in stile Uber. I suoi autisti sono lavoratori autonomi, e pertanto l'azienda può ignorare tutte le

leggi che devono rispettare i comuni corrieri.

Non ci sorprende che le aziende cerchino di hackerare le regole. Ma nel caso delle aziende di car sharing e di noleggio e prestito a breve termine, aggirare le regole è un punto chiave del loro business model. Molti servizi *disruptive* della gig economy non sarebbero sostenibili se dovessero aderire alle stesse regole delle aziende "normali" che fanno loro concorrenza. Di conseguenza, le nuove aziende – e il venture capital che le sostiene – sono disposte a spendere cifre incredibili per combattere le regole vigenti. Le conseguenze sono due. La prima è evidente: la concorrenza, costretta a seguire le regole, si trova in una posizione di svantaggio. La seconda conseguenza è che la possibilità di generare un profitto a lungo termine da parte di queste nuove aziende dipenderà o da una violazione continuata delle regole (e, di conseguenza, dallo sfruttamento di lavoratori mal pagati) o dalla completa sostituzione dei loro lavoratori con le macchine.

Il governo, a livello centrale e locale, ha provato a mettere una patch a queste vulnerabilità, e la risposta delle aziende ci fa capire fin dove sono disposte a spingersi. Dopo la sentenza della Corte Suprema dello Stato della California del 2018 e dopo la legge statale del 2019 che abbiamo già citato, molte aziende della gig economy si sono associate per proporre un referendum (la Proposition 22) che avrebbe privato i loro gig worker di molte difese: non sarebbero stati più considerati impiegati, niente più salari minimi, niente assicurazioni sulla disoccupazione, niente assicurazioni mediche ecc. Guidate da Uber, Lyft e DoorDash, le aziende della gig economy hanno speso 200 milioni di dollari per sostenere questo referendum e convincere i lavoratori che era per il loro bene. È stato approvato nel 2020, mandando all'aria i tentativi della California di proteggere i lavoratori. La battaglia non è finita, e senza dubbio dopo la pubblicazione di questo libro ci saranno ulteriori sviluppi.

Probabilmente potrei scrivere un libro intero su come le aziende hackerano le regole che limitano i loro profitti, ma vi darò solo un altro paio di esempi. I *payday loan*[6] sono prestiti a breve termine pensati per i più poveri: cifre esigue concesse a tassi d'interesse astronomici. Quattro quinti delle persone che chiedono questi

prestiti, si trovano costrette a rinnovarli, volenti o nolenti, e finiscono intrappolate in un circolo vizioso di debiti, interessi e commissioni, che portano in media il tasso d'interesse al 400% annuo più commissioni. Alcuni Stati hanno cercato di regolare il settore dei prestiti a breve termine, riducendo i tassi esigibili, ma le aziende di payday loan hanno sempre trovato il modo di aggirare le regole. Si sono trasformate in aziende che offrono prestiti rateali, e non prestiti da ripagare totalmente con la prossima busta paga, sfuggendo così alla definizione di "payday loan" (il prestito del giorno di paga). Operano inoltre come *loan broker*:[7] intermediari che possono stabilire tariffe esenti da qualunque restrizione. In Montana, alcune aziende di payday loan si sono trasferite nelle riserve indiane per evitare le normative statali e federali.[8] Nel 2020, il Consumer Financial Protection Bureau (Cfpb) ha cassato una serie di nuove regole che avrebbero limitato le pratiche rapaci di queste aziende.

Un ultimo esempio. Durante la pandemia di Covid-19, Usa e Canada hanno impedito di oltrepassare i loro confini per viaggi non essenziali via terra. Ci si poteva spostare in volo tra i due Paesi, ma chi lo faceva in auto era soggetto a restrizioni di ogni tipo. Era senza dubbio un problema per gli "*snowbirds*" canadesi, i ricchi che vanno a svernare negli Stati Uniti. Esisteva però un loophole:[9] le merci si potevano ancora spostare. Un'azienda di trasporti di Hamilton, Ontario, ha proposto pertanto una scappatoia: il cliente poteva far arrivare la propria auto con un camion negli Usa, all'aeroporto di Buffalo, dove l'avrebbe potuta riprendere arrivando in elicottero. Chi si poteva permettere questo servizio, era pertanto in grado di aggirare completamente le normative sulla chiusura dei confini.

Dovunque ci sia una regola, c'è qualcuno che la subisce. In genere le regole sono utili, ma possono anche favorire chi è già privilegiato, intralciare l'innovazione e sostenere idee obsolete. Le nuove aziende cercano pertanto le vulnerabilità presenti in queste leggi, e ideano hack per rispettarle formalmente e al tempo stesso violarne lo spirito. Non c'è regola che non sia incompleta o in qualche modo incoerente, pertanto non c'è regola che non si presti a venire hackerata.

Tutto questo ci pone di fronte a un importante quesito: come

impedire gli hack di corporation ricche, potenti e tecnologicamente all'avanguardia, aziende la cui stessa esistenza dipende dalla loro capacità di hackerare le regole? Quale può essere una soluzione brillante e resiliente a questo problema?

Una possibile misura di sicurezza è sottoporre a un red team ogni nuova regola prima di attuarla. Secondo Jeremy Rosenblum, un avvocato di Philadelphia che fa da consulente alle società di payday loan, le aziende cercano costantemente di sviluppare prodotti finanziari prima che le regole si mettano di mezzo:[10] "Chi opera in questo mercato deve sempre considerare delle strategie alternative, nel caso il Cfpb stabilisca qualche nuova regola". È la stessa filosofia che ritroveremo nelle aziende prese in esame nei prossimi capitoli. Per contrastarla, chi fa le regole deve essere proattivo, e individuare in anticipo le possibili vulnerabilità e le reazioni delle aziende. In tal modo, potranno prevedere e prevenire azioni e innovazioni finanziarie socialmente nocive.

Bisogna inoltre puntare sulla vigilanza costante e sull'agilità. Certo, si può sperare – o credere – che una norma efficace possa prevenire ogni possibile hack, ma il regolatore deve essere pronto a ogni contromossa inattesa e potenzialmente deleteria. Per combatterle, deve monitorare le aziende ed essere pronto ad agire in fretta per occuparsi dei nuovi prodotti finanziari nati dopo la regolamentazione del settore. Deve sapere che non sempre il primo intervento è risolutivo, e che dovrà progressivamente mettere patch alle vulnerabilità che si manifesteranno.

1. L'azienda inizialmente si chiamava UberCab ma ha cambiato nome proprio per questo motivo.
2. Ruth Berens Collier, Veena Dubal e Christopher Carter (marzo 2017), "The regulation of labor platforms: The politics of the Uber economy", University of California Berkeley, https://brie.berkeley.edu/sites/default/files/reg-of-labor-platforms.pdf.
3. Uber Technologies, Inc. (2021), "2021 Form 10-K Annual Report", US Securities and Exchange Commission, www.sec.gov/ix?doc=/Archives/edgar/data/1543151/000154315122000008/uber-20211231.htm.
4. Brian Dean (23 marzo 2021), "Uber statistics 2022: How many people ride with Uber?" *Backlinko*, https://backlinko.com/uber-users.
5. Paris Martineau (20 marzo 2019), "Inside Airbnb's 'guerilla war' against local governments", *Wired*, www.wired.com/story/inside-airbnbs-guerrilla-war-against-local-governments/.
6. Carter Dougherty (29 maggio 2013), "Payday lenders evading rules pivot to installment loans", *Bloomberg*, www.bloomberg.com/news/articles/2013-05-29/payday-lenders-evading-rules-pivot-to-installmant-loans.
7. S. Lu (22 agosto 2018), "How payday lenders get around interest rate regulations", *WRAL* (in precedenza sul blog MagnifyMoney), www.wral.com/how-payday-lenders-get-around-interest-rate-regulations/17788314.
8. Liz Farmer (4 maggio 2015), "After payday lenders skirt state regulations, Feds step in", *Governing*, www.governing.com/topics/finance/gov-payday-lending-consumer-crackdown.html.
9. Dave McKinley e Scott May (30 novembre 2020), "Canadians buzz through Buffalo as a way to beat border closure", *WGRZ*, www.wgrz.com/article/news/local/canadians-buzz-through-buffalo-as-a-way-to-beat-border-closure/71-07c93156-1365-46ab-80c1-613e5b1d7938.
10. Carter Dougherty (29 maggio 2013), "Payday lenders evading rules pivot to installment loans", *Bloomberg*, www.bloomberg.com/news/articles/2013-05-29/payday-lenders-evading-rules-pivot-to-installmant-loans.

CAPITOLO 31

Interazioni tra diverse giurisdizioni

Il loophole fiscale “Double Irish with a Dutch Sandwich” usato da aziende come Cisco, Pfizer, Merck, Coca-Cola e Facebook per non pagare le tasse negli Usa era il frutto dei limiti imposti alle leggi dai confini nazionali. Un uso scaltro delle sussidiarie straniere e il trasferimento a esse di diritti e introiti, ha permesso a grosse aziende americane di non pagare le tasse su gran parte del proprio reddito globale. (Nel frattempo i singoli cittadini statunitensi vengono tassati sul proprio intero reddito, a prescindere da dove lo guadagnino: questo trucchetto vale solo per le corporation).

È solo uno dei molti hack basati sui paradisi fiscali sparsi nel mondo, un tipo di elusione che costa agli Usa quasi 200 miliardi di dollari l’anno,[1] pari a circa l’1,1 % del loro prodotto interno lordo. Il costo totale per il gettito fiscale globale,[2] a seconda della stima, oscilla tra i 500 e i 600 miliardi di dollari. La cosa interessante è che questi hack sfruttano le interazioni tra vulnerabilità di diversi Paesi.

Per risolvere questo problema servono semplicità e trasparenza. Negli Usa, ventisei Stati e il Distretto di Columbia hanno adottato il Combined Reporting System for State Corporate Income Tax,[3] che aiuta a prevenire il trasferimento dei profitti tra varie giurisdizioni interne. Sottoposte a diversi sistemi, le aziende e le loro sussidiarie devono dichiarare i propri profitti totali (o meglio, i propri profitti “domestici” totali) e in che percentuale i propri affari si svolgono in una determinata giurisdizione (ad esempio uno Stato). Tale giurisdizione può tassare l’azienda per una quota del profitto proporzionata al volume d’affari da essa svolto sul proprio territorio: in tal modo le aziende non possono evadere le tasse sfruttando l’interazione fra diverse giurisdizioni e l’eventuale spostamento dei profitti. È un approccio che ha già permesso di recuperare miliardi di dollari di gettito fiscale, in precedenza occultati sfruttando i paradisi fiscali interni.

Questa innovazione non ha però risolto il problema più vasto dell'evasione fiscale a livello internazionale. In primo luogo, quasi tutti gli Stati americani che utilizzano un sistema di dichiarazione combinato (con l'eccezione notevole del Montana) non richiedono alle aziende di dichiarare i propri profitti offshore, consentendo loro di evadere le tasse sui profitti interni trasferiti all'estero. In secondo luogo, come ho già sottolineato, le tasse sul reddito non si basano sui profitti esteri, cosa che agevola l'elusione fiscale e il trasferimento dei profitti all'estero a livello federale.

Il Tax Cuts and Jobs Act del 2017 è stato un tentativo poco convinto di risolvere tale problema per mezzo della Global Intangible Low Tax Income Provision, che richiedeva alle aziende di pagare una tassa nominale del 10,5 % sui profitti non tassati dei paradisi fiscali all'estero, ma che non è riuscito a causare un significativo spostamento dei profitti a livello internazionale.

Mi sembra invece molto più efficace il Mandatory Worldwide Combined Reporting (Mwcr) un metodo d'esemplare semplicità e chiarezza per affrontare una questione complessa quale quella delle giurisdizioni fiscali. Somiglia a un sistema di dichiarazioni combinate, e stabilisce che un'azienda e le sue sussidiarie dichiarino non solo i propri profitti complessivi a livello mondiale, ma anche la percentuale riconducibile alle singole giurisdizioni (in genere espressa tramite il fatturato). Tali giurisdizioni possono di conseguenza tassare una quota dei profitti proporzionata al giro d'affari dell'azienda in quel luogo.

Mentre scrivo, l'amministrazione Biden e l'Ocse, che comprende una serie di Paesi sviluppati, stanno dandosi da fare per realizzare qualcosa del genere. Nel 2021, l'Ocse ha annunciato che già centotrenta Paesi e giurisdizioni hanno accettato di tassare le più grandi aziende multinazionali a un tasso minimo del 15% dei profitti effettuati nei rispettivi territori, superando il sistema attuale, nel quale le aziende vengono tassate solo nella propria "madrepatria". La proposta di Biden è simile, ma con alcune differenze rilevanti; ad esempio si rivolge a una gamma molto più ampia di organizzazioni a scopo di lucro. Staremo a vedere l'evoluzione di queste proposte e come le corporation – come già fatto con le riforme passate –

cercheranno di hackerarle.

A volte sono gli Stati stessi a facilitare tale arbitraggio giurisdizionale intervenendo sulle proprie leggi per attirare denaro da tutto il mondo. Ad esempio il sistema della "bandiera di comodo", utilizzato per registrare le navi, ha reso più semplice evitare le leggi sulla manutenzione delle flotte e quelle in difesa dei lavoratori, oltre a mettersi a riparo dalle inchieste per danni ambientali come quelli dovuti alle fuoriuscite di petrolio. Storicamente, le navi sventolavano la bandiera del proprio Paese, ricevendone la tutela e accettandone le leggi. All'inizio del Ventesimo secolo, Panama concesse a chiunque di issare bandiera panamense in cambio di una somma di denaro. La pratica venne ripresa da Paesi come Liberia e Singapore, diventando una grossa opportunità di guadagno per Stati con poche risorse naturali, come la Repubblica di Vanuatu. Si trattava di un hack amatissimo dagli armatori, viste le esigue legislazioni di questi Paesi. Tra gli anni Cinquanta del Novecento e gli anni Dieci del nuovo millennio, la quantità di navi appartenenti a questi "registri aperti" è passata dal 4 al 60%. La Convenzione delle Nazioni Unite sul diritto del mare del 1994 specifica che ci deve essere un "legame effettivo" tra una nave e la sua bandiera, ma più di un quarto di secolo dopo ancora si dibatte su come interpretare questa espressione.

È per lo stesso motivo che le aziende si registrano in Delaware. All'inizio del Diciannovesimo secolo il Delaware fu il primo Stato americano ad adattare la propria legislazione fiscale col fine di attirare investitori da Stati più grandi e ricchi come quello di New York. Il Delaware divenne un paradiso fiscale "onshore" per le aziende statunitensi, non solo perché semplificava gli affari, ma anche grazie al "Delaware loophole":[4] lo Stato non esige alcuna tassa sul reddito derivante da asset intangibili appartenenti a una holding del Delaware. In tal modo le aziende possono girare a una holding in Delaware i proventi di royalties e similari,[5] evitando di pagare le tasse, con una perdita di milioni di dollari per gli Stati dove sono effettivamente operative. Un loophole che costa circa un miliardo di dollari l'anno agli altri quarantanove Stati.[6]

L'hack non sta nel fatto che le aziende registrino le proprie navi a Panama o che si registrino in Delaware, ma che queste giurisdizioni

si rendano più desiderabili sfruttando le normative esistenti. Il Delaware si contrappone agli altri Stati, sovvertendo l'intento della normativa commerciale federale e l'autorità fiscale degli Stati. Allo stesso modo, le bandiere di comodo sovvertono l'intento della Convenzione delle Nazioni Unite sul diritto del mare.

Sono tutti esempi nei quali gli hack sono resi possibili dal fatto che un'organizzazione sia più grande dell'organismo che le regola. Le corporation in genere fanno affari dentro e fuori il Delaware. Le aziende che trasportano merci via mare operano a livello mondiale, ben oltre Panama. Sta accadendo lo stesso con le grandi aziende tecnologiche. Non esiste istituzione pubblica in grado di domarle dal punto di vista normativo. Aziende come Facebook sono globali ma sono sottoposte a regolamenti nazionali. Non esistono ancora strutture normative adatte all'era dell'informazione, ed è per questo che le aziende possono sfruttare a proprio vantaggio i conflitti giurisdizionali.

1. Alex Cobham e Petr Jansky (marzo 2017), “Global distribution of revenue loss from tax avoidance”, United Nations University *WIDER Working Paper* 2017/55, www.wider.unu.edu/sites/default/files/wp2017-55.pdf.
2. Ernesto Crivelli, Ruud A. de Mooij e Michael Keen (29 maggio 2015), “Base erosion, profit shifting and developing countries”, *International Monetary Fund Working Paper* 2015118, www.imf.org/en/Publications/WP/Issues/2016/12/31/Base-Erosion-Profit-Shifting-and-Developing-Countries-42973.
3. Center for Budget and Policy Priorities (2019), “28 states plus D.C. require combined reporting for the state corporate income tax”, www.cbpp.org/27-states-plus-dc-require-combined-reporting-for-the-state-corporate-income-tax.
4. The Institute on Taxation and Economic Policy (dicembre 2015), “Delaware: An onshore tax haven”, https://itep.org/delaware-an-onshore-tax-haven/.
5. Patricia Cohen (7 aprile 2016), “Need to hide some income? You don’t have to go to Panama”, *New York Times*, www.nytimes.com/2016/04/08/business/need-to-hide-some-income-you-dont-have-to-go-to-panama.html.
6. Leslie Wayne (30 giugno 2012), “How Delaware thrives as a corporate tax haven”, *New York Times*, www.nytimes.com/2012/07/01/business/how-delaware-thrives-as-a-corporate-tax-haven.html.

CAPITOLO 32

Il carico amministrativo

Ci sono hack che nascono per necessità, dal dover adattarsi a circostanze avverse. Se una tattica non funziona se ne prova un'altra. In questo capitolo parleremo degli hack attuati tramite il cosiddetto "carico amministrativo". In genere il suo obiettivo è il welfare, dalle assicurazioni per la disoccupazione al Medicaid, tutte cose molto dibattute negli Stati Uniti. Chi si oppone a queste politiche cerca in primo luogo di abolirle, ma a volte non ci riesce, per mancanza di voti o perché si mette di mezzo quell'impicciona della Costituzione.

Ma la difficoltà aguzza l'ingegno. Chi ha il compito di applicare le leggi può renderle molto difficili da rispettare, soffocandone le finalità e intralciando chi volesse raggiungerle con un'infinità di ostacoli burocratici. Le possibilità non mancano – lunghi tempi d'attesa, moduli a non finire, archivi insensati, colloqui a ripetizione, siti impossibili da navigare – e l'obiettivo è sempre lo stesso: rendere l'accesso a certi benefit un miraggio per chi avrebbe invece tutto il diritto di ottenerli, persone spesso già gravate da povertà, malattie, scarsa istruzione e mancanza di una fissa dimora. Gli studiosi di politiche pubbliche Pamela Herd e Donald Moynihan hanno ribattezzato administrative burden, carico amministrativo, questo fenomeno,[1] che possiamo considerare un hack delle decisioni politiche.

Un buon esempio è quanto accade in Florida con le assicurazioni per la disoccupazione.[2] Secondo un consigliere del governatore DeSantis, tale sistema è stato volutamente pensato per "rendere più difficile ottenere e mantenere i propri sussidi". L'intero sistema per fare domanda è stato messo online su un sito a malapena funzionante. Una verifica del 2019 ha riscontrato che spesso "segnala errori inesistenti" e blocca del tutto l'inserimento della domanda.[3] Si tratta inoltre di un modulo suddiviso su molte pagine: dopo aver inserito solo pochi dati, come nome e data di nascita, ti costringe a

passare alla pagina successiva, moltiplicando la possibilità che il sito si blocchi e rimandandoti alla casella di partenza. Il sito è inoltre accessibile solo in determinati orari[4] e richiede a chi fa domanda di tornare sulle sue pagine ogni due settimane per "verificare le proprie richieste". Questo sistema ha causato particolari problemi per 4,5 milioni di abitanti della Florida rimasti disoccupati per colpa del Covid-19. Nel 2020, in tanti hanno dovuto passare ore o giorni interi a cercare di inserire la domanda.[5] Secondo il sito, alla fine 2,4 milioni di persone sono state dichiarate inidonee da questo sistema poco trasparente. Di conseguenza, quei cittadini hanno avuto anche maggiori difficoltà ad accedere al Fondo federale di disoccupazione per la pandemia Cares Act.

Alcuni carichi amministrativi sono il frutto di differenze legittime nell'applicazione di una politica. Nell'ideazione di qualunque sistema che attribuisca un sussidio economico bisogna fare attenzione a due tipi di errore: il primo è che qualcuno che ne ha diritto non riceva il benefit, il secondo è che chi non ne ha diritto lo riceva. Rendere troppo semplice una cosa, faciliterà l'altra. Se sarà troppo facile ottenere un benefit, anche chi non dovrebbe ottenerlo potrà approfittarne. Se invece il processo di selezione sarà troppo complicato, verranno tagliate fuori alcune persone a cui spetterebbe. C'è chi preferirà correre il primo rischio e chi il secondo, a seconda dell'inclinazione politica.

Creare apposta dei carichi amministrativi significa estremizzare questo aspetto e non limitarsi a negare il sussidio ai non aventi diritto, ma a spingere anche chi ne avrebbe diritto ad arrendersi. È un rifiuto passivo-aggressivo.

Negli Usa questa tattica viene usata ad esempio per l'aborto, costituzionalmente legale da circa cinquant'anni. Una volta nelle condizioni di non poter più vietarlo, alcuni Stati hanno creato carichi amministrativi sull'accesso effettivo a questo diritto, pur restando tecnicamente nella legalità. Ad esempio hanno imposto periodi d'attesa, colloqui obbligatori, la necessità di farsi visitare in diverse cliniche, il consenso dei genitori ed ecografie forzate. Lo Stato che ha più calcato la mano è la Louisiana,[6] che dal 1973 a oggi ha imposto ottantanove nuove regolamentazioni dell'aborto, costringendo ad

esempio le cliniche a richiedere costose certificazioni con la minaccia di chiusura immediata anche in caso di lievi violazioni burocratiche. Nel 1992, la Corte Suprema degli Stati Uniti stabilì[7] che gli Stati non dovevano "porre ostacoli significativi alle donne che richiedevano di abortire", e nei trent'anni successivi si è combattuto per definire che cosa volesse dire "significativo".

Possiamo fare molti altri esempi. Il programma alimentare del governo Women, Infants and Children (Wic) impone restrizioni dettagliate, interminabili, e quasi comicamente complicate sui cibi che si possono comprare. Ad esempio, non è possibile mescolare diverse marche di cibo per bambini. Si tratta di un carico amministrativo efficace: meno della metà delle famiglie che potrebbero ottenere i benefit del Wic li ricevono davvero.[8] Allo stesso modo è possibile hackerare anche il processo per richiedere e ottenere i buoni alimentari e il Medicaid. L'Arkansas è riuscito a tagliare fuori molte persone dal Medicaid richiedendo una certificazione lavorativa: il problema non stava tanto nel rientrare nei parametri, ma nel fatto che in tanti non riuscissero a compilare i moduli necessari.

Questi sono esempi di come ricchi e potenti hackerino i sistemi a discapito del cittadino medio. Gli effetti penalizzano in modo sproporzionato chi non dispone di capacità, risorse e tempo per superare tali ostacoli.

Difficile trovare una soluzione all'infuori di un intervento giudiziario, visto che sono proprio le autorità politiche a creare questi carichi amministrativi. Una soluzione parziale potrebbe essere l'utilizzo di benchmark indipendenti o di controlli esterni per determinare dimensioni e impatto di un carico amministrativo. In questo modo non si risolverebbe direttamente il problema, ma perlomeno, quantificandone l'impatto sui cittadini (soprattutto su quelli appartenenti a classi giuridicamente tutelate), chi si occupa delle valutazioni – raccogliendo, studiando e condividendo dati di alta qualità – potrebbe convincere il legislatore ad agire o potrebbe innescare un movimento d'opinione dal basso. Per il resto, non saprei proprio che cosa fare.

1. Pamela Herd e Donald P. Moynihan (2019), *Administrative Burden: Policymaking by Other Means*, Russell Sage Foundation.
2. Rebecca Vallas (15 aprile 2020), "Republicans wrapped the safety net in red tape. Now we're all suffering." *Washington Post*, www.washingtonpost.com/outlook/2020/04/15/republicans-harder-access-safety-net.
3. Redazione di Vox (10 giugno 2020), "Why it's so hard to get unemployment benefits", *Vox*, www.youtube.com/watch?v=ualUPur6iks.
4. Emily Stewart (13 maggio 2020), "The American unemployment system is broken by design", *Vox*, www.vox.com/policy-and-politics/2020/5/13/21255894/unemployment-insurance-system-problems-florida-claims-pua-new-york.
5. Palm Beach Post Editorial Board (30 novembre 2020), "Where is that probe of the broken Florida unemployment system, Governor?", *Florida Today*, https://eu.floridatoday.com/story/opinion/2020/11/30/where-probe-broken-florida-unemployment-system-governor/6439594002/.
6. Elizabeth Nash (11 febbraio 2020), "Louisiana has passed 89 abortion restrictions since Roe: It's about control, not health", Guttmacher Institute, www.guttmacher.org/article/2020/02/louisiana-has-passed-89-abortion-restrictions-roe-its-about-control-not-health.
7. Corte Suprema degli Stati Uniti (29 giugno 1992), Planned Parenthood of Southern Pennsylvania *vs* Casey, 505 U.S. 833 (1992), www.oyez.org/cases/1991/91-744.
8. L.V. Anderson (17 febbraio 2015), "The Federal Nutrition Program for Pregnant Women is a bureaucratic nightmare", *Slate*, https://slate.com/human-interest/2015/02/the-wic-potato-report-a-symptom-of-the-bureaucratic-nightmare-that-is-americas-welfare-system.html.

CAPITOLO 33

L'hacking della common law

I sistemi complessi che stiamo osservando tendono a essere troppo o troppo poco definiti, e sono noti come *wicked problems*. Significa che sono troppo complessi per le tecniche di analisi tradizionali.[1] Le uniche soluzioni tendono a essere iterative. Una soluzione iterativa può tanto essere hackerata quanto usare gli hack per migliorarsi.

Gli hack prevedono la contraddizione delle regole di un sistema. Le regole sono però in genere soggette a interpretazione e le interpretazioni sono mutevoli. Per capirlo meglio, prendiamo in esame un sistema giuridico pensato per evolversi in questo modo: la *common law*. La common law è l'esempio migliore – oltre che un modello per il futuro – di grande sistema in grado di adattarsi per mezzo di un hacking iterativo. Questa sua caratteristica è integrale alla progettazione del sistema. E funziona.

Nel 1762, lo scrittore e insegnante John Entick venne accusato di scrivere pamphlet diffamatori contro il governo inglese. I messaggeri del re, agli ordini del segretario di Stato, fecero irruzione in casa di Entick, sequestrandogli centinaia di faldoni e libelli, da usare come prove contro di lui. In modo del tutto inatteso, Entick fece causa ai messaggeri per aver violato la sua proprietà, per quanto l'avessero fatto per applicare la legge. Oggi potrà non sembrarci un hack, ma nel 1765 si trattava di un utilizzo della legge sull'inviolabilità del domicilio inatteso e non voluto. Prima di allora, tale legge veniva usata solo per evitare che un cittadino entrasse nella proprietà di un altro, ma non limitava l'azione del governo. Si presupponeva che la polizia, nello svolgimento delle proprie funzioni, avesse il diritto di perquisire la casa di un individuo. Entick sostenne invece che il diritto del soggetto sulla sua proprietà era di ordine superiore. Sovvertì le norme esistenti su come la legge dovesse venire applicata. Si trattava di un'interpretazione avanzata – o addirittura estrema – della legge, ma i tribunali inglesi ne stabilirono la validità:[2] "Secondo

le leggi d'Inghilterra, ogni invasione della proprietà privata, seppur minima, è una violazione". La sentenza del caso Entick ampliò la perseguibilità per violazione di domicilio al segretario di Stato e i suoi sottoposti. Da allora divenne parte della common law inglese. Entick hackerò la legge sulla violazione di domicilio. Propose un'interpretazione che seguiva la lettera della legge dal punto di vista logico, per quanto fosse inattesa e non voluta. Il tribunale consentì quell'hack e lo rese legge. Il caso Entick divenne una pietra miliare per come ridefiniva le libertà civili degli individui e limitava il potere dello Stato. Negli Stati Uniti, lo spirito della sentenza Entick è racchiuso nel quarto emendamento.

A volte un hack ha un effetto positivo. Può violare l'intento di una norma o una regola vigente, ma non è detto che violi il contratto sociale in generale. Nell'esempio che abbiamo appena visto, il tribunale decise che il contratto sociale prevedeva che i cittadini si sentissero al sicuro nelle loro proprietà e che la privacy delle loro case non dovesse essere violata da nessuno per alcun motivo. Un hack porta beneficio all'hacker, mentre un'altra parte del sistema ne fa le spese. A volte, però, si tratta di spese molto irrisorie. Un hack che rispetta lo spirito del contratto sociale può diventare un'innovazione salutare per il sistema.

In questi casi, non è un solo organismo pubblico a decidere, ma molti tribunali che cercano di ricondurre a una serie di precedenti le proprie interpretazioni da applicare a nuovi hack strada facendo. Le regole della common law possono essere un gran pasticcio: complicato, incompleto e sovente contraddittorio. A differenza delle leggi ordinarie, non vengono ideate con uno scopo generale. Sono iterative e si evolvono tramite il contributo di molte persone, ognuna con uno scopo diverso. Nei sistemi governati da una molteplicità di soggetti serve un meccanismo diverso per valutare le sfide allo status quo e i tentativi di sovvertirlo. È così che funziona la common law.

Una definizione sintetica: la common law è una legislazione che deriva dalle decisioni giurisprudenziali, vale a dire dai precedenti legali. Si differenzia dalla legge codificata (*civil law*), approvata da un legislatore, e dai regolamenti, stabiliti da organi amministrativi. La common law è più flessibile della legge codificata. Può mantenersi

coerente nel tempo, ma anche evolversi, grazie al lavoro di giudici che riapplicano, trovano analogie e trasformano i precedenti per adattarsi alle nuove circostanze. Tale evoluzione è essenzialmente una serie di hack passati in giudicato, e che pertanto o sono stati dichiarati illegali o sono degni di essere considerati dei precedenti.

Pensiamo ad esempio alla legge sui brevetti. Si basa sulla legislazione ordinaria, ma i suoi dettagli sono stati per larga parte decisi da pronunce giudiziarie. Ed è una legge molto complicata. I brevetti possono valere milioni e le cause legali sono all'ordine del giorno. Vista la posta in palio, gli hack del sistema non mancano di certo. Proverò a farvi un esempio: le ingiunzioni sui brevetti. Chi vede violato un proprio brevetto può ottenere una rapida ingiunzione che impedisca la violazione fino alla sentenza definitiva di un tribunale. Fino al 2006 era semplice ottenere tali ingiunzioni. Di conseguenza, erano diventate l'hack preferito delle grandi aziende – in particolare del settore tecnologico – che volevano ostacolare la concorrenza: le ingiunzioni venivano usate per impedire ad aziende più piccole di vendere i loro prodotti o per costringerle a pagare cifre esorbitanti a chi deteneva il brevetto (una pratica che molti consideravano una sorta di estorsione).

Ci fu un pronunciamento su questo hack[3] quando l'azienda tecnologica MercExchange fece causa a eBay, sostenendo che stesse violando i suoi brevetti sui sistemi di aste online. La corte suprema degli Stati Uniti si occupò del caso nel 2006, riscrivendo le regole sull'ingiunzione e mettendo una patch alla vulnerabilità stabilendo che i tribunali dovessero applicare un controllo più rigoroso, che tenesse conto di quattro fattori, prima di stabilire l'ammissibilità di una richiesta di ingiunzione.

Le leggi non sono mai complete. Col tempo e i cambiamenti sociali, emergono zone grigie e punti ciechi. Sia la legge codificata che la common law possono dare adito a loophole, omissioni ed errori, e qualcuno cercherà di stravolgere le leggi per sfruttarli in modi imprevisti e non voluti dal legislatore per trarne vantaggio. Qualcun altro – in genere un soggetto penalizzato da tale stravolgimento – porterà l'hack in tribunale. Un giudice fungerà dunque da arbitro neutrale per stabilire l'eventuale legittimità dell'hack. Nel caso ne

determini l'illegittimità, l'hack sarà dichiarato illegale, e la decisione fungerà da patch per il sistema. Se invece il giudice dichiarerà legittimo l'hack, questo diventerà parte della common law e sarà considerato legale. La common law è per sua natura un hack del sistema giudiziario, le cui decisioni, basate sull'interpretazione e l'applicazione creativa di principi e precedenti, sono a loro volta un hack sociale per risolvere quanto altrimenti sarebbe irrisolvibile.

Tramite l'hacking, la legge si adatta a nuove circostanze, nuovi sviluppi e nuove tecnologie. In ambito giuridico, nessuno parla di hacking, eppure è di questo che si tratta. La common law non è altro che una serie di hack e pronunciamenti. È il miglior sistema che abbiamo per controllare la forza dell'hacking al fine di migliorare la legge. L'hacking è il modo che ha la legge di adattarsi al passare del tempo.

Vi faccio un altro esempio. Nel medioevo, quando un proprietario terriero partiva per le Crociate, spesso trasferiva il titolo della sua proprietà immobiliare a una persona di fiducia. In tal modo, mentre era via, l'affidatario avrebbe badato alla sua proprietà e avrebbe ottemperato agli obblighi previsti, come i pagamenti feudali. Non andava sempre a finir bene. Accadeva che al ritorno del crociato, il suo ex amico si rifiutasse di restituirgli il titolo. Era un hack della legge: l'intento originale del crociato non era certo quello di vendere i propri possedimenti. Per risolvere il problema, i crociati si rivolsero al lord cancelliere e alla sua Court of Chanchery. Questi mise una patch alla vulnerabilità creando un nuovo diritto. Un possedimento avrebbe potuto avere due proprietari: un proprietario *legale*, detentore del titolo, e un possessore *secondo equità*, che in base a un principio di correttezza (*equity*) è detentore della terra. Il proprietario secondo equità, prendendosi cura delle terre, avrebbe anche goduto dei benefici della proprietà, come l'utilizzo, mentre i crociati restavano comunque i proprietari per legge. Si trattò di una patch di facile applicazione, con incentivi per entrambe le parti in causa. I nobili volevano conservare i propri diritti di proprietà e i reduci delle crociate erano un gruppo potente e disponibile al compromesso.

La stessa divisione dei diritti esiste ancora oggi in molti Paesi che

adottano la common law. Negli Usa persiste la divisione tra *matter of law* e *matter of equity*, che consente l'esistenza del trust come struttura finanziaria. In sintesi: qualcun altro è detentore del trust (e dei suoi asset), mentre il "vero" proprietario e beneficiario può godere del ricavato di tali asset (ad esempio dei suoi dividendi monetari).

1. Jon Kolko (6 marzo 2012), “Wicked problems: Problems worth solving”, *Stanford Social Innovation Review*, https://ssir.org/books/excerpts/entry/wicked_problems_problems_worth_solving.
2. England and Wales High Court (King’s Bench), Entick *vs* Carrington (1765), EWHC KB J98 1066.
3. Corte Suprema degli Stati Uniti (15 maggio 2006), eBay Inc. *vs* MercExchange, LLC, 547 U.S. 388, www.supremecourt.gov/opinions/05pdf/05-130.pdf.

CAPITOLO 34

L'hacking come evoluzione

Gli ebrei ortodossi sono bravissimi ad hackerare le loro regole religiose. È vietato lavorare durante lo *Shabbat*, che va dal venerdì sera al sabato sera. Anche accendere un fuoco – e per estensione l'accensione di qualunque luce – o qualunque attività che richieda l'elettricità sono considerati lavoro. Quando ero ragazzo, i miei cugini avevano un timer attaccato all'alimentazione della loro tv, per accenderla in modo automatico, senza alcuna azione umana. L'unico problema era scegliere prima di venerdì sera l'unico canale che avremmo potuto vedere. È vietato portare con sé degli oggetti quando si va in giro, ad esempio la chiave di casa, a meno che la chiave non faccia parte di un gioiello che si indossa. È concesso invece portare oggetti con sé mentre si è in casa. Alcune comunità facevano pertanto passare un filo – detto *eruv*[1] – in tutto il circondario, per hackerare l'antica definizione di aree comuni semi-private e permettere di considerare "casa" qualunque cosa all'interno dell'area racchiusa dal filo.

I "gentili" non devono seguire le stesse regole. Quando ero bambino, nella mia sinagoga, ci servivamo appositamente di un custode non ebreo che potesse fare quel che a noi ebrei non era consentito. Non potevamo però chiedergli aiuto in modo diretto. Ad esempio, non potevamo dirgli "potresti accendere i riscaldamenti?", ma potevamo ottenere lo stesso risultato dicendo "fa un po' freddo". Allo stesso modo, un ebreo osservante non può entrare in un ascensore e chiedere a qualcuno "potrebbe premere il pulsante del quinto piano?", ma può invece domandarsi ad alta voce "chissà se qualcuno ha premuto il cinque". Durante lo Shabbat molti ascensori nelle zone più religiose di Israele si fermano automaticamente a ogni piano.[2]

Da piccolo, questo sistema per seguire le regole alla lettera senza rispettarne lo spirito mi sembrava una forzatura. Si tratta però del

metodo usato dalla millenaria legge ebrea per adattarsi alla modernità. È hacking ed è – cosa ancor più importante – l'integrazione di tali hack in una società in perenne evoluzione. L'hacking serve a trovare nuovi errori non ancora sfruttati. Quando gli hack funzionano, hanno esiti inattesi. È questo l'importante. L'hacking non è solo la manipolazione nociva di un sistema. Un hack riuscito cambia il sistema hackerato, in misura di quanto viene utilizzato e riesce a diffondersi. Cambia il funzionamento del sistema, sia nel caso gli richieda una patch sia nel caso lo costringa ad ampliarsi per inglobarlo. L'hacking è un processo tramite il quale chi usa un sistema lo cambia in meglio, come reazione a nuove tecnologie, nuove idee, nuovi modi di vedere il mondo. È in tal senso che possiamo considerare l'hacking come una forma di evoluzione. Lo possiamo vedere nel banking moderno, nel trading ad alta frequenza, nel mercato immobiliare di lusso, e – probabilmente – nelle azioni di gran parte delle aziende della gig economy.

E non solo. Esiste ad esempio un device Bluetooth per usare lo smartphone durante lo Shabbat:[3] una lieve corrente elettrica passa costantemente attraverso i suoi pulsanti, e in tal modo premerli non chiude un circuito e non viola la legge ebraica.

Se sfruttato al meglio, l'hacking accelera l'evoluzione di un sistema, permettendogli di incorporare le forze che lo avversano. Se invece viene sfruttato nel modo peggiore, l'hacking può accelerare la distruzione di un sistema, rivelandone le debolezze e permettendo di sfruttarle per il proprio tornaconto personale fino al punto di farlo a pezzi.

L'innovazione è essenziale per la sopravvivenza dei sistemi. Un sistema calcificato non può reagire agli hack e pertanto non riuscirà a evolversi. Lo scienziato politico Francis Fukuyama teorizza che Stati e istituzioni nascono per rispondere a determinate condizioni ambientali,[4] e che quando queste cambiano, se non si evolvono di conseguenza, sono condannati a crollare o a essere conquistati (come nell'esempio dell'Impero Ottomano). Le ricerche della scienza politica contemporanea ci spiegano che, quando le forze conservatrici che rappresentano i ricchi e i potenti non consentono alle società di evolversi, c'è il rischio che l'intero sistema politico

possa collassare.[5] Lo stesso potere dirompente può essere sfruttato come motore per il cambiamento anche da chi si trova alla base della scala sociale: è così che avvengono le rivoluzioni. Per i più deboli, l'hacking può trasformarsi in un'arma. Una delle più efficaci.

Un altro esempio: c'è chi sta hackerando il concetto di personalità giuridica per difendere la natura, dai grandi primati ai fiumi.[6] Il concetto stesso di personalità giuridica è un hack del quattordicesimo emendamento, che stabilisce le regole sulla cittadinanza e i diritti dei cittadini.

In modo quasi darwiniano, Madre Natura decide quali hack scompaiono e quali permangono. Può essere spietata, ma non fa favoritismi. Nell'evoluzione dei sistemi sociali, chi è potente è sempre avvantaggiato, e spesso può decidere quali hack avranno un futuro. Se la cosa non cambia, affidare l'evoluzione di un sistema agli hack contribuirà a perpetuare le ingiustizie presenti nello status quo. Per evitare il collasso, in futuro l'hacking sociale dovrà armonizzare la spinta evolutiva e la lotta per il bene comune. L'hacking può essere anche una rivoluzione.

Forse una metafora migliore per comprenderlo è quella delle specie invasive. Specie diverse si evolvono in ambienti specifici, dove si stabilisce un equilibrio tra prede, predatori e altri fattori. Spostando una specie da un ambiente all'altro, può accadere che questa sfrutti le proprie caratteristiche diverse in modi nuovi e inattesi. Può ad esempio succedere che nel nuovo ambiente una specie non venga più limitata dal suo solito predatore o da un suo sostituto di qualche sorta (pensiamo al pitone birmano in Florida). Oppure può venire a mancare un fattore ambientale che ne limitava la crescita (come il freddo per la pianta di kudzu, il Flagello del Sud). O ancora può accadere che una specie trovi cibo in modo innaturalmente abbondante (è il caso della famelica carpa asiatica). Di conseguenza, una specie invasiva riesce a moltiplicarsi a una velocità senza precedenti. Con gli hack accade la stessa cosa. Rappresentano un elemento di discontinuità in un ecosistema impreparato ad accoglierlo. Un ecosistema che sappia trovare le giuste difese potrà stroncare le specie invasive, ma nel caso contrario rischierà di soccombere. In quei casi si parla di "collasso dell'ecosistema", dovuto

a un hack tanto devastante da distruggerlo completamente.

1. M. Olin (2019), "The Eruv: From the Talmud to Contemporary Art", in S. Fine (a cura di), *Jewish Religious Architecture: From Biblical Israel to Modern Judaism*, Koninklijke Brill NV.
2. Elizabeth A. Harris (5 marzo 2012), "For Jewish Sabbath, elevators do all the work", *New York Times*, www.nytimes.com/2012/03/06/nyregion/on-jewish-sabbath-elevators-that-do-all-the-work.html.
3. Redazione di JC (12 agosto 2010), "Israeli soldiers get Shabbat Bluetooth phone", www.thejc.com/news/israel/israeli-soldiers-get-shabbat-bluetooth-phone-1.17376.
4. Francis Fukuyama (2014), *Political Order and Political Decay: From the Industrial Revolution to the Globalization of Democracy*, Farrar, Straus & Giroux.
5. Yoni Appelbaum (dicembre 2019), "How America ends", *Atlantic*, www.theatlantic.com/magazine/archive/2019/12/how-america-ends/600757; Uri Friedman (14 giugno 2017), "Why conservative parties are central to democracy", *Atlantic*, www.theatlantic.com/international/archive/2017/06/ziblatt-democracy-conservative-parties/530118; David Frum (20 giugno 2017), "Why do democracies fail?", *Atlantic*, www.theatlantic.com/international/archive/2017/06/why-do-democracies-fail/530949.
6. Adam Winkler (5 marzo 2018), "'Corporations are people' is built on an incredible 19th-century lie", *Atlantic*, www.theatlantic.com/business/archive/2018/03/corporations-people-adam-winkler/554852.

PARTE QUINTA
L'HACKING DEI SISTEMI POLITICI

CAPITOLO 35

Le disposizioni nascoste nelle leggi

Quando la Svr russa hackerò la SolarWinds, inserendo una backdoor in un aggiornamento del software Orion, 17mila utenti lo installarono, consentendo involontariamente alla Svr di accedere a un numero enorme di reti divenute vulnerabili. A quel punto la Svr aveva solo l'imbarazzo della scelta e selezionò con cura le più appetibili. Fu un caso di *supply chain attack*, visto che l'attacco alle reti non avvenne in modo diretto. La Svr attaccò invece uno dei software usati dalle reti bersaglio. I supply chain attack sono un modo brillante per attaccare i sistemi, in quanto possono colpirne migliaia in un colpo solo. Altri attacchi di questo tipo? Hackerare il Google Play store per inserirvi una falsa app, o intercettare la spedizione di dispositivi tecnici per installarvi dispositivi spia (come per esempio ha fatto la Nsa).[1]

Qualcosa di simile avviene hackerando il sistema legislativo. Nei capitoli precedenti, abbiamo visto come gli hacker scovino e sfruttino le vulnerabilità delle leggi una volta che queste vengono approvate. Gli hacker possono però prendere di mira anche il processo legislativo in sé. Come nel caso dell'aggiornamento di Orion, gli hacker possono volutamente inserire vulnerabilità in un disegno di legge, per sfruttarlo nel caso venga approvato.

In un certo senso, stiamo portando il discorso sull'hacking a un livello successivo. Invece di andare a caccia di hack nelle leggi e nei regolamenti, in questo caso si hackera il processo col quale leggi e regolamenti vengono creati. Gli hacker più potenti sono in grado di farlo. Non si tratta solo di hackerare un sistema, ma di hackerare anche gli strumenti per applicare eventuali patch.

Spesso le leggi presentano loophole, ma in genere non li possiamo considerare hack. Sono eccezioni deliberate a una regola generale, create per perseguire un determinato obiettivo politico, per accontentare alcuni elettori o per raggiungere un compromesso. Un

esempio può essere una legge del 2004, sospinta dall'attività di lobby di Starbucks.[2] Secondo questa legge, la tostatura del caffè può essere considerata "manifattura domestica". Un altro esempio sono le esenzioni antitrust per i "monopoli naturali"[3] per i settori che richiedono un coordinamento tra diverse aziende, come le leghe sportive. Non si tratta di loophole imprevisti e involontari. Non si basano sulla capacità di essere più scaltri del sistema che crea, discute e approva una legge. È per questo che non possiamo considerarli hack.

Non significa però che il processo legislativo che crea tali loophole non venga costantemente hackerato. Basta solo che qualcuno aggiunga una frase a una legge scegliendone accuratamente le parole. Quella frase potrà fare riferimento a molte altre leggi, creando un'interazione volta a ottenere un esito ben preciso, inatteso e non voluto per tutti gli altri.

C'è un intero settore di lobbisti che si occupano di progettare questi esiti inattesi in grado di avvantaggiare i propri ricchi sponsor. Nel 2017, mentre veniva stilato il Tax Cuts and Jobs Act, più della metà dei lobbisti di Washington DC rivelò di occuparsi solamente di questioni fiscali: più di 6mila lobbisti, più di undici per ogni singolo membro del Congresso.[4]

Per fare un esempio, una normativa sul debito approvata dal Congresso nel 2013 prevedeva questa frase: "Sez. 145. Sottosezione (b) della sezione 163 della legge pubblica 5 111-242, già emendata, viene ulteriormente emendata eliminando '2013-2014' e inserendo '2015-2016'". Questa disposizione innocua, inserita dal senatore Tom Harkin, era un regalo nascosto per Teach For America.[5] Prolungava infatti per altri due anni una legge a favore degli studenti nei programmi di formazione insegnanti, compresi quelli di Teach for America.

Nel 2020, il Congresso ha approvato il Cares Act da 2000 miliardi di dollari, per elargire sovvenzioni post Covid-19. A pagina 203 (su 808) c'era un cambiamento nel modo in cui gli investitori del mercato immobiliare potevano rifarsi delle proprie perdite.[6] Si trattava di sgravi fiscali per i magnati dell'immobiliare – come Donald Trump, all'epoca presidente – pari a 17 miliardi di dollari.

Non contava che il provvedimento non avesse niente a che fare col Covid-19 o che lo sgravio retroattivo coprisse un periodo di gran lunga precedente l'arrivo della pandemia. Zitti zitti e rapidissimi, i lobbisti erano riusciti a inserire questo passaggio. Il testo era stato ultimato meno di un'ora prima del voto, e i repubblicani avevano aggiunto il provvedimento all'ultimo istante.[7]

La vulnerabilità risiede nel fatto che le leggi sono lunghe e complicate e contengano un gran numero di provvedimenti dagli effetti poco chiari. L'exploit sta nella possibilità di intrufolare un provvedimento in un disegno di legge senza attirare l'attenzione del legislatore. Un gioco di prestigio di questo tipo può richiedere la complicità più o meno consapevole di un membro del Congresso, ma può bastare anche che un componente dello staff agisca all'insaputa di tutti, o che quanto scritto da un lobbista finisca direttamente nel testo di una legge. È una pratica tanto comune da non venire quasi più considerata un hack.[8]

Negli ultimi decenni, il potere si è sempre più centralizzato, gestito dai leader di partito nelle due camere a discapito delle commissioni legislative, ed è per questo che il processo legislativo è diventato sempre più oscuro e indecifrabile. Inoltre il Congresso tende ad approvare meno leggi, ma sempre più lunghe, rendendo possibile l'inserimento di provvedimenti nascosti a favore di aziende e singoli individui. L'abbiamo visto anche in una puntata dei Simpson: Krusty il Clown viene eletto al congresso[9] e inserisce una modifica al controllo del traffico aereo in una legge per regalare bandierine agli orfani.

Non è facile porre rimedio a una situazione del genere. Per quanto il linguaggio delle leggi possa essere analogo a quello informatico, il modo in cui i due linguaggi vengono creati e utilizzati è molto diverso. Il codice informatico viene scritto da un gruppo di persone che seguono un piano generale, in genere sotto la direzione di una persona o un'azienda. I programmatori conoscono lo scopo del proprio codice, e capiscono quando serve o meno a tale scopo. Sono inoltre i soli ad avere l'autorità per riparare i bug del proprio codice.

La legge non funziona così. È decentralizzata a ogni livello. In una democrazia, la legge viene scritta da molte persone in competizione

tra loro, con obiettivi diversi e varie opinioni su quali dovrebbero essere i suoi scopi. Ciò che per una persona è un bug, per un'altra può essere una caratteristica desiderata, a prescindere dalla consapevolezza dei fini della legge. I provvedimenti nascosti, e le vulnerabilità che rappresentano, sarebbero meno problematici se i regolamenti della Camera e del Senato prevedessero un certo periodo di revisione per i disegni di legge dopo la stesura definitiva e la pubblicazione del testo, magari proporzionale alla lunghezza della legge. I provvedimenti nascosti non sarebbero più "nascosti" se venissero scoperti e analizzati da media competenti, in grado di portarli al cospetto dell'opinione pubblica in tempo per innescare un cambiamento e mettere i politici di fronte alle loro responsabilità. Se invece si concede ai rappresentanti poco tempo per occuparsi degli emendamenti a leggi importanti, i provvedimenti nascosti possono passare senza difficoltà.

Nel 2019, la Commissione selezionata per la modernizzazione del Congresso, tra le sue novantasette raccomandazioni per snellire la Camera dei Rappresentanti,[10] ha proposto di "approntare un nuovo sistema che consenta al popolo americano di controllare facilmente i cambiamenti alle leggi apportati dagli emendamenti e l'impatto sulla legislazione vigente delle proposte di legge". Si tratta in sostanza di un sistema di tracciamento delle modifiche della legge, un'espansione del precedente "Comparative Print Project". Il suo scopo dovrebbe essere quello di rendere più semplice individuare e comprendere i cambiamenti alle leggi, permettendo di scovare i provvedimenti nascosti.[11] Di certo il problema non verrebbe risolto del tutto, anche perché la Commissione propone solo di espandere l'accesso a "tutti gli uffici della Camera", ma sarebbe comunque un passo nella direzione giusta, che potrebbe essere ulteriormente potenziato garantendo l'accesso ai comuni cittadini e imponendo per legge tempi di revisione adeguati.

Ma anche prendere più tempo non basta: servono incentivi che spingano i cittadini a smascherare i provvedimenti nascosti. Prendendo spunto dalle vulnerabilità del software, potremmo creare per le leggi un equivalente del *bug bounty system*, e premiare con una "taglia" i cittadini in grado di riscontrare vulnerabilità nei

disegni di legge. L'ambito perfetto per farlo sarebbe quello delle leggi con implicazioni fiscali: la taglia potrebbe essere una piccola percentuale del gettito fiscale previsto.

I disegni di legge potrebbero anche sfruttare delle pratiche di red teaming, nelle quali team specializzati (mettendosi nei panni delle élite più ricche o delle aziende private) cercherebbero di "hackerare" le leggi in attesa di approvazione per scoprire nuove vulnerabilità.

Queste due pratiche sarebbero molto utili, ma si scontrano entrambe con un problema-chiave delle leggi moderne: il fatto che in genere vengano stilate da pochi legislatori e lobbisti, che inseriscono volontariamente gran parte dei loophole. Supponiamo che un red team trovi una vulnerabilità in una legge fiscale. La dovrà considerare un bug o una caratteristica voluta? Chi potrà deciderlo? E su quali basi? Inoltre molte leggi vengono approvate in tutta fretta dal Congresso dopo essere state rivelate al pubblico, rendendo impossibile per chiunque leggerle e comprenderle nei dettagli. Il red teaming funzionerebbe solo se avesse abbastanza tempo per agire e far valere le proprie scoperte.

Ad esempio, nel 2017, il Tax Cuts and Jobs Act venne votato solo poche ore dopo che il suo testo finale era stato reso disponibile ai legislatori. Una scelta voluta; gli autori non volevano che uno staff di professionisti avesse abbastanza tempo per analizzarlo a fondo. Allo stesso modo, alle due del pomeriggio del 21 dicembre 2020 è stato diffuso il testo del Cares Act,[12] approvato dalla Camera alle nove di sera e dal Senato a mezzanotte, malgrado fosse lungo 5.593 pagine. Il testo prevedeva 110 miliardi di "proroghe fiscali"[13] passate in esame a cuor leggero, e un taglio permanente delle accise per i "produttori di birra, vino e distillati alcolici". Gran parte dei legislatori non sapeva niente dei numerosi loophole fiscali presenti al suo interno.[14]

Forse ci penseranno le velocissime AI a leggere le leggi e identificare gli hack prima della loro approvazione. Di certo sarebbe un contributo alla risoluzione del problema, per quanto altrettanto sicuramente ne creerebbe di nuovi.

1. Sarah Silbert (16 maggio 2014), "Latest Snowden leak reveals the Nsa intercepted and bugged Cisco routers", *Engadget*, www.engadget.com/2014-05-16-nsa-bugged-cisco-routers.html.
2. Ben Hallman e Chris Kirkham (15 febbraio 2013), "As Obama confronts corporate tax reform, past lessons suggest lobbyists will fight for loopholes", *Huffington Post*, www.huffpost.com/entry/obama-corporate-tax-reform_n_2680880.
3. Leah Farzin (1 gennaio 2015), "On the antitrust exemption for professional sports in the United States and Europe", *Jeffrey S. Moorad Sports Law Journal* 75, https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1321&context=mslj.
4. Taylor Lincoln (1° dicembre 2017), "Swamped: More than half the members of Washington's lobbying corps have plunged into the tax debate", Public Citizen, www.citizen.org/wp-content/uploads/migration/swamped-tax-lobbying-report.pdf.
5. Valerie Strauss (16 ottobre 2013), "The debt deal's gift to Teach For America (yes, TFA)", *Washington Post*, www.washingtonpost.com/news/answer-sheet/wp/2013/10/16/the-debt-deals-gift-to-teach-for-america-yes-tfa.
6. Jesse Drucker (26 marzo 2020), "Bonanza for rich real estate investors, tucked into stimulus package", *New York Times*, www.nytimes.com/2020/03/26/business/coronavirus-real-estate-investors-stimulus.html; Nicholas Kristof (23 maggio 2020), "Crumbs for the hungry but windfalls for the rich", *New York Times*, www.nytimes.com/2020/05/23/opinion/sunday/coronavirus-economic-response.html.
7. Akela Lacy (19 aprile 2020), "Senate Finance Committee Democrats tried to strike millionaire tax break from coronavirus stimulus – then failed to warn others about it", *Intercept*, https://theintercept.com/2020/04/19/coronavirus-cares-act-millionaire-tax-break.
8. Nel 2017, Billy Pitts, assistente dei deputati repubblicani al Congresso, dichiarò: "come diavolo ha fatto a intrufolarsi 'sta roba? Con le leggi belle grosse c'è sempre il rischio che dentro ci nascondano qualcosa": www.npr.org/2017/03/11/519700465/when-it-comes-to-legislation-sometimes-bigger-is-better.
9. Matt Groening e J.L. Brooks (11 febbraio 1996), "Bart la spia", *I Simpson*, stagione 7, episodio 12 (15 negli Usa), Fox Broadcasting Company/YouTube, www.youtube.com/watch?v=hNeIkS9EMV0.
10. Select Committee on the Modernization of Congress (2019), "116th Congress recommendations", https://www.govinfo.gov/committee/house-modernization?path=/browsecommittee/chamber/house/committee/modernization/collection/CRPT/congress/116.
11. Select Committee on the Modernization of Congress (2019), "Finalize a new system that allows the American people to easily track how amendments change legislation and the impact of proposed legislation to currentlaw", rapporto conclusivo, https://www.govinfo.gov/committee/house-modernization?path=/browsecommittee/chamber/house/committee/modernization/collection/CRPT/congress/116.
12. Mia Jankowicz (22 dicembre 2020), "'It's hostage-taking.' AOC lashed out after lawmakers got only hours to read and pass the huge 5,593-page bill to secure COVID-19 relief", *Business Insider*, www.businessinsider.com/aoc-angry-representatives-2-hours-read-covid-19-stimulus-bill-2020-12.
13. Yeganeh Torbati (22 dicembre 2020), "Tucked into Congress's massive stimulus bill: Tens of billions in special-interest tax give-aways", *Washington Post*,

www.washingtonpost.com/business/2020/12/22/congress-tax-breaks-stimulus.
14. Akela Lacy (19 aprile 2020), "Senate Finance Committee Democrats tried to strike millionaire tax break from coronavirus stimulus – then failed to warn others about it", *Intercept*, https://theintercept.com/2020/04/19/coronavirus-cares-act-millionaire-tax-break.

CAPITOLO 36

Leggi da approvare a ogni costo

Certi disegni di legge sono per loro natura più importanti. I disegni di legge di spesa o quelli approntati in risposta a eventi esterni come i disastri naturali, le pandemie o le minacce alla sicurezza, vengono in genere considerati non differibili, da approvare a tutti i costi. Consentono ai legislatori di agganciarvi alcuni provvedimenti, noti come *rider*, che da soli non ce la farebbero mai a restare a galla. Provvedimenti impopolari, contro l'interesse pubblico, che avvantaggiano solo poche persone, o che sono il frutto di intrallazzi politici. Inserire questi rider incongruenti in leggi da approvare a tutti i costi consente ai legislatori di evitare lo scrutinio e le critiche altrimenti inevitabili per un provvedimento controverso, e di affermare in modo credibile che si stia votando per una misura di legge nel suo complesso. È un hack ormai diffuso, che capovolge il normale iter di un disegno di legge: si fa una proposta specifica e poi la si vota. Tre esempi:

– Tra il 1982 e il 1984, una serie di rider – il cosiddetto emendamento Boland – furono aggiunti a leggi di spesa che dovevano venire per forza approvate; questo emendamento limitò gli aiuti degli Usa ai Contras in Nicaragua.

– Nel 2016, un disegno di legge per le spese agricole e alimentari incluse un rider che impediva alla Food and Drug Administration di dettare legge sui "sigari grandi e di alta qualità".

– Nel 2021, i legislatori aggregarono tre norme sul copyright delle proprietà intellettuali al Consolidated Appropriation Act, che si occupava di tutt'altro. Si trattava di misure da tempo tenute in stand by per la possibile reazione delle aziende tecnologiche e degli appassionati di tecnologia, e che ora potevano approfittare dell'inserimento in una legge più grande e complessa, e da approvare a ogni costo.

Questo tipo di hack sfrutta il fatto che il presidente non possa mettere il veto a singoli passaggi di un disegno di legge: può porre il suo veto all'intero testo, oppure approvarlo com'è, con tutti i rider al suo interno. L'hack sfrutta inoltre il modo di procedere delle commissioni parlamentari. L'assemblea non può votare un disegno di legge se prima non è stato approvato dalle commissioni competenti. In tal modo, i membri delle commissioni possono semplicemente inserire i rider nelle leggi, apertamente o in segreto.

I tentativi di porre un freno a questa pratica si sono rivelati inefficaci. Nel 1996, il Congresso cercò di attribuire al presidente Clinton il potere di veto su un singolo passaggio di testo, potere che venne però dichiarato incostituzionale nel 1998. Nell'arco di un solo anno, era stato utilizzato ottantadue volte. Tra i promotori della sua abrogazione, ci fu un gruppo di produttori di patate che si opponeva al veto di Clinton su un rider che li avvantaggiava.

Nel caso di un codice modulare informatico, ogni segmento indipendente svolge una singola funzione e grazie a questa struttura i programmi sono più resilienti e riparabili, e i loro problemi più facilmente diagnosticabili. Se le leggi affrontassero un numero minore di problemi ben distinti, questo hacking sarebbe più difficile da attuare. È proprio questa la logica[1] dietro al One Subject at a Time Act del 2021 (legge per provvedimenti su un solo argomento alla volta), più volte presentato al Congresso senza mai essere convertito in legge.

A livello dei singoli Stati, i tentativi di limitare i rider incongruenti sono stati più efficaci. Nella costituzione di quarantatré Stati viene richiesto che ogni legge si limiti a un solo argomento. Ad esempio nella costituzione del Minnesota[2] c'è scritto: "Le leggi devono affrontare un solo tema, che deve essere espresso nel loro titolo". Anche queste restrizioni sono state però hackerate. Come ha scritto Richard Briffault, docente di diritto alla Columbia University, "il fatto che una misura riguardi uno o più temi sarà comunque soggettivo". Da un lato, come ha spiegato la Corte Suprema del Michigan, "virtualmente, non esiste provvedimento che non possa venire suddiviso e attuato con leggi separate". D'altro canto, come deliberato in un caso discusso dalla Corte Suprema della

Pennsylvania,[3] “non esistono argomenti tanto distanti da non poter essere ricondotti allo stesso focus, basta solo allontanare un po’ il punto di vista”.

Un’altra forma di difesa sta nella resilienza di un sistema. Le leggi da approvare a ogni costo sono particolarmente vulnerabili ai rider a causa delle conseguenze nefaste di una loro mancata approvazione. Alcune di queste conseguenze, come il blocco delle attività amministrative dovuto alla mancata approvazione della legge di spesa, sono però del tutto artificiali, e possono essere alleviate da politiche efficaci. Ad esempio, molte organizzazioni hanno proposto[4] al Congresso di rendere più resiliente l’azione di governo tramite la creazione di risoluzioni attuate in modo automatico e continuo. In uno scenario simile, i finanziamenti al governo continuerebbero ad arrivare anche se il Congresso non riuscisse ad approvare una legge di spesa convenzionale. Rendendo più lievi le conseguenze dei ritardi sulle leggi obbligatorie, chi si oppone ai rider potrebbe fare ostruzione fino a vederli espunti dal disegno in fase di approvazione.

1. Congresso degli Stati Uniti (10 aprile 2019; ultima modifica 20 maggio 2019), H.R. 2240: One Subject at a Time Act, 116th Congress, www.congress.gov/bill/116th-congress/house-bill/2240.
2. Stato del Minnesota (13 ottobre 1857; revisione del 5 novembre 1974), Costituzione dello Stato del Minnesota, Articolo IV: Legislative Department, www.revisor.mn.gov/constitution/#article_4.
3. Richard Briffault (2019), "The single-subject rule: A state constitutional dilemma", *Albany Law Review* 82, https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3593&context=faculty_scholarship.
4. Committee for a Responsible Federal Budget (17 settembre 2020), "Better Budget Process Initiative: Automatic CRs can improve the appropriations process", www.crfb.org/papers/better-budget-process-initiative-automatic-crs-can-improve-appropriations-process.

CAPITOLO 37

Legislazione delegata e ritardata

Dopo la fine della Guerra Fredda, il Congresso dovette affrontare il problema non semplice della chiusura di molte basi militari in tutti gli Stati Uniti. Si parlava di centinaia, se non migliaia, di posti di lavoro: nessun rappresentante al Congresso avrebbe accettato la chiusura di una base nel proprio collegio di appartenenza. Il Congresso evitò di prendere una decisione diretta e trovò invece un hack per depoliticizzare tale processo. Delegò i propri poteri legislativi a un corpo esterno separato, creando la Commissione per la riconversione e la chiusura delle basi, col potere di decidere quali chiudere e quali ridimensionare. Era previsto che a meno che non intervenisse il Congresso, le decisioni della Commissione entrassero direttamente in vigore. Il sistema funzionò: dal 1988 a oggi sono state formate cinque commissioni del genere, portando alla chiusura di più di trecentocinquanta installazioni militari.

Questo hack consente al Congresso di risolvere temi difficili o molto sentiti senza dover davvero decidere qualcosa. In questo caso fa in modo che non siano interessi di parte a stabilire la chiusura delle basi. Il Congresso riesce in tal modo anche ad aggirare tutta quella serie di procedimenti e regole che potrebbero rallentare il processo decisionale.

Non è però un hack che viene usato spesso. Nel 2010, il Congresso fondò l'Ipab (Independent Payment Advisory Board) per stabilire i tagli al piano Medicare. In genere è necessario un atto del Congresso per apportare cambiamenti al Medicare, il Congresso autorizzò però questo organismo a effettuare cambiamenti che avrebbero potuto essere respinti solo da un voto del Congresso stesso a maggioranza qualificata. L'intento, anche in questo caso, era di evitare ogni responsabilità e riuscire comunque ad approvare un provvedimento in grado di tagliare i fondi al Medicare. L'opposizione dei gruppi ospedalieri privati e gli attacchi all'Ipab di politici come l'ex

candidata alla vicepresidenza Sarah Palin impedirono però al Congresso di nominare i membri di questo board, fino ad abrogarlo nel 2018, dopo cinque anni senza alcun componente.

Un hack analogo è il *title-only bill*, un disegno di legge puramente nominale, che si presenta come un guscio vuoto. Non ha un contenuto effettivo, eppure a Washington non c'è sessione durante la quale non ne venga presentato uno. Ha un valore simbolico, nel caso nel corso dell'anno i legislatori vogliano trovarsi in vantaggio su regole e scadenze. Alla fine della sessione legislativa del 2019, i democratici usarono uno di questi disegni di legge puramente nominali per approvare una nuova tassa bancaria al riparo dal dibattito e dall'opinione pubblica.

Questo hack fa parte di una categoria più ampia di deleghe legislative all'esecutivo. Ci sono molte persone secondo le quali lo "Stato amministrativo" e il potere normativo concesso all'esecutivo dal potere legislativo rappresentano un grande hack in grado di sbilanciare il meccanismo di formazione delle leggi. Questo hack viene usato costantemente. Negli Usa, ogni anno vengono varati tra i 3mila e i 4mila nuovi provvedimenti amministrativi,[1] un numero di gran lunga superiore alle leggi emanate dal Congresso. È l'effetto principale di un Congresso che agisce in modo sempre più disfunzionale e cede il suo potere ad agenzie federali che invece si comportano in modo relativamente efficiente; inoltre i membri del Congresso non vogliono essere inquadrati come sostenitori o oppositori di alcune leggi.

Non è semplice porre riparo a una situazione simile. Nel caso che il potere legislativo ritenga, in qualunque momento, che l'esecutivo abbia invaso il suo campo o che stia perseguendo obiettivi sbagliati può intervenire con una legge restringendo il campo d'azione delle autorità delegate. Molti studiosi di diritto auspicano un intervento del Congresso in questa direzione, mentre altri invitano la Corte Suprema a darsi da fare in tal senso.

I rappresentanti possono non solo delegare la propria responsabilità nel creare le leggi, ma anche rifiutarsi di votarle. Un deputato o un senatore possono fare ostruzionismo (*filibustering*) con discorsi interminabili per evitare che una proposta o un disegno

di legge vengano approvati in tempo. Accade soprattutto al Senato degli Stati Uniti, ma è una tattica adottata in tutto il mondo, dalla Gran Bretagna al Canada, dall'Austria alle Filippine.

Non è certo una novità: già nel 60 a.C. il senatore romano Catone l'Uticense si dilungava in discorsi lunghissimi per rimandare il voto. Il Senato romano era tenuto a decidere entro il tramonto, ma votare era impossibile se Catone non smetteva di parlare. Il senatore riuscì ad andare avanti per sei mesi. Non poco.

Questo tipo di ostruzionismo negli Usa è permesso da una vulnerabilità dovuta a un effetto collaterale di una modifica normativa. Nel 1805, il vicepresidente Aaron Burr decise che il Senato non avrebbe dovuto seguire troppe norme procedurali. Una delle regole abbandonate per dar retta al suo consiglio – nel 1806, dopo la fine del suo mandato – fu la *motion to previous question*, il "ritorno al punto", che imponeva di interrompere le discussioni su un disegno di legge. Solo nel 1837 qualcuno cominciò a sfruttare questa vulnerabilità. Nel 1917 venne messa una patch con la regola della "ghigliottina": chi faceva ostruzionismo non doveva mai smettere di parlare o altrimenti si sarebbe andati al voto. Nel 1975 venne aggiunta la richiesta di una maggioranza di tre quinti dell'aula – pari a sessanta senatori – eliminando l'obbligo di non interrompersi mai. È un hack attuato su una patch messa su un hack, che solo un hack potrà cambiare.

L'ostruzionismo è una sovversione del sistema legislativo. Un corpo legislativo deve difendere la libertà di esprimersi della minoranza e allo stesso tempo il diritto di deliberare della maggioranza. Questo assunto è stato però ribaltato: oggi la minoranza può fare ostruzione per bloccare il processo legislativo di qualunque disegno di legge che non disponga di una maggioranza qualificata di sessanta voti, ma di fatto in questo modo dibattere di certi argomenti in modo significativo diventa impossibile. La cosa danneggia non solo il partito di minoranza in Senato, ma anche le minoranze sociali in genere. Storicamente, l'ostruzionismo è stato spesso usato per bloccare le leggi a favore dell'uguaglianza razziale.[2]

Negli Usa ormai l'ostruzionismo viene considerato una pratica normale. Le regole al Senato sono così lasche che un senatore non

deve nemmeno parlare per giorni o mesi per fare ostruzionismo; gli basta esprime l'intenzione di farlo per rimandare un voto. Nel 60 a.C. di certo però era qualcosa di inatteso e non voluto da chiunque avesse stabilito le regole del Senato romano. I discorsi ostruzionisti erano un modo di sovvertire quelle regole e per impedire lo scopo stesso dell'esistenza del Senato: votare le leggi.

L'ostruzionismo tramite i discorsi prolungati non è l'unica tattica per rinviare un voto. In Gran Bretagna, i membri della Camera dei Comuni possono stabilire che le sedute siano segrete: un metodo che dovrebbe servire a discutere questioni d'interesse nazionale, ma che spesso – più di recente nel 2001 – viene usato per rinviare un'approvazione.[3] I parlamentari della Dieta nazionale del Giappone talvolta usano "l'andatura del bue",[4] spostandosi tra i banchi con estrema lentezza per rallentare le votazioni. Se usata in modo strategico, l'andatura del bue può fare slittare una votazione alla sessione successiva. Nel 2016, in Italia, vennero inseriti in un disegno di riforma costituzionale ben 84 milioni di emendamenti.[5] Non è un errore di stampa.

Sono hack buoni o cattivi? Dipende da quale pensate che sia lo scopo principale di un sistema di governo. Se pensate che debba agire solo in presenza di una maggioranza qualificata o dopo lunghi dibattiti, allora apprezzerete queste tattiche per posticipare le decisioni e dare alla minoranza un posto al tavolo dei negoziati. Se pensate invece che un governo debba essere più attivo e rispondere rapidamente alle sfide del presente, per poi sottoporsi al giudizio degli elettori, concedere una sorta di potere veto alla minoranza vi sembrerà una pessima idea.

Per cambiare queste pratiche, le soluzioni vanno da una patch al sistema di base tramite il divieto di effettuare certi hack – ad esempio eliminando il filibustering negli Usa – a meccanismi per renderli semplicemente più difficili da attuare. Oggi fare ostruzionismo non è difficile: non serve più passare giorni a parlare al Senato, ma basta dichiarare con una mozione di volerlo fare. E se la maggioranza vuole bloccare questa pratica, deve trovare almeno sessanta voti: in questo modo è più facile fare ostruzionismo che interrompere chi lo fa. Ci sono state varie proposte di riforma di

questa pratica, la più interessante delle quali è quella di Norm Ornstein dell'American Enterprise Institute, che propone di ribaltare le carte in tavola: invece di richiedere sessanta voti per mettere fine all'ostruzionismo, bisognerebbe chiederne quaranta per attuarlo. L'idea di base è che la maggioranza sia in grado di far durare giorni o settimane una sessione del Senato, e che la minoranza debba essere allerta e presente, e dormire nei pressi del Senato, pronta a votare in ogni momento.

1. Clyde Wayne Crews e Kent Lassman (30 giugno 2021), "New Ten Thousand Commandments report evaluates the sweeping hidden tax of regulation; Provides definitive assessment of Trump deregulatory legacy", Competitive Enterprise Institute, https://cei.org/studies/ten-thousand-commandments-2020.
2. Zack Beauchamp (25 marzo 2021), "The filibuster's racist history, explained", *Vox*, www.vox.com/policy-and-politics/2021/3/25/22348308/filibuster-racism-jim-crow-mitch-mcconnell.
3. Lauren C. Bell (14 novembre 2018), "Obstruction in parliaments: A cross-national perspective", *Journal of Legislative Studies*, www.tandfonline.com/doi/full/10.1080/13572334.2018.1544694.
4. Michael Macarthur Bosack (31 gennaio 2020), "Ox walking, heckling and other strange Diet practices", *Japan Times*, www.japantimes.co.jp/opinion/2020/01/31/commentary/japan-commentary/ox-walking-heckling-strange-diet-practices.
5. Redazione della Gazzetta del Sud (11 aprile 2016), "Democracy doesn't mean obstructionism says Renzi", www.ansa.it/english/news/2016/04/11/democracy-doesnt-mean-obstructionism-says-renzi-2_e16b1463-aa10-432a-b40e-28a00354b182.html.

CAPITOLO 38

Il contesto di un hack

Sto cercando di spiegare una sfumatura estremamente complessa del concetto di hacking. Gli hack non sono per loro natura cattivi, indesiderabili o qualcosa dalla quale ci si debba per forza difendere. È sufficiente riconoscere che gli hacker sovvertono i sistemi sottostanti e decidere se tale sovversione è dannosa o benefica.

Ad esempio, mi sono dilungato sull'hacking delle leggi fiscali. In molti casi, gli hacker (commercialisti e avvocati esperti di diritto fiscale) scovano vulnerabilità non volute (loophole) nelle leggi fiscali. Le inesattezze linguistiche[1] nell'American Job Creation Act del 2004 crearono una serie di vulnerabilità nelle leggi fiscali che gli studi più abili furono in grado di sfruttare al meglio. Il caso più rilevante fu quello della deduzione per le attività di produzione interna, che avrebbe dovuto aiutare le manifatture americane a essere più competitive sul mercato internazionale; la definizione di manifattura era tanto ampia – "mettere assieme o assemblare due o più articoli" – che aziende di ogni sorta cercarono di avvantaggiarsene. Ad esempio la World Wrestling Entertainment, sostenendo di produrre video di wrestling; oppure i negozi di alimentari, che spruzzavano antiparassitari sulla frutta; o le farmacie, che reclamavano lo status di manifattura per le macchine delle fototessera presenti nei loro locali. Un produttore di cesti regalo richiese di rientrare nel provvedimento in quanto nello stesso pacchetto metteva vino e cioccolata. Il governo lo portò in tribunale contestandogli questa deduzione, e perse.

Non possiamo esserne sicuri,[2] ma è possibile che una formulazione tanto vaga sia divenuta parte della legge a causa delle pressioni dei lobbisti e del bisogno di accaparrarsi abbastanza voti al Congresso per approvarla. Era solo uno dei molti sgravi fiscali previsti, anche se nessun altro ha causato effetti tanto inattesi. Ha avuto tale fortuna da persistere fino al 2017, quando è stato sostituito da una deduzione

sul reddito per le aziende qualificate.

Passando dagli esempi più semplici a quelli più complessi, diviene più arduo capire la bontà di un hack. Qual è "l'intento" delle regole dell'hockey? I bastoni ricurvi vanno a favore o contro tale intento? Certo, rendono il dischetto più rapido e le partite più emozionanti.[3] Più velocità significa però anche maggiore pericolo e rischio di infortuni. Quando la National Hockey League fissò in una regola quale dovesse essere la giusta curvatura, di fatto stava provando a trovare un equilibrio tra sport e sicurezza. Dal 1967 in poi le regole sono cambiate, sempre in cerca del giusto compromesso: si passò da una curvatura massima di un pollice e mezzo a una di un pollice, per poi arrivare prima a mezzo pollice e attualmente a tre quarti di pollice.

È ancor più difficile capire le intenzioni dello staff di legislatori responsabile di quella forte deduzione fiscale per la manifattura. Sono stati dei lobbisti a hackerare il processo legislativo, spiegando a qualche membro del Congresso o al suo team quale formulazione volutamente vaga sarebbe stata perfetta per i loro interessi? Oppure quel membro del Congresso era profondamente convinto che tassare le aziende sia sbagliato e ha deciso di inserire nella legge una frase che sapeva non sarebbe stata notata dalla commissione in fase di dibattito? Si è trattato solo di una legge scritta male?

Il fatto che un hack rappresenti o meno un progresso dipende dalle persone coinvolte. Un imprenditore scaltro può sfruttare un loophole normativo a proprio vantaggio. Magari ne possono approfittare anche i suoi clienti, a discapito però del governo.

Abbiamo definito un hack come una tecnica che aderisce formalmente alle regole di un sistema ma ne sovverte gli intenti. Non è sempre un male. Come abbiamo visto, alcuni hack sono innovazioni che fanno del bene a tutti. Prima o poi vengono normalizzati, e contribuiscono al miglioramento di un sistema. In Cina, ad esempio, i governi riformisti degli anni Ottanta e Novanta del Novecento aggirarono le restrizioni alla proprietà privata[4] offrendo a chi occupava un terreno concessioni di settant'anni rinnovabili. Formalmente quei governi seguirono le regole del partito comunista, sovvertendone però del tutto gli intenti.

Un sistema non può decidere il valore di un hack al suo interno, il compito spetta a un sistema più ampio: si tratta infatti di una definizione che dipende dal contesto. Un bancomat esiste in un contesto ben più ampio di quello bancario. Le regole dell'hockey esistono all'interno di un contesto più vasto, fatto di giocatori, tifosi, campionati e società. I casi che ho affrontato in questo libro – inerenti a banche, economia, diritto e alla stessa psicologia – esistono nel contesto più ampio della società: identità, rapporti, desideri, valori e obiettivi.

Il che ci porta a una domanda inevitabile: chi decide l'intento di un hack? Chi decide se un hack è a fin di bene o meno, chi stabilisce se riesce effettivamente a migliorare un sistema? Può divenire molto complicato stabilirlo, specialmente nei sistemi progettati da più soggetti, o in quelli che si sono evoluti col tempo. A volte gli hack fanno bene a qualcuno e nuocciono a qualcun altro.

Ecco quindi che alcune verità sui sistemi non possono essere comprese da chi si trova al loro interno e diventano più chiare solo se viste da un livello superiore. Tutti i programmi informatici sono essenzialmente un codice complesso di circuiti che si aprono e chiudono, e rappresentano uno e zero; ma gli esseri umani non ragionano in questi termini: nessuno programma in codice macchina. Ci interessano solo le funzioni e le finalità di tale codice: il film che vogliamo guardare, il messaggio che vogliamo inviare, le notizie e i comunicati che vogliamo leggere. Per usare la metafora della biologia: le strutture molecolari e le reazioni chimiche alla base della vita ci appaiono come un universo chiassoso ed estremamente complicato, a meno di non spostarci al livello superiore dell'organismo nel suo complesso e capire che servono tutti a mantenere in vita un certo individuo.

Negli ultimi capitoli abbiamo incontrato molti organi amministrativi che servono a determinare se un hack è buono o meno. I sistemi più semplici possono essere governati da un solo organismo con un solo scopo. La Nevada Gaming Commission aggiorna le regole dei casinò in base agli hack. La Fédération Internationale de l'Automobile (Fia) fa lo stesso per la Formula 1 e la Fédération Internationale de Football Association (Fifa) per il calcio.

Gli hack sovvertono l'intento del sistema? O lo fanno progredire? Ma soprattutto: qual è l'intento del sistema? La risposta (che non è mai unica) non dipende solo dall'analisi degli hack e del sistema, ma anche dalle convinzioni morali, etiche e politiche di una persona. Inevitabilmente ci saranno opinioni diverse sull'opportunità di normalizzare un hack. La cosa più importante sarà capire chi viene avvantaggiato o penalizzato da quell'hack, altra questione con valenze politiche. Da questo scaturisce un dibattito, e magari un voto, ed entrambi vengono influenzati da ricchezza e potere.

Un esempio. Nel 2020, il presidente Trump voleva nominare sottosegretario della difesa Anthony Tata, ex generale di brigata dell'esercito. Una nomina del genere richiede l'approvazione del Senato. Una volta chiaro che il Senato non l'avrebbe confermata, Trump ha ritirato la nomina,[5] nominando invece Tata "facente funzioni" di vice-sottosegretario alla Difesa. Ha anche sottolineato più volte il termine "svolgere" per evitare di scontrarsi con lo scoglio dell'approvazione del Senato. Si è trattato di un hack del Vacancies Reform Act del 1998, che ha costituito un'evidente mancanza di rispetto dei doveri di supervisione del Senato? Oppure è stata una reazione comprensibile all'assurda richiesta che il Senato confermi milleduecento nomine? Dipende da come riteniamo che debba funzionare il governo.[6]

1. Natalie Kitroeff (27 dicembre 2017), “In a complex tax bill, let the hunt for loopholes begin”, *New York Times*, www.nytimes.com/2017/12/27/business/economy/tax-loopholes.html.
2. Edmund L. Andrews (13 ottobre 2004), “How tax bill gave business more and more”, *New York Times*, www.nytimes.com/2004/10/13/business/how-tax-bill-gave-business-more-and-more.html.
3. National Hockey League (ultimo accesso 11 maggio 2022), “Historical rule changes”, https://records.nhl.com/history/historical-rule-changes.
4. Donald Clarke (19 gennaio 2017), “The paradox at the heart of China’s property regime”, Foreign Policy, https://foreignpolicy.com/2017/01/19/the-paradox-at-the-heart-of-chinas-property-regime-wenzhou-lease-renewal-problems; Sebastian Heilmann (2008), “Policy experimentation in China’s economic rise”, Studies in Comparative International Development 43, https://link.springer.com/article/10.1007/s12116-007-9014-4.
5. Lara Seligman (2 agosto 2020), “Trump skirts Senate to install nominee under fire for Islamaphobic tweets in Pentagon post”, *Politico*, www.politico.com/news/2020/08/02/donald-trump-anthony-tata-pentagon-390851.
6. Kevin Drum (3 agosto 2020), “Do we really need Senate confirmation of 1,200 positions?” *Mother Jones*, www.motherjones.com/kevin-drum/2020/08/do-we-really-need-senate-confirmation-of-1200-positions.

CAPITOLO 39

Hack per impedire ai cittadini di votare

Ci sono tanti modi per truccare le elezioni. La storia ci ha fornito un gran numero di esempi, dall'uso di schede fasulle alla falsificazione dei registri. Spesso però il sistema migliore per farlo non è agire direttamente, ma hackerare il processo. Come nel caso dei mercati azionari e del processo legislativo, la democrazia si basa su informazione, scelta e agency, tre cose che possono essere hackerate. Gli hacker possono dunque utilizzare le regole stesse che regolano le elezioni per sovvertirne l'intento.

Chi non vota, non ha voce in capitolo: per questo molti hack intervengono sulla agency degli elettori.

Il quindicesimo emendamento, ratificato nel 1870 dopo la fine della Guerra Civile, rese illegale impedire a un uomo di votare per motivi di razza o colore, o per il fatto che in precedenza fosse uno schiavo (alle donne non era ancora permesso votare o detenere una carica). Ben presto, i neri cominciarono a far sentire la propria influenza in sede elettorale e ricoprire cariche pubbliche, con grande scorno dei bianchi del Sud e della élite politica un tempo a favore della schiavitù. La loro reazione fu quella di hackerare le elezioni limitando il diritto di voto e il potere politico degli afroamericani (per riuscirci usarono anche tattiche che non possiamo considerare hack, dalla violenza all'omicidio).

In Alabama, ad esempio, i *Redeemers* ("redentori"), una coalizione di democratici conservatori,[1] arrivarono al potere nel 1874, dopo un'elezione segnata da brogli e un uso paramilitare della violenza (non considerabile un hack). Nei trent'anni a venire, sabotarono gradualmente l'influenza politica degli afroamericani tramite una serie di restrizioni strategiche. Il culmine[2] fu la ratifica di una nuova costituzione dello Stato nel 1901 con l'obiettivo di "imporre la supremazia dei bianchi in questo Stato". La Costituzione[3] limitò il numero degli afroamericani col diritto di voto negandolo a chi non

superava i test di alfabetizzazione e a chi non poteva pagare l'imposta sulle persone fisiche o dimostrare il possesso di determinati diritti di proprietà (in questo caso ci troviamo di fronte a un hack). La trovata funzionò: all'inizio degli anni Settanta dell'Ottocento potevano votare più di 140mila afroamericani. Nel 1903[4] meno di tremila poterono registrarsi per votare.

"Test di alfabetizzazione" è un nome fuorviante. Questi test non misuravano infatti la capacità di leggere e scrivere, ma erano un insieme di domande complicate pensate a cui quelle persone non erano in grado di rispondere. Possiamo discuterne la costituzionalità, ma l'hack consisteva nell'attribuire agli ufficiali locali la possibilità di decidere quali elettori dovessero affrontare quei questionari impossibili. Di fatto, gli ufficiali elettorali potevano negare tale diritto a proprio piacimento. Il test della Louisiana del 1964[5] è facilmente reperibile online. Una domanda – e non sto scherzando – chiedeva: "Scrivi una parola su due di questa frase e in grassetto una parola su tre [le prime delle due in un carattere più piccolo, terminando la prima riga alla virgola] ma scrivi con la maiuscola la quinta parola". Tutt'oggi l'Alabama impiega ancora una serie di tattiche per limitare la partecipazione al voto, escludendo persone con precedenti penali, appartenenti a minoranze, immigrate e provenienti dalle campagne. In Alabama le barriere iniziano già dal sistema di registrazione al voto. Lo Stato non registra i cittadini automaticamente e non dà loro la possibilità di farlo online, presso gli uffici della motorizzazione o il giorno stesso delle elezioni; non offre inoltre alcuna pre-registrazione ai giovani che dovranno votare per la prima volta. La legge statale richiede che per registrarsi si debba dimostrare la propria cittadinanza; ancora non è stata attuata a causa di un'indagine federale ancora in corso, ma nel caso accadesse, negherà il voto a molti cittadini appartenenti a varie minoranze, che spesso non hanno il passaporto o altri documenti. Con una regola similare, il Kansas ha tenuto migliaia di nuovi elettori alla larga dalle urne.

Storicamente, in Alabama il voto è stato precluso a chi aveva precedenti politici, un espediente col quale sono state ulteriormente indebolite le minoranze. In base ai *Black Codes* adottati in molti stati

del Sud, anche reati minori (come il furto di bestiame) venivano considerati gravi crimini, portando all'esclusione perenne dal voto degli afroamericani che li commettevano. Nel 2017, il parlamento dell'Alabama ha abrogato questa legge, dando a quasi 60mila persone la possibilità di riappropriarsi del diritto di voto. Il segretario di Stato non si è però dato da fare perché la notizia si diffondesse, e pertanto ancora molti cittadini non sono a conoscenza dei propri diritti. Chi prova invece a farli valere, si scontra con ostacoli amministrativi e una scarsa comprensione della legge da parte degli ufficiali locali e statali.

Si può togliere il diritto di voto a qualcuno anche cancellandone il nome dalle liste a sua insaputa, ad esempio depennando chi non ha votato alle ultime tornate elettorali. Gli elettori inattivi difficilmente ritornano alle urne prima della cancellazione definitiva. Con questo metodo, a partire dal 2015 l'Alabama ha tolto dai propri registri elettorali 658mila elettori saltuari.

Rientriamo quindi nella categoria dei carichi amministrativi già affrontati nel capitolo 32. Per i cittadini ricchi e delle classi più agiate, questi carichi non rappresentano un grande ostacolo, ma per chi non ha a disposizione tempo o denaro, per chi si affaccia per la prima volta sul mondo della politica o per chi è diversamente abile, regole del genere rendono più difficile votare. In molti si armano di buona volontà e cercano di votare malgrado queste regole, senza però riuscirci. In genere queste regole limitano la partecipazione al voto di chi è più povero o appartiene a una minoranza, persone che tendono a votare per il partito Democratico. A causa di questi hack, in Alabama, solo il 69% degli aventi diritto è registrata per votare.

1. Joshua Shiver (16 aprile 2020), “Alabama Constitution of 1875”, *Encyclopedia of Alabama*, http://encyclopediaofalabama.org/article/h-4195.
2. Alabama Legislature (22 maggio 1901), “Constitutional Convention, second day”, www.legislature.state.al.us/aliswww/history/constitutions/1901/proceedings/1901_proceedings_vol1/day2.html.
3. John Lewis e Archie E. Allen (1° ottobre 1972), “Black voter registration efforts in the South”, *Notre Dame Law Review* 48, n. 1, p. 107, https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=2861&context=ndlr.
4. Rachel Knowles (10 febbraio 2020), “Alive and well: Voter suppression and election mismanagement in Alabama”, Southern Poverty Law Center, www.splcenter.org/20200210/alive-and-well-voter-suppression-and-election-mismanagement-alabama#Disenfranchisement.
5. en Culture staff (16 novembre 2014), “Watch Harvard students fail the literacy test Louisiana used to suppress the Black vote in 1964”, *Open Culture*, www.openculture.com/2014/11/harvard-students-fail-the-literacy-test.html.

CAPITOLO 40

Altri hack elettorali

Un altro tipo di hack della agency interviene direttamente sul processo di voto. Ci sono cittadini registrati intenzionati a votare per un candidato che non ci aggrada? Bene, possiamo rendere il loro voto tanto scomodo da convincerli a non recarsi nemmeno alle urne. Molti hack di questo tipo possono rientrare nella categoria dei carichi amministrativi.

Subito dopo la ratifica del quindicesimo emendamento, gli Stati del Sud adottarono restrizioni al voto che non citavano la razza in modo esplicito, ma che riuscivano comunque a colpire soprattutto i cittadini neri, come ad esempio l'imposta sulle persone fisiche che i più poveri non potevano permettersi di pagare. Altre regole impedivano di votare a qualcuno se i suoi nonni non avevano diritto di voto prima della Guerra Civile, per non parlare dei già citati test di alfabetizzazione, architettati in modo diabolico, somministrati a cittadini accuratamente selezionati, e valutati in modo sleale. Gran parte di questi hack[1] vennero vietati solo dopo l'approvazione del ventiquattresimo emendamento (ratificato nel 1964), il Voting Rights Act del 1965 e la sentenza del 1966 della Corte Suprema degli Stati Uniti sul caso South Carolina vs Katzenbach. Nel 2015, la Corte Suprema ha cassato alcuni passaggi fondamentali del Voting Right Act, consentendo il ritorno di alcune di queste tattiche, soprattutto sotto forma di leggi sull'identificazione degli elettori. Ad esempio, in Alabama, per poter votare gli elettori devono presentare una carta d'identità con foto rilasciata dallo Stato. Quasi il 25% di loro vive però a più di dieci miglia da un dipartimento della motorizzazione (che rilascia patenti e documenti d'identità) e in molti casi non possiede un'auto. Si tratta in genere dei cittadini più poveri, in larga parte appartenenti a minoranze. Le autorità statali hanno provato inoltre a chiudere trentuno uffici della motorizzazione, situati tutti nelle sei contee dove più del 70% della popolazione è afroamericano.

Il piano non è stato attuato grazie all'opposizione del dipartimento dei trasporti degli Stati Uniti. Ci sono comunque più di 100mila potenziali elettori dell'Alabama che non dispongono di un documento accettabile: insieme costituiscono un po' meno del 3% degli elettori dello Stato, ma più del 10% degli elettori afroamericani.

Si può discutere dell'opportunità di creare un ostacolo amministrativo e del bilanciamento tra il garantire l'esercizio di un diritto legittimo e impedire quello di un diritto inesistente. Certo, può avere un senso accertarsi che non voti nessuno che non ne abbia il diritto, ma visto il tasso estremamente basso di brogli (come confermato più volte dai tribunali di tutto il Paese) è evidente che le misure appena descritte cerchino solo di impedire di votare a chi in realtà avrebbe tutto il diritto di farlo.

Un altro sistema per impedire a qualcuno di votare[2] è fare in modo che non abbia seggi elettorali vicino a casa. Dal 2013 in poi, l'Alabama ha cominciato a chiudere un gran numero di seggi, soprattutto nei quartieri afroamericani. Ad esempio, nella città di Daphne (28mila abitanti), nel 2016 si è passati da cinque a due seggi; i tre seggi eliminati si trovavano nelle zone a prevalenza afroamericana.

Ma l'Alabama è solo un esempio. Ci sono anche altri Stati altrettanto aggressivi e sempre più bellicosi nel combattere il diritto di voto. Le autorità della Georgia, ad esempio, richiedono documento d'identità e certificato di cittadinanza, cancellano i nomi dai registri, impediscono il voto postale e chiudono i seggi più comodi per la comunità afroamericana (e non parliamo della Florida!). In tutto il Paese vengono approvate nuove misure per impedire il voto ai giovani, soprattutto agli universitari attivisti che si suppone votino per il Partito democratico.

In fatto di hack la pratica del *gerrymandering* non è una novità. Il termine (Gerry + *salamander*) è dovuto al governatore del Massachusetts – firmatario della Dichiarazione d'Indipendenza – Elbridge Gerry. Nel 1812 Gerry promulgò una legge che a Boston creava un distretto senatoriale dai confini tanto tortuosi da ricordare una salamandra, appositamente studiato per rafforzare i voti ai Federalisti e frammentare quelli per i Democratici-Repubblicani.

L'idea di base è che se si riesce a controllare le proporzioni dei diversi elettorati nei vari collegi è possibile influenzare il risultato finale e ottenere una maggiore rappresentanza all'interno di un organismo legislativo multicircoscrizionale. Si può operare sulla composizione demografica dell'elettorato per vincere di poco – ad esempio del 10% – in molti collegi, lasciandone pochi al partito avversario, nei quali potrà vincere con una percentuale altissima, anche del 90%.

Ci sono due modi per attuare la pratica del gerrymandering. La prima è quella di "ingolfare" un collegio elettorale riempiendolo di quanti più elettori del partito d'opposizione possibile. In questo modo il partito al governo potrà prevalere più facilmente nei collegi vicini, dove l'opposizione risulterà indebolita. Il secondo è quello di "spaccare" un collegio, dividendo gli aggregati di elettori avversari in molti distretti, aumentando le possibilità che si trovino in minoranza.

C'è di fondo un problema di conflitto di interessi: i legislatori incaricati di stabilire i confini dei collegi ne trarranno vantaggio. La soluzione, evidente per chiunque si sia occupato del tema, è quella della compartimentazione. Bisognerebbe affidare la progettazione dei collegi a commissioni indipendenti che non abbiano interesse a sfruttare il risultato del proprio lavoro. Nel 2018, il Michigan ha approvato un referendum che imponeva la creazione di una commissione simile. Ancora nel 2020 i Repubblicani si opponevano a tale commissione, segno della forza del gerrymandering.

A prescindere da come e dove votino i cittadini, i politici possono usare un'infinità di metodi per hackerare le elezioni. Chi è al governo può deciderne la data, può influenzare conteggio e controllo dei voti, e decidere quali candidati e proposte referendarie passeranno al vaglio dei cittadini. In alcuni territori esistono le commissioni elettorali, che possono perfino squalificare un potenziale candidato per questioni di tempistiche, di mancanza di firme o altri aspetti tecnici. L'uso selettivo di questi poteri è un hack.

Vediamone ancora uno: nel 2018, il governatore del Wisconsin Scott Walker si rifiutò di indire un'elezione speciale per alcuni seggi del Parlamento statale, nel timore che potessero vincere i democratici, capitolando solo dopo la sentenza in appello di un

giudice federale. Anche i governatori di Florida e Michigan hanno provato lo stesso hack. Nel 2018, Stacey Abrams quasi perse le elezioni per la carica di governatore a vantaggio di Brian Kemp, che come segretario di Stato aveva supervisionato le elezioni e poco prima del voto aveva cancellato dai registri mezzo milione di elettori.

1. Constitutional Rights Foundation (ultimo accesso 1° giugno 2022), "Race and voting", www.crf-usa.org/brown-v-board-50th-anniversary/race-and-voting.html; Corte Suprema degli Stati Uniti (7 marzo 1966), South Carolina *vs* Katzenbach (Case No. 22), 383 U.S. 301, http://cdn.loc.gov/service/ll/usrep/usrep383/usrep383301/usrep383301.pdf.
2. Peter Dunphy (5 novembre 2018), "When it comes to voter suppression, don't forget about Alabama", Brennan Center, www.brennancenter.org/our-work/analysis-opinion/when-it-comes-voter-suppression-dont-forget-about-alabama.

CAPITOLO 41

Soldi e politica

Il denaro può controllare l'informazione e influenzare le scelte dei cittadini. Può inoltre comprare l'agency: il potere di dar vita a un cambiamento. Questi hack hanno natura politica in quanto sovvertono l'intento originale del processo di voto democratico. Lo vediamo soprattutto negli Stati Uniti, dove le elezioni hanno un costo esorbitante per una serie molto complessa di motivi. Ne elencherò solo quattro, i più importanti.

Uno, negli Stati Uniti i cicli elettorali sono molto lunghi; i candidati iniziano la propria campagna più di un anno prima delle elezioni. (Per fare un paragone, in Giappone una campagna elettorale dura nel complesso dodici giorni, in Francia due settimane, in Gran Bretagna in media da due a quattro settimane. In Australia o in Canada nessuna campagna ha mai superato le undici settimane, durata record che si è verificata solo nel 1910 e nel 1926). Due, negli Usa la disciplina di partito è più debole rispetto agli altri Paesi. Dove i partiti sono molto coesi, ha meno senso foraggiare i candidati per farli scontrare tra di loro nelle primarie. Tre, gli Usa sono un Paese molto vasto, con una popolazione molto numerosa e le pubblicità in tv costano tanto. A differenza di quanto accade in altri Paesi, non c'è limite a quanto si può spendere. Quattro, negli Usa ci sono talmente tanti loophole nelle leggi sulla trasparenza dei finanziamenti che chi accetta contributi inappropriati (ad esempio da altri Paesi) per le sue campagne elettorali di rado viene chiamato a risponderne. Diviene in tal modo molto più semplice hackerare le norme sui finanziamenti e servirsi dei propri patrocinatori per hackerare il processo politico. Ai ricchi piacciono questi hack e si danno da fare per legalizzarli, con lo scopo di acquisire ancor maggior influenza politica.

Dopo l'approvazione del Federal Election Campaign Act del 1972 e dei suoi emendamenti del 1974 che limitavano contributi e spese, un provvedimento del 1976[1] vietò le spese a sostegno di un partito o di

un candidato, ma non quello "in coordinamento" con un partito o un candidato. La decisione diede il via all'ascesa del *soft money*, denaro speso per attività volte a "rafforzare il partito", in genere attaccando gli altri candidati con pubblicità mirate. Nel corso degli anni, spesso il potere economico ha cercato di aggirare i limiti ai finanziamenti ai partiti. Nel 2002 ci mise una pezza il Bipartisan Campaign Reform Act. Con nuove regole arrivano però nuovi hack. Una proposta del 2010 di Citizens United, resa effettiva nel 2014 da una sentenza della Corte Suprema degli Stati Uniti, riaprì le porte all'utilizzo politico di finanziamenti d'ogni sorta, prima proibiti, compresi quelli provenienti dalle aziende.

Certo, il denaro non garantisce il successo in politica, ma quando ce n'è poco o nulla il fallimento è assicurato. Come sostiene il professore di diritto di Harvard Lawrence Lessig,[2] "per partecipare alla corsa politica, devi prima vincere la corsa all'oro". È il denaro che consente di restare a galla in un processo lungo come quello delle primarie americane. L'abbiamo visto nelle primarie repubblicane del 2012,[3] influenzate dall'appoggio dato a candidati poco appetibili dai miliardari Sheldon Adelson, Foster Friess e Jon Huntsman Sr. Possiamo definirlo l'equivalente politico del sistema del venture capital. Convincere qualche ricco investitore a scommettere sulla tua candidatura è più importante delle tue qualità reali.

Il denaro può contribuire a seminare il caos. Il sistema politico statunitense è di fatto bipartitico; lo si può hackerare finanziando un candidato indipendente o di un terzo partito per erodere i voti del proprio rivale. Un repubblicano può ad esempio appoggiare finanziariamente un candidato liberal non affiliato per indebolire il principale candidato democratico. Allo stesso modo, un democratico può finanziare un conservatore indipendente per dividere i repubblicani.

Negli Usa, l'hack del "guastatore indipendente" non è facile da attuare, visto che si tratta di una vulnerabilità alla quale entrambi i partiti vogliono mettere le patch. Alcuni Stati fissano scadenze molto rigorose, penalizzando chi entra in gara in extremis, oppure stabiliscono regole che rendono più arduo arrivare al voto per chi non è democratico o repubblicano. Quarantaquattro Stati adottano la

legge del *sore loser*, la legge di chi non sa perdere, per impedire a chi ha perso le primarie di ripresentarsi alle stesse elezioni come candidato indipendente.

Non vuol dire però che questo hack non venga mai attuato. Dopo aver constatato l'influenza di Ralph Nader sulle elezioni del 2000, in tutto il Paese i dirigenti repubblicani hanno cercato di sfruttare i candidati del Green Party[4] per togliere voti ai democratici. Nel 2002, a Seattle, Young Han, un diciottenne che aveva fatto volontariato per Nader, aveva deciso di presentarsi alle elezioni. Un certo "Mr Shore" aiutò Han a presentare la sua candidatura, contribuendo anche economicamente alla sua campagna. Mr Shore era però uno stratega repubblicano di Washington DC, e anche sua moglie stava dando il proprio appoggio a un candidato verde di Seattle. Qualcosa del genere è successo anche in Arizona nel 2010, a New York nel 2014, e in Montana nel 2018 e 2020. Sempre nel 2020, i Repubblicani hanno appoggiato il tentativo di Kanye West di presentarsi alle presidenziali, con la speranza che avrebbe sottratto voti a Joe Biden. Si è trattato sempre di hack falliti, in quanto una strategia del genere è più facile a dirsi che a farsi.

Confondere le acque la rende più efficace. Nel 2020, in Florida, alle elezioni per il Congresso, Alex Rodriguez,[5] un "ex" repubblicano, ha sfidato il quasi omonimo Jose Rodriguez, senatore dello Stato, usando il suo stesso cavallo di battaglia: il cambiamento climatico. Alex non aveva alcuna esperienza politica e non ha fatto nulla durante la campagna elettorale: è bastata la confusione causata per fargli ottenere il 3% dei voti. La repubblicana Ileana Garcia ha vinto per soli trentadue voti, dopo un secondo spoglio manuale delle schede. La campagna elettorale di Alex Rodriguez aveva ricevuto 550.000 dollari da un'azienda appena fondata, chiamata Proclivity Inc., e da *political action committee*, comitati di sostegno elettorale, collegati a esponenti repubblicani.

Questa strategia per dividere i voti può arrivare a livelli assurdi. In India capita spesso di sfidare un candidato mettendogli contro qualcuno che abbia il suo identico nome e cognome.[6] Nelle elezioni parlamentari del 2014, ad esempio, quattro dei trentacinque candidati a un determinato seggio si chiamavano Lakhan Sahu, e uno

solo di loro era un politico vero e in grado di vantare qualche esperienza. Il candidato del principale partito di opposizione dichiarò che era solo "una pura coincidenza" che così tanti Lakhan Sahu avessero deciso di scendere in campo contemporaneamente.

La grande vulnerabilità degli Usa è il sistema bipartitico, ma anche il sistema uninominale secco che consente a chi ottiene più voti di prendersi tutto è un grosso punto debole. E un sistema che richiede solo una maggioranza relativa fa in modo che un candidato venga indebolito dalla competizione di qualcuno con un profilo politico (o perfino con un nome) simile al suo. Il voto di una certa area politica si frammenta.

Un sistema per porvi rimedio è quello di chiedere agli elettori di classificare i candidati in ordine di preferenza. Il candidato con meno voti viene eliminato, e si torna a votare con lo stesso meccanismo, facendo una classifica dei candidati rimasti fino a quando uno ottiene la maggioranza. Questo sistema previene la partecipazione di guastatori esterni (i suoi voti verrebbero spostati a un candidato diverso, probabilmente proprio quello che avrebbero voluto danneggiare) e contribuisce alla vittoria del candidato preferito dalla vera maggioranza degli elettori. Le elezioni parlamentari australiane del 2022 ne hanno dimostrato l'efficacia: i voti ricevuti da molti candidati di partiti indipendenti al primo turno non sono andati "sprecati" nella tornata successiva.

1. Yasmin Dawood (30 marzo 2015), “Campaign finance and American democracy”, *Annual Review of Political Science*, www.annualreviews.org/doi/pdf/10.1146/annurev-polisci-010814-104523.
2. Lawrence Lessig (2014), *The Usa Is Lesterland*, CreateSpace Independent Publishing Platform.
3. Kenneth P. Vogel (12 gennaio 2012), “3 billionaires who’ll drag out the race”, *Politico*, www.politico.com/story/2012/01/meet-the-3-billionaires-wholl-drag-out-the-race-071358.
4. Sam Howe Verhovek (8 agosto 2001), “Green Party candidate finds he’s a Republican pawn”, *New York Times*, www.nytimes.com/2001/08/08/us/green-party-candidate-finds-he-s-a-republican-pawn.html.
5. Sun-Sentinel Editorial Board (25 novembre 2020), “Evidence of fraud in a Florida election. Where’s the outrage?”, *South Florida Sun-Sentinel*, www.sun-sentinel.com/opinion/editorials/fl-op-edit-florida-election-fraud-20201125-ifg6ssys35bjrp7bes6xzizon4-story.html.
6. Rama Lakshmi (23 aprile 2014), “Sahu vs. Sahu vs. Sahu: Indian politicians run ‘clone’ candidates to trick voters”, *Washington Post*, www.washingtonpost.com/world/sahu-vs-sahu-vs-sahu-indian-politicians-run-clone-candidates-to-trick-voters/2014/04/23/613f7465-267e-4a7f-bb95-14eb9a1c6b7a_story.html.

CAPITOLO 42

Hackerare per distruggere

Nel 1729, Parigi dichiarò il default sulle sue obbligazioni municipali. Il governo organizzò una lotteria che consentiva a ogni creditore di comprare biglietti in base al valore delle proprie obbligazioni: il costo di un biglietto era di un millesimo di obbligazione. Ogni mese il governo sorteggiava il vincitore e lo premiava elargendogli il valore nominale dei suoi titoli e un bonus di 500.000 livre. Voltaire si accorse che il premio era superiore al numero dei biglietti venduti, e così – ecco a voi un perfetto hack – formò un'associazione[1] con alcuni ricchi finanziatori per comprare tutti i titoli e i biglietti necessari. In meno di due anni di vittorie, mese dopo mese, accumularono circa 7,5 milioni di franchi, che oggi equivarrebbero a circa 100 milioni di dollari. Gli organizzatori della lotteria parigina a un certo punto si resero conto che erano sempre le stesse persone a riscuotere i premi. Voltaire, col suo tipico fare da Voltaire (e ben consapevole che niente dura per sempre, quindi valeva la pena di divertirsi), sul retro dei biglietti scrisse anche degli indovinelli che aiutarono il governo a rintracciare l'hacker. Il ministero delle Finanze francese portò in tribunale l'associazione, ma visto che non aveva fatto niente di illegale, poté tenere la cifra vinta. Con una decisione estrema – ma efficace – il governo parigino mise fine alla lotteria.

Più di recente, lo Stato dell'Ohio ha creato un sito dove gli impiegati potevano segnalare i colleghi che si erano rifiutati di lavorare durante la pandemia di Covid-19, in modo che non potessero accedere ai sussidi di disoccupazione. Un hacker si è accorto che non era necessario autenticarsi per segnalare qualcuno e che pertanto tutti potevano farlo. Ha scritto un programma che creava false segnalazioni[2] – aggirando anche il Captcha, la procedura per dimostrare di essere umani – e l'ha postato online. Non sappiamo quante segnalazioni automatiche abbiano raggiunto il sistema online, e gli ufficiali del governo dell'Ohio sostengono di

essere riusciti a isolarle ed eliminarle tutte, il risultato è stato comunque l'abbandono del sito come strumento per tagliar fuori alcuni cittadini dai sussidi di disoccupazione.

Come abbiamo visto nel capitolo 10, gli hack hanno una natura parassitica e come ogni parassita devono trovare un equilibrio tra la sovversione di un sistema e la sua distruzione. Troppo hacking può fare collassare un sistema. A volte, come nel caso della lotteria di Parigi, l'eccessivo successo di un hack porta alla cancellazione di un sistema. In altri casi, come in quello del sito dell'Ohio, lo scopo dell'hacker è proprio quello di far chiudere un sistema.

Gli hack con scopo di lucro in genere non vogliono distruggere il sistema hackerato. Troppi hack ai bancomat potrebbero portare alla loro scomparsa. Hackerare uno sport fino a renderlo poco divertente da praticare o da guardare significa condannarlo a morte. In questi casi, gli hacker vogliono invece mantenere in vita il sistema, e al contempo ottenere qualche vantaggio per sé stessi. L'eventuale distruzione di un sistema è pertanto in genere imprevista e indesiderata.

Non è così quando gli hacker agiscono in nome di una convinzione morale. In quel caso hackerano il sistema perché lo disapprovano e non per sfruttarlo. Come nel caso dell'hacker del sito dell'Ohio, lo scopo è ridurne funzionalità ed efficacia o distruggerlo. Un altro esempio del genere si è verificato nel 2020, quando gli utenti di TikTok si sono coordinati per inviare false richieste di biglietti per l'evento elettorale di Trump a Tulsa,[3] con lo scopo di fargli trovare un palazzetto vuoto. È stato un hack molto semplice, che sfruttava il fatto che per prenotare un biglietto bastassero un indirizzo email falso e un numero di telefono fittizio, facilmente ottenibile con Google Voice. Il sistema di biglietteria non è stato distrutto, ma Trump è stato comunque beffato dallo scarso numero di presenti. Da quel momento in poi, la sua campagna ha adottato un sistema di biglietteria meno vulnerabile. Qualunque sia la spinta iniziale, l'hacking può distruggere sistemi sociali su scala molto più vasta della lotteria di Voltaire, della biglietteria di Trump o del sito per i sussidi di disoccupazione in Ohio. Lo abbiamo visto nel 2008, con la crisi delle banche: ripetuti hack del sistema hanno quasi portato al

collasso l'intera rete finanziaria degli Stati Uniti. Vale anche per l'influenza del denaro sulla politica americana, con la disinformazione e coi social network. Quando c'è una rivoluzione, tutti i meccanismi di una società vengono hackerati per perseguire uno scopo del tutto nuovo. L'hacking può essere una cosa positiva, necessaria all'evoluzione di un sistema, ma può anche verificarsi in modo eccessivo e troppo in fretta.

Pensiamo a un altro esempio dal mondo dell'economia: la carta moneta. Risale perlomeno all'Undicesimo secolo, ai tempi della dinastia Sung in Cina, ed è un hack. Il denaro dovrebbe rappresentare una cifra con un valore economico reale, ma i governi hanno il potere di stampare tutto il denaro che vogliono, a prescindere dall'effettiva produttività dell'economia. In tal modo, i governi possono hackerare i sistemi di finanziamento pubblico stampando abbastanza denaro da pagare i propri debiti, invece di finanziare i propri programmi tramite le tasse o il debito con investitori privati. Il primo ad attuare questo hack in Europa fu l'economista John Law, per aiutare Luigi XV di Francia a finanziare le sue guerre. Si tratta di un hack positivo, oggi normalizzato. La capacità di stampare denaro è essenziale nelle crisi economiche. È così che nel 2008-2009 il governo degli Stati Uniti finanziò gli interventi volti a calmierare i mercati, ed è così che si è posto un freno al fallout economico dopo la pandemia e i lockdown del 2020. Questo hack ha in parte permesso al governo degli Stati Uniti di pagare l'enorme mobilitazione militare decisiva per vincere la Prima e la Seconda Guerra Mondiale.

Se un governo si affida troppo a questa pratica per finanziare il debito con l'estero, gli effetti però possono essere nefasti. L'iperinflazione è rara, ma può causare danni enormi in pochissimo tempo. Nel 2007 lo Zimbabwe attraversò un periodo di iperinflazione[4] e nel giro di un anno il dollaro locale perse il 99,9% del suo valore. La ricchezza media precipitò sotto i livelli del 1954 e l'ammontare di denaro col quale un tempo si potevano comprare dodici auto non bastava più a pagare una pagnotta. In Venezuela l'iperinflazione iniziata nel 2017[5] ha fatto talmente lievitare i prezzi che una famiglia aveva bisogno di cento volte il salario minimo per

comprare i beni di prima necessità; più del 10% della popolazione è stato pertanto costretto a emigrare.

Possiamo trovare altri esempi di hacking che porta alla distruzione nella recente ascesa di governi autoritari in tutto il mondo, in Paesi come Russia, Siria, Turchia, Filippine, Ungheria, Polonia, Brasile ed Egitto. Ancora si tengono le elezioni, col conteggio dei voti. I parlamenti approvano ancora le leggi, e i tribunali le fanno rispettare. Almeno formalmente continuano a sussistere i diritti di parola e di libera associazione. Tutti questi meccanismi e istituzioni sono stati però hackerati, e sottoposti alle esigenze della dittatura.

Ci sono invece sistemi che devono essere hackerati per poter essere distrutti. I boicottaggi e la disobbedienza civile sono hack: sovvertono le regole di politica e mercati per protestare contro pratiche ritenute ingiuste. Suscitano una reazione che rende esplicita la violenza e la crudeltà implicite nel sistema, e mettono al centro dell'agenda politica la distruzione di sistemi quali leggi discriminatorie non più accettabili come "normali" e che è impossibile continuare a ignorare. Abbiamo una sfida davanti a noi: fare in modo che i nostri hack distruggano le cose sbagliate e non intacchino quelle giuste... oltre alla sfida di saperle distinguere.

1. Andy Williamson (16 maggio 2013), "How Voltaire made a fortune rigging the lottery", *Today I Found Out*, www.todayifoundout.com/index.php/2013/05/how-voiltaire-made-a-fortune-rigging-the-lottery.
2. Janus Rose (8 maggio 2020), "This script sends junk data to Ohio's website for snitching on workers," *Vice*, www.vice.com/en_us/article/wxqemy/this-script-sends-junk-data-to-ohios-website-for-snitching-on-workers.
3. Taylor Lorenz, Kellen Browning e Sheera Frenkel (21 giugno 2020), "TikTok teens and K-Pop stans say they sank Trump rally", *New York Times*, www.nytimes.com/2020/06/21/style/tiktok-trump-rally-tulsa.html.
4. Janet Koech (2012), "Hyperinflation in Zimbabwe," *Federal Reserve Bank of Dallas Globalization and Monetary Policy Institute 2011 Annual Report*, www.dallasfed.org/~/media/documents/institute/annual/2011/annual11b.pdf.
5. Patricia Laya and Fabiola Zerpa (5 ottobre 2020), "Venezuela mulls 100,000 Bolivar bill. Guess how much it's worth?", *Bloomberg*, www.bloomberg.com/news/articles/2020-10-05/venezuela-planning-new-100-000-bolivar-bills-worth-just-0-23; Gonzalo Huertas (settembre 2019), "Hyperinflation in Venezuela: A stabilization handbook", Peterson Institute for International Economics Policy Brief 19-13, www.piie.com/sites/default/files/documents/pb19-13.pdf.

PARTE SESTA
HACKERARE I SISTEMI COGNITIVI

CAPITOLO 43

Gli hack cognitivi

Negli anni Novanta, quando ancora i biglietti aerei erano di carta, usavo sempre un hack per risparmiare. Prendere la carta d'imbarco e comprare il biglietto erano due azioni distinte: potevi ottenere la carta d'imbarco con settimane d'anticipo sul volo e per farlo dovevi parlare con una persona in carne e ossa. Vivevo a Washington DC, e spesso dovevo prendere l'aereo per motivi di lavoro. Mi avrebbe fatto comodo passare i weekend a Chicago, ma al lavoro non mi avrebbero pagato una tappa tanto costosa. Per fortuna avevo trovato un hack. Supponiamo che avessi un biglietto per andare di domenica da Seattle a Washington, con scalo a Chicago. Andavo alla biglietteria e mi facevo stampare le carte d'imbarco, che venivano spillate ai miei biglietti. Le toglievo e le mettevo da parte. Qualche giorno dopo ritornavo in biglietteria e spostavo al venerdì entrambi i voli (all'epoca costava poco farlo). L'agente registrava il cambiamento sul suo computer e mi dava un altro paio di carte d'imbarco, sempre spillate allo stesso biglietto. Poi volavo da Seattle a Chicago di venerdì, e passavo il weekend a Chicago. La domenica tornavo in aeroporto e andavo al gate del volo per Washington col mio biglietto originale e la vecchia carta d'imbarco (che ovviamente avevo conservato). Per quanto la mia prenotazione non fosse più registrata sul computer, avevo un biglietto e una carta d'imbarco con la data giusta. Nel caso qualcuno mi avesse chiesto qualcosa, avevo anche biglietto e carta d'imbarco per il volo di domenica da Seattle a Chicago. L'addetto al gate, in preda alla confusione, non dava retta a quello che gli diceva il computer e mi stampava una nuova carta d'imbarco, lasciandomi salire sull'aereo.

Un hack fantastico, che ha funzionato fino a quando le compagnie aeree sono passate ai biglietti elettronici e hanno abbandonato le carte d'imbarco separate. Chiediamoci però che cosa stessi hackerando. Non si trattava del sistema di prenotazione della

compagnia aerea. Il computer diceva esplicitamente che non avevo alcuna prenotazione per quel volo. In realtà stavo hackerando l'addetto al gate. Ero un maschio bianco, sicuro di sé, dotato di un biglietto impeccabile e di una carta d'imbarco. Il problema poteva essere attribuito a un pasticcio del computer, o almeno così conveniva pensare all'addetto. Per quanto possa sembrare strano, stavo hackerando la sua mente.

Il nostro cervello è un sistema, che si è evoluto nel corso di milioni di anni per salvarci la pelle e – cosa ancor più importante dal punto di vista dei nostri geni – per continuare a farci riprodurre. L'interazione ininterrotta con l'ambiente circostante ha permesso di ottimizzare tale sistema, ma si è trattato di un'ottimizzazione per gli esseri umani che 100mila anni fa vivevano in piccoli gruppi familiari negli altopiani dell'Africa orientale, e non per chi vive nel Ventunesimo secolo a New York, Tokyo o Nuova Delhi. Il cervello umano può essere manipolato in virtù di tutte le scorciatoie cognitive che prende per adattarsi al contesto sociale moderno.

Definire il presunto funzionamento "naturale" dei sistemi biologici, psicologici e sociali e affermare che un hack possa sovvertirne gli intenti può apparire semplicistico. Non sono sistemi il cui funzionamento sia stato pianificato. Si tratta però di una semplificazione che ci può aiutare a contestualizzare i nostri ragionamenti. Possiamo ipotizzare lo "scopo" o "l'intento" dei sistemi biologici e psicologici – lo scopo del pancreas o della fiducia – rifacendoci solo al processo evolutivo (come nel caso dei sistemi politici, altro esempio di sistema senza un progettista univoco). Gli hack prendono di mira questi sistemi in modo creativo e anche in questo caso sfruttano una vulnerabilità per sovvertirne l'intento.

L'hacking dei sistemi cognitivi è molto potente. Molti dei sistemi alla base della nostra società – la democrazia, l'economia di mercato ecc. – si basano sul fatto che gli esseri umani prendano decisioni razionali. Nei capitoli precedenti, abbiamo visto una serie di hack in grado di limitare uno dei tre aspetti di una decisione razionale. Informazione, scelta e agency. Nei capitoli seguenti, vedremo come sia possibile hackerarli in modo diretto, nella nostra mente.

Ad esempio, la disinformazione è un hack che sovverte il sistema

della libertà di parola e della libertà di stampa. Non è certo una novità. Goebbels, ministro della Propaganda di Hitler, dichiarò: "Uno degli aspetti più ridicoli della democrazia rimarrà sempre il fatto che abbia offerto ai suoi nemici mortali i mezzi per distruggerla".[1] La disinformazione sovverte molti dei sistemi cognitivi che prenderemo in esame: attenzione, persuasione, fiducia, autorità, tribalismo e talvolta anche la paura.

Gli hack cognitivi stanno a monte di tutti gli altri. Le leggi governano i fondamenti di tutte le transazioni economiche e molte altre aree della nostra società, parlamenti e tribunali si occupano di creare e far funzionare le leggi, la Costituzione di una nazione (o una carta equivalente) fissa le regole del processo legislativo e del sistema giudiziario. I nostri sistemi sociali – e tutti i sistemi tecnologici che prevedono l'interazione con utenti umani – si basano però su come le persone pensano, e molto spesso sulle scorciatoie cognitive usate per pensare. Chi è in grado di hackerare le menti può hackerare qualunque sistema governato dall'azione umana.

Gli hack cognitivi sono antichi quanto la nostra specie e spesso sono stati normalizzati talmente tanto tempo fa che non ci rendiamo neanche più conto della loro presenza, e ovviamente non li riteniamo hack. Gli esseri umani sono intelligenti e consapevoli, possiedono una teoria della mente e la capacità di pianificare: per questo i nostri hack sono più complessi di quelli di ogni altra creatura. Come gran parte degli hack che abbiamo già visto, quelli cognitivi prendono di mira informazione, scelta o agency necessarie a prendere decisioni consapevoli ed efficaci.

Nel corso degli ultimi cinquant'anni, a causa dei computer e delle loro interfacce, si sono moltiplicate le occasioni di manipolare le percezioni degli altri. Gli algoritmi e la scienza del comportamento rendono la manipolazione ancor più rapida e complessa, con effetti tangibili.

Certo, non sempre è così. Cory Doctorow, scrittore e attivista, ci consiglia di non credere ciecamente alla "tesi che Big Tech abbia usato i big data per creare un raggio in grado di controllare la mente e venderci i fidget spinner".[2] Nei prossimi capitoli parlerò soprattutto di spinte (nudges) cognitive che ci orientano verso determinate

direzioni. Ignorare queste tecniche è un grosso rischio, in quanto, anche grazie alle AI, diventeranno sempre più efficaci.

Quando si tratta di sistemi cognitivi, in genere non basta applicare una patch, anche se la consapevolezza di un hack è per sua natura una patch. Per difenderci dagli hack cognitivi abbiamo bisogno di prevenirli e limitarne i danni. Molte truffe funzionano perché riescono a hackerare emozioni quali avidità, fiducia o paura.

Non possiamo applicare una patch al nostro cervello, ma possiamo usare vari sistemi per dichiarare illegali determinati hack – stabilendo quindi che oltrepassano i confini del comportamento accettabile – e educare le vittime potenziali a starne alla larga.

Un'ultima puntualizzazione: gli hack dei sistemi cognitivi non sono delineati in modo netto come quelli descritti nei precedenti capitoli. Ad esempio, pensiamo ai molti trucchetti nel design delle interfacce web usate durante la campagna elettorale di Trump per spingere le persone a donare più di quanto volessero e per scopi diversi dal finanziamento della campagna: spunte precompilate che autorizzavano prelievi settimanali dal conto del donatore, somme scritte in piccolo, autorizzazioni minuscole a usare il denaro per le spese personali del candidato e così via. Sono chiaramente hack: esempi tipici del *dark pattern*, un tema che affronteremo in seguito. Li possiamo però definire come hack delle nostre percezioni, delle nostre emozioni oppure del nostro sistema decisionale? Sono un po' tutte e tre le cose, ed è un'ambiguità che non mi infastidisce. Gli esseri umani sono complicati. I sistemi cognitivi sono incasinati. Se vogliamo parlarne, dobbiamo essere pronti a un po' di casino.

1. Jason Stanley (2016), *How Propaganda Works*, Princeton University Press, https://press.princeton.edu/books/paperback/9780691173429/how-propaganda-works (ed it. *La propaganda, cos'è e come funziona*, Mondadori, 2020).
2. Cory Doctorow (26 agosto 2020), "How to destroy surveillance capitalism", *OneZero*, https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59.

CAPITOLO 44

Attenzione e dipendenza

Tutti odiano i pop-up pubblicitari.[1] Perfino il loro inventore, Ethan Zuckerman, si è scusato pubblicamente di averli ideati. Si sono però diffusi a macchia d'olio perché sono remunerativi, e lo sono perché riescono a hackerare l'attenzione quanto basta per aumentare le vendite degli inserzionisti. A differenza dei banner pubblicitari, che in genere riusciamo a ignorare, i pop-up ci costringono a dedicar loro un po' d'attenzione, seppure controvoglia, anche solo per toglierceli dai piedi. In genere ci si piazzano davanti e ci impediscono di vedere quel che volevamo. Molti pop-up alle scritte aggiungono immagini, suoni e video. Bisogna attivarsi per chiuderli, e spesso non è facile capire come farlo, e sono necessari più tentativi. I pop-up funzionano: catturando, seppur per poco, la nostra attenzione, possono avere un effetto a lungo termine.

L'attenzione è un sistema cognitivo che ci permette di focalizzarci sulle cose importanti. In ogni singolo momento, attorno a noi avviene un'infinità di eventi. Abbiamo una mente potente, ma la sua capacità di processare le informazioni è limitata. Non possiamo stare attenti a tutto. Dati i nostri limiti, impieghiamo un'attenzione selettiva. Diamo la priorità a cose ed eventi che favoriscono la nostra sopravvivenza, dando meno attenzione alle cose delle quali già ci fidiamo. La nostra attenzione viene catturata da fenomeni che possono indicare la presenza di un predatore o altre minacce: movimenti improvvisi, rumori forti, luci accecanti. Diamo inoltre la priorità ai fenomeni che possono influire sulla nostra sopravvivenza sociale, come la sicurezza e la nostra posizione all'interno di un gruppo, oppure a fenomeni che riguardano la capacità di attrarre e tenere con noi partner sessuali, o ancora a fenomeni che aiutano il nostro benessere. In quest'ultimo caso, si tratta di qualunque cosa ci dia una ricompensa, che si tratti di cibo, denaro, droghe, sorprese dell'ovetto Kinder o anche solo di un "like" al nostro profilo digitale.

Non possiamo scegliere sempre in modo consapevole come e dove focalizzare la nostra attenzione, visto che gran parte del sistema che lo delibera fa parte dell'hardware del nostro cervello. La pubblicità in sé non cattura la nostra attenzione, ed è per questo che i pubblicitari cercano di hackerare il nostro sistema cognitivo. Negli anni Sessanta del Diciannovesimo secolo, il litografo francese Jules Chéret inventò un nuovo tipo di poster pubblicitario,[2] con colori nitidi e brillanti, belle donne mezze nude e immagini dinamiche: era impossibile da ignorare. Leonetto Cappiello fece progredire ulteriormente questo tipo di pubblicità, con immagini sbalorditive, esagerate, pensate espressamente per essere riconoscibili anche per chi viaggiava nei veloci vagoni della metropolitana di Parigi, all'epoca appena completata.

Da sempre i pubblicitari si sforzano in ogni modo di hackerare la nostra attenzione. È per questo motivo che i supermercati, e perfino i negozi di cancelleria e casalinghi, piazzano i dolcetti prima delle casse, un hack noto come "posizionamento nel punto d'acquisto". Per lo stesso motivo, gli spot televisivi un tempo avevano un volume più alto dei programmi che interrompevano, fino a quando nel 2012 la pratica venne vietata dalla Fcc, la Commissione federale per le comunicazioni. È proprio per una questione d'attenzione che esistono i pop-up.

Dagli anni Cinquanta del Ventesimo secolo, con l'ascesa delle indagini di mercato e delle campagne fondate sugli studi di psicologia, la pubblicità può usare il microtargeting per hackerarci uno per uno. Pubblicitari e data broker accumulano un'enormità di informazioni personali con le quali arricchirsi, mettendo a repentaglio la nostra privacy in nome della caccia all'attenzione.

I circuiti della nostra attenzione vengono hackerati anche sui social network, tramite la manipolazione della rabbia. Facebook ottimizza il nostro feed per mezzo degli algoritmi. Il suo scopo è farci passare più tempo sulla piattaforma – più restiamo su Facebook, più pubblicità vedremo, più l'azienda si arricchirà – e pertanto ci mostra contenuti in grado di catturare la nostra attenzione (non dimentichiamolo: lo scopo di questi sistemi è vendere pubblicità, finalizzata a farci fare acquisti).

Allo stesso modo, Google vorrebbe che passassimo quanto più tempo possibile a guardare video su YouTube (YouTube appartiene a Google). L'algoritmo di YouTube ha capito che i contenuti più estremi e divisivi sono anche i più coinvolgenti: un hack imprevisto ma molto remunerativo. Facebook e YouTube sono divisivi non perché siano stati progettati per questo scopo, ma perché 1) l'algoritmo è ottimizzato per offrire contenuti specifici in base all'interesse dell'utente e 2) i dirigenti hanno deciso di non curarsi degli eventuali effetti collaterali di questa cosa. In ambito politico, questi schemi tendono a polarizzare gli utenti indirizzandoli verso una bolla ideologica abitata da altre persone che condividono la loro visione del mondo e dando la priorità a quei contenuti che suscitano le emozioni più forti. Grazie a un processo sempre più rapido e raffinato, queste piattaforme ci propongono in modo automatico contenuti polarizzati e tagliati su misura per noi e riducono le possibilità di interazioni non filtrate, che magari ci spingerebbero a mettere in discussione le nostre convinzioni.

Si potrebbe affrontare questo problema regolando l'uso delle informazioni per il microtargeting. Dopo le elezioni del 2020, Google ha implementato una policy per limitare il targeting della pubblicità elettorale ad alcune macro-categorizzazioni: età, genere, codice postale. Si tratta di semplici strategie difensive, che potrebbero perfino funzionare, sempre se Google decidesse di farle rispettare. Gli appartenenti a entrambi gli schieramenti fanno però del loro meglio per mandarle all'aria, visto che il microtargeting è di vitale importanza nella politica moderna.

Una soluzione migliore è far rispettare le leggi antitrust. Il fatto che tutti i contenuti siano disponibili nello stesso posto rende tale iper-specializzazione al contempo semplice e problematica. Se invece proliferasse una serie di piccoli social media – ognuno con meno contenuti – tale specializzazione diverrebbe impossibile. L'abbiamo visto con i social media di estrema destra nati dopo che Donald Trump è stato bannato da Twitter, senza dubbio privi della potenza di fuoco dei grandi social media appartenenti ad aziende multinazionali.

L'hacking dell'attenzione mira logicamente alla dipendenza, il

metodo più efficace per non far scappare gli utenti. In questo caso, l'hack risiede nel processo per rendere qualcuno dipendente. Aziende e sviluppatori progettano i loro prodotti perché creino dipendenza, facendo in modo che i loro utenti e clienti continuino a utilizzarli. A volte si tratta di una dipendenza fisiologica, ma in genere tutto comincia da una fissazione comportamentale, che si radica mediante endorfine, adrenalina e altre sostanze neurochimiche innescate da una determinata azione.

Per capire come funzioni una dipendenza comportamentale, pensiamo alle slot machine. Le ricompense variabili – elemento fondante del gioco d'azzardo – creano più dipendenza delle ricompense fisse. Nel dettaglio: la prima fase è caratterizzata da qualcosa che innesca la nostra attenzione. Le slot machine sono progettate per essere quanto più possibili luccicanti e fracassone. Fanno rumore anche quando nessuno le usa, e se qualcuno vince scatenano un gran chiasso. La seconda fase consiste in un'azione che porta ad aspettarsi una ricompensa. È la fase della scommessa: una volta inserita la moneta nella slot, possiamo premere un pulsante. La terza fase è la ricompensa variabile: a volte vinci, a volte perdi. La quarta fase è l'investimento emotivo, che aumenta le possibilità che il giocatore rientri nel loop: a chi non piace un vincitore? Basta solo premere di nuovo il pulsante e – chi può dirlo? – magari vinceremo ancora, e potremmo addirittura ottenere il jackpot.

I giochi online cercano di creare dipendenze proprio grazie alle ricompense variabili, in particolare con quei tesori digitali chiamati *loot boxes*. I giocatori pagano – a volte denaro fittizio, ma in genere soldi veri – e in cambio ricevono una serie casuale di oggetti utilizzabili all'interno del gioco. Gli oggetti di valore sono rari, a volte rarissimi, proprio come il jackpot di una slot machine. Nella progettazione dei videogiochi vengono usati espedienti comportamentisti per tenere agganciati i giocatori: chi lavora nel mondo dei videogiochi sa bene che le aziende vogliono soprattutto creare dipendenza.

Altri prodotti informatici, come le app per smartphone e i social network, vengono progettati in modo molto simile, sempre con lo scopo di tenere agganciato l'utente. L'innesco sta nelle notifiche che

attirano la nostra attenzione: bip, squilli, vibrazioni, notifiche push (esatto: roba da Pavlov). L'azione è l'apertura della app per vedere la notifica, l'anticipazione di una ricompensa. Le ricompense variabili sono i post, i commenti, le immagini e qualunque cosa potrà comparire nel nostro feed.

Non c'è niente di casuale. Se i progettisti lo volessero, le piattaforme digitali potrebbero aggiornare le pagine in modo automatico, senza l'intervento dell'utente. Costringere gli utenti a cliccare o a scorrere la pagina consente però di ricreare la dinamica di una slot machine, offrendo una piccola dose di controllo in grado di creare dipendenza, abituandoci a farlo ripetutamente. Alla stessa stregua, raggruppare le notifiche – inviarle tutte assieme una volta al giorno – ridurrebbe l'impatto delle ricompense variabili e la loro capacità di creare dipendenza, per questo non c'è social media che proponga una soluzione tanto semplice da applicare.

Tendiamo a considerare le dipendenze una sorta di fallimento morale, ma dovremmo invece considerarle un hack molto efficace. Conosciamo le proprietà che portano esperienze e comportamenti a diventare dipendenze. Le aziende possono mettere in atto queste strategie dove vogliono, in genere in modo tanto subdolo che il cliente non se ne accorgerà nemmeno. Come vedremo, gli algoritmi e il rapid testing stanno consentendo alle piattaforme digitali di creare sempre più dipendenze, ricorrendo sempre meno all'intervento umano.

1. Ethan Zuckerman (14 agosto 2014), "The internet's original sin", *Atlantic*, www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041.
2. Richard H. Driehaus Museum (14 marzo 2017), "Jules Chéret and the history of the artistic poster", http://driehausmuseum.org/blog/view/jules-cheret-and-the-history-of-the-artistic-poster.

CAPITOLO 45

La persuasione

Nel 2014, su Tinder c'erano bot che fingevano di essere ragazze, scambiavano due chiacchiere con gli utenti, raccontavano di stare giocando a Castle Clash e mettevano il link per scaricarlo. Non un granché come hack cognitivo. Cercava di sfruttare una serie di emozioni maschili, come la fiducia e il desiderio sessuale, ma per chi non era del tutto ingenuo era evidente che la nuova "amica" fosse un bot. Non sappiamo quanti utenti questi account falsi abbiano convinto a scaricare il gioco, prima di essere rimossi da Tinder.

Uno scam del genere non è certo una rarità. I chatbot da tempo vengono usati per manipolare le emozioni umane e convincere le persone a fare qualcosa per scopi commerciali o politici. Nel 2006, l'esercito degli Stati Uniti usava Sgt Star, un chatbot progettato per convincere le persone ad arruolarsi. Grazie alle AI e alla robotica, oggi questi espedienti sono molto più efficaci.

Negli anni Settanta, la Federal Trade Commission chiese ad alcuni dirigenti del settore pubblicitario di spiegarle il funzionamento del marketing. Era praticamente a digiuno dell'argomento, e sapeva solo che la pubblicità serviva a far conoscere i prodotti delle aziende ai potenziali consumatori. Naturalmente la pubblicità è molto di più e le sue tecniche servono soprattutto ad hackerare i sistemi cognitivi.

La persuasione non è una cosa semplice. Le persone fanno resistenza,[1] non vogliono mutare opinioni e comportamenti, sia per paura delle manipolazioni sia per semplice paura del cambiamento. Ma per quanto possiamo opporci, in modo consapevole o inconsapevole, ci sono un'infinità di trucchetti per cambiare la mente di una persona. Molti sono subdolamente semplici, come l'effetto di "verità illusoria": tendiamo a credere alle cose che sentiamo ripetutamente (esatto, la tecnica della Grande Bugia funziona: se ripeti una bugia tante volte chi ti ascolta comincerà a crederci). Anche le persone più brillanti e analitiche rischiano di soccombere

alle verità illusorie proprio come tutte le altre. A dire il vero, è proprio la ripetizione di mezze verità e bugie da parte delle élite e dei media a perpetuare le false convinzioni. È comunque evidente che semplici trucchi come la ripetizione possano sfuggirci, e persuaderci più di quanto ci aspetteremmo.

Pensiamo all'esempio del *drip pricing*, il prezzo-civetta. Compagnie aeree e catene di hotel usano spesso questo espediente, visto che quando si tratta di servizi del genere i clienti pensano innanzitutto al prezzo. Il trucco sta nell'ostentare un prezzo basso per poi farlo lievitare con tariffe aggiuntive, sperando che l'acquirente non se ne accorga. Uno studio dedicato a StubHub, un marketplace online per comprare i biglietti, ha riscontrato che grazie al drip pricing le persone spendono il 21% in più di quanto spenderebbero altrimenti.[2]

Ci sono venditori che usano altri prezzi-esca. Se ci troviamo a scegliere tra due prodotti, uno più economico e uno più costoso, e li valutiamo per quel che valgono, potremmo preferire il più economico perché l'altro non giustifica la spesa maggiore. Per questo spesso il venditore ci propone anche un terzo prodotto, ancor più costoso e di lusso, spingendoci a preferire l'opzione intermedia.

Online, la persuasione va spesso di pari passo con i cosiddetti *dark pattern*. Il design delle interfacce si serve in genere di regole e metafore che ci consentono di comprendere cosa accade nei computer a nostra insaputa: cartelle, file, directory, sono tutte astrazioni e rappresentazioni di qualche tipo. Non sono però sempre accurate. Quando spostiamo un file in una cartella, non spostiamo niente materialmente, solo cambiando il puntatore che indica dove il file è archiviato. Cancellare un file non equivale alla distruzione fisica di un oggetto: lo scoprono amaramente gli avvocati, quando un file che credevano distrutto viene usato contro un loro cliente. In genere però queste rappresentazioni simboliche sono utili e, per quanto possibile, si ricorre a regole che ricalcano quelle del mondo reale.

Con l'espressione "dark pattern" si fa riferimento a trucchi usati in modo sovversivo nella progettazione delle interfacce, che sfruttano grafiche molto diffuse per spingere gli utenti a determinati comportamenti. In genere le grafiche standardizzate ci guidano nelle

nostre interazioni online; ci fidiamo del loro linguaggio visivo. Quando compiamo un'azione basata sull'abitudine come guidare, ad esempio, ci fermiamo al rosso e non ci fermiamo se il semaforo è verde. Gli stessi colori vengono costantemente usati nella progettazione delle *user experience*. Diventano però un dark pattern quando una serie di pulsanti verdi "Continua" portano a un acquisto all'interno di una app, come nel caso del gioco per smartphone "Two Dots", oppure quando la pubblicità di un altro software con la scritta "Clicca qui per il download" interrompe una serie di pulsanti "Continua" durante la navigazione di un sito. Ci accade fin troppo spesso di cliccare e non ottenere il risultato voluto: dobbiamo stare sempre attenti.

Intuit ha creato un programma gratuito per compilare la propria dichiarazione dei redditi chiamato Free File, ma l'ha reso volutamente difficile da trovare; l'azienda cerca invece di spingere i suoi utenti a pagare per fare la stessa cosa col suo prodotto TurboTax (nel 2022, alcuni Stati hanno condannato Intuit a pagare 141 milioni di dollari di rimborsi; staremo a vedere se in futuro l'azienda si comporterà in modo diverso). Chatmost ha creato un banner pubblicitario con sopra una finta macchia di sporco, spingendo con l'inganno gli utenti a cliccarci sopra mentre cercano di pulire lo smartphone.

Nel 2019, i senatori americani Mark Warner e Deb Fischer hanno presentato un disegno di legge per vietare i dark pattern. Non è stato approvato. Nel caso venga riproposto in futuro, sarà importante scegliere bene la formulazione della legge. Programmatori e app, per aggirare le regole, proveranno infatti per prima cosa proprio a hackerare la definizione stessa di dark pattern.

1. Marieke L. Fransen, Edith G. Smit e Peeter W.J. Verlegh (14 agosto 2015), "Strategies and motives for resistance to persuasion: an integrative framework", *Frontiers in Psychology* 6, article 1201, www.ncbi.nlm.nih.gov/pmc/articles/PMC4536373.
2. Morgan Foy (9 febbraio 2021), "Buyer beware: Massive experiment shows why ticket sellers hit you with last-second fees", Haas School of Business, University of California, Berkeley, https://newsroom.haas.berkeley.edu/research/buyer-beware-massive-experiment-shows-why-ticket-sellers-hit-you-with-hidden-fees-drip-pricing.

CAPITOLO 46

Fiducia e autorità

Il 19 marzo 2016, John Podesta, all'epoca a capo della campagna presidenziale della senatrice Hillary Clinton, ricevette una email apparentemente inviatagli da Google. Era un avviso di sicurezza, che rimandava a una pagina di log-in, anch'essa simile a quelle reali. Podesta inserì i suoi dati, ma la pagina in realtà era gestita dalla Gru, l'agenzia russa di intelligence militare. Gli agenti della Gru ottennero così la password Gmail di Podesta e si impossessarono di 20mila sue vecchie email, che poi inoltrarono a WikiLeaks per farle pubblicare. Si trattò di un caso di hack basato sul *social engineering*, una strategia molto comune per hackerare i sistemi informatici. Perché possa venire attuata, questa strategia richiede che una persona dotata di accesso specializzato a un sistema lo usi come non avrebbe dovuto. Più di vent'anni fa, ho scritto: "Solo i principianti attaccano le macchine; i professionisti prendono di mira le persone".[1] Questo motto vale anche oggi, e alla base di tutto c'è l'hacking della fiducia.

Vi propongo un altro esempio di attacco basato sul social engineering: si chiama il servizio di assistenza tecnica di una linea telefonica, ci si spaccia per qualcun altro e si cerca di convincere l'operatore a trasferire il numero di cellulare di quella persona a un telefono che controlliamo noi. È una tecnica nota come *Sim swapping*, particolarmente perniciosa in quanto il controllo di un numero telefonico consente frodi di ogni tipo e spesso causa alle vittime danni per migliaia di dollari. Una vittima di questa truffa una volta ha perso 24 milioni di dollari:[2] le perdite complessive sono enormi.

Il social engineering può assumere forme innumerevoli. Può basarsi su una telefonata al nostro datore di lavoro – è così che nel 2020 gli hacker di Twitter sono entrati nella rete dell'azienda[3] impadronendosi di più di centotrenta account – o su una email. Si parla di *phishing* quando qualcuno manda una falsa email cercando

di spingere qualcuno a cliccare su un link, ad aprire un allegato o a fare qualcosa che comporti rischi per il suo computer o il suo conto in banca. Non è una strategia molto efficace: chi la attua pesca "a strascico" sperando che qualcuno ci caschi e nel testo della email si tiene volutamente sul vago. Se le email sono personalizzate, si parla invece di *spear phishing*, pesca "con la fiocina". Bisogna effettuare ricerche approfondite per confezionare un messaggio persuasivo, ma il risultato può essere un hacking molto efficace. Podesta ci è cascato, proprio come l'ex segretario di stato Colin Powell.

Nel capitolo 12, ho parlato del compromesso necessario nella gestione delle email di lavoro. Un hacker accede alla email di un dirigente di un'azienda e scrive a un suo sottoposto: "Ciao, sono il Ceo. Potrà sembrarti anomalo, ma sono in viaggio e non posso accedere alla rete come al solito. Mi servirebbe che tu trasferissi immediatamente 20 milioni di dollari a questo conto estero. È molto importante, ne va di un grosso affare. Quando torno in hotel poi ti mando i moduli". A seconda di quanto l'hacker è bravo a inserire dettagli plausibili, di quanto l'impiegato è distratto o di quanto si fida, e di quanto lo scenario complessivo descritto nella email è coerente, c'è la possibilità che una truffa del genere vada in porto. Per colpa di questo scam, nel 2019 Toyota ha perso 37 milioni di dollari, e si tratta solo di una delle molte vittime, grandi e piccole.

Nel 2015, alcuni agenti siriani si sono spacciati per belle donne su Skype, e hanno rubato piani di battaglia a un gruppo di ribelli particolarmente ingenui, risalendo anche alle identità e ai dettagli personali dei loro capi. Gli agenti russi hanno usato la stessa tattica per mettere le mani su informazioni segrete appartenenti a membri del servizio statunitense.

Con la tecnologia, fare imbrogli del genere è sempre più semplice. Oggi i criminali possono usare i deep-fake per i loro attacchi di social engineering. Nel 2019, il Ceo di un'azienda britannica del settore energetico[4] è caduto in un trabocchetto: ha versato 220.000 euro in un conto bancario, pensando che – prima al telefono e poi via email – glielo stesse ordinando il Ceo dell'azienda madre. Questo hack era basato su un fake audio, ma presto sarà possibile farlo anche in video. Un mago della truffa si è servito di maschere di silicone per

registrare video e convincere le sue vittime a versargli milioni di dollari.[5]

È possibile usare una truffa del genere anche in ambito geopolitico. I ricercatori hanno creato video deep-fake di politici che dicono e fanno cose che non hanno mai detto o fatto. Nel 2022, il presidente ucraino Volodymyr Zelensky ha dovuto smentire un video in cui ordinava all'esercito del suo Paese di arrendersi agli invasori russi. Era un video di scarsa qualità, evidentemente falso, ma senza dubbio col passare del tempo e coi progressi della tecnologia diventerà più facile realizzare prodotti credibili.

Il semplice fatto che una tecnologia del genere esista basta a farci perdere fiducia nelle registrazioni audio e video. Nel 2019, un video di Ali Bongo, presidente del Gabon, a lungo assente dalla scena pubblica[6] e ritenuto gravemente malato o addirittura già morto, è stato etichettato come un deep-fake dai suoi oppositori e ha innescato un fallimentare colpo di Stato da parte dell'esercito gabonese. In verità il video era reale, ma come poteva sincerarsene una persona non esperta?

Queste tecniche, assieme alle AI che permettono ai bot di creare testi realistici – saggi, messaggi, conversazioni – ci porteranno presto a disporre di tecnologie persuasive in grado di hackerare la nostra percezione di che cosa è umano.

Lo abbiamo già potuto osservare durante la campagna elettorale americana del 2016. BuzzFeed individuò centoquaranta siti di fake news[7] che dal nome del dominio sembravano americani, e che sparavano notizie sensazionaliste molto condivise su Facebook. Era solo l'inizio: questi siti, creati per apparire autorevoli, cominciarono ben presto a moltiplicarsi. Domini come BostonTribune.com, KMT11.com o ABCNews.com.co avevano un'aria ufficiale e molti lettori pensavano che i loro contenuti fossero credibili. Siti quali Tennessee Star, Arizona Monitor e Maine Examiner avevano proprio l'aspetto dei quotidiani più diffusi, ma servivano alla diffusione di propaganda estremista.

Molti capisaldi storici della fiducia sono crollati. Un tempo libri e tv venivano considerati autorevoli, in quanto editoria ed emittenti televisive fungevano da *gatekeeper*, da guardiani. Con l'avvento di

internet non ci si può più fidare tanto ingenuamente. Oggi chiunque può pubblicare qualsiasi tipo di libro. Creare un finto quotidiano cartaceo è più difficile, ma per un sito web è semplice imitare la pagina di uno stimato quotidiano. Le banche avevano le loro sedi in grandi palazzi che davano un'idea di forza e affidabilità; su un sito web è molto più facile riprodurre lo stesso tipo di iconografia.

Qualche altro esempio di hacking della fiducia. I "contenuti sponsorizzati", i cosiddetti "publiredazionali", riprendono forma e funzione della piattaforma che li ospita, pur essendo pubblicità a pagamento (gran parte delle piattaforme però identificano i contenuti sponsorizzati scrivendolo all'inizio dell'articolo). Le recensioni dei clienti, oggi onnipresenti sui siti di e-commerce, possono essere facilmente falsificate. Allo stesso modo, è diventato più semplice presentare false credenziali: pensiamo ai malintenzionati che fingono di essere ufficiali dell'immigrazione per estorcere denaro ai nuovi arrivati in un Paese; a chi si spaccia per medico ostentando lauree senza alcun valore, per vendere finti rimedi online; ai truffatori che si spacciano per agenti del fisco, ottenendo l'accesso ai computer e alle password di qualche ignaro contribuente.

Un'ultima cosa: quando si tratta di fiducia, il nostro sistema cognitivo parte innanzitutto dai singoli individui. Non siamo fatti per valutare l'affidabilità di organizzazioni, brand, aziende ecc. Per questo i grandi marchi si servono di mascotte e testimonial; ormai da decenni i pubblicitari danno ai brand un volto umano per conquistare la nostra fiducia. Da qualche anno, hanno imparato anche a sviluppare una personalità ben definita sui social media. Il profilo Twitter di Wendy, la catena di fast food, ha un approccio sempre piuttosto sarcastico, mentre Amazon reagisce in modo veemente alle critiche del governo. Sono espedienti volti a simulare un rapporto di confidenza con gli utenti, e a ottenere la loro fiducia come gli influencer e i politici. Aziende e movimenti politici si servono sempre più della AI per ottimizzare la propria presenza sui media e ricorrono a falsi account per dare l'impressione di avere un grande seguito; di conseguenza anche i più scettici e cinici presto potrebbero cadere nella trappola e accorgersi che la loro fiducia è

stata hackerata.

1. Bruce Schneier (15 ottobre 2000), “Semantic attacks: The third wave of network attacks”, *Crypto-Gram*, www.schneier.com/crypto-gram/archives/2000/1015.html#1.
2. Joeri Cant (22 ottobre 2019), “Victim of $24 million SIM swap case writes open letter to FCC chairman”, *Cointelegraph*, https://cointelegraph.com/news/victim-of-24-million-sim-swap-case-writes-open-letter-to-fcc-chairman.
3. Twitter (18 luglio 2020; ultimo aggiornamento 30 luglio 2020), “An update on our security incident”, Twitter blog, https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.
4. Nick Statt (5 settembre 2019), “Thieves are now using AI deepfakes to trick companies into sending them money”, *Verge*, www.theverge.com/2019/9/5/20851248/deepfakes-ai-fake-audio-phone-calls-thieves-trick-companies-stealing-money.
5. Hugh Schofield (20 giugno 2019), “The fake French minister in a silicone mask who stole millions”, *BBC News*, www.bbc.com/news/world-europe-48510027.
6. Drew Harwell (12 giugno 2019), “Top AI researchers race to detect ‘deepfake’ videos: ‘We are outgunned’”, *Washington Post*, www.washingtonpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned.
7. Craig Silverman e Lawrence Alexander (3 novembre 2016), “How teens in the Balkans are duping Trump supporters with fake news”, *BuzzFeed*, www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.

CAPITOLO 47

Rischio e paura

Il nostro senso della paura è innato; si è evoluto nel corso dei millenni, con i nostri antenati che imparavano a sfuggire all'appetito dei predatori e – più di recente – ad altri umani che volevano farci del male per motivi loro. Come abbiamo appena visto parlando dell'attenzione, il sistema della paura si serve di scorciatoie cognitive ed è ottimizzato per il mondo di tanti anni fa, quando ci stavamo ancora evolvendo. Si tratta di funzioni fondamentali del cervello, controllate in prevalenza dall'amigdala.[1] Il nostro cervello non se la cava molto bene con l'analisi di rischi e probabilità. Tendiamo a dare troppa importanza a eventi strani, rari, spettacolari, sottovalutando quelli comuni, familiari, ordinari. Pensiamo che certi pericoli molto rari siano invece dietro l'angolo. Li temiamo più di quanto ci consiglierebbero le probabilità.

Molti psicologi hanno cercato di spiegarne il motivo, e hanno riscontrato che tendiamo a reagire ai pericoli più in base alle storie che ai dati. Le storie ci coinvolgono a livello viscerale, specialmente quando sono appassionanti, realistiche, oppure quando ci coinvolgono personalmente. Se dobbiamo andare in un Paese lontano, un amico che ci racconta di essere stato rapinato ci influenzerà molto più di una statistica sul tasso di criminalità. Sommiamo paura, curiosità e una buona storia e otterremo una reazione esagerata.

Lo possiamo vedere ovunque. Abbiamo paura che uno sconosciuto ci uccida, ci rapisca, ci violenti, ci aggredisca, mentre in realtà questi crimini vengono compiuti soprattutto da parenti o amici. Temiamo i disastri aerei e i pazzi che cominciano a sparare alle persone, ma non ci preoccupiamo degli incidenti d'auto e della violenza domestica, cose molto più diffuse e mortali. Inizialmente non sapevamo come reagire ai rischi del Covid-19, piccoli per l'individuo ma enormi per la collettività, rischi estremamente dipendenti da piccoli cambiamenti

delle condizioni sociali e in mutamento costante.

Il terrorismo cerca proprio di hackerare queste scorciatoie cognitive.[2] I fatti ci dicono che, dal punto di vista statistico, è un rischio di scarsa entità. Negli attacchi dell'11 settembre sono morte circa tremila persone e nei due decenni successivi le vittime di attacchi terroristici negli Stati Uniti sono state trecento. Ogni anno negli Usa muoiono invece 38mila persone in incidenti automobilistici; nello stesso arco di tempo si arriva pertanto a circa 750mila morti. E più di un milione di persone negli Usa sono morte a causa del Covid-19. Il terrorismo nasce proprio per andare oltre ogni logica. È terrificante, impressionante, appariscente, casuale e feroce, caratteristiche che ci spingono a esagerarne i rischi e a reagire in modo inconsulto. La paura prende il sopravvento e accettiamo un trade-off sicurezza/restrizioni che altrimenti non avremmo nemmeno preso in considerazione. Ansie e istinti sociali vengono hackerati collettivamente.

Anche i politici hackerano la paura. Un politico che fonda la sua campagna sulla sicurezza e che promette di sconfiggere la minaccia del momento probabilmente troverà molti elettori disposti a seguirlo. Ascoltando i leader di partito, la gente comune è ben disposta a dare il benvenuto a una nuova paura, anche se non la coinvolge direttamente. Ci sono elettori del New Hampshire del nord terrorizzati dagli immigrati provenienti dal confine meridionale degli Stati Uniti, pur non avendo mai conosciuto una singola persona originaria del Centro America. Come disse Bill Clinton: "Chi non si sente al sicuro preferisce votare una persona forte che sbaglia invece di una persona debole che ha ragione".[3]

Il tribalismo è un sistema di identità di gruppo. Per nostra natura, formiamo gruppi ed escludiamo chi ne resta fuori. La vulnerabilità risiede nel fatto che la minima provocazione ci induce a creare nuovi gruppi, anche quando non avrebbe senso. Quando da ragazzino andavo in colonia, gli organizzatori decisero di farci fare la "guerra dei colori". Per una settimana, l'intero campeggio veniva diviso in gruppo rosso e gruppo oro. Non mangiavamo più tutti assieme, e anche i giochi erano separati. Gli effetti furono immediati. Noi eravamo i buoni, e gli altri erano il nemico. Naturalmente non

ricordo neanche più quale fosse il mio colore, ma ricordo con chiarezza la distanza che si era creata coi miei vecchi amici.

Ci sono tre modi fondamentali di sfruttare la nostra vulnerabilità al tribalismo. Il primo è quello di rafforzare l'identità del gruppo e le divisioni tra gruppi. L'ha messo in atto l'Agenzia di ricerca su internet russa nei mesi prima delle elezioni del 2016, con tattiche varie, dalle donazioni alle organizzazioni più estremiste ai post sui forum online pensati appositamente per far litigare la gente. La tecnica è "andare a caccia di spaccature": trovare i punti di distacco e renderli vere e proprie divisioni.

Il secondo modo è la creazione deliberata di gruppi tribali. Nel Diciannovesimo e Ventesimo secolo, i governi coloniali sono ricorsi spesso a questa tattica. In Ruanda, tedeschi e belgi al governo della regione trasformarono le differenze economiche tra Hutu (contadini) e Tutsi (pastori) in un conflitto di classe e di etnia, che decenni dopo avrebbe portato al genocidio. Le aziende oggi usano strategie simili – seppur con minore intensità – per venderci di tutto, dalle auto alle scarpe da ginnastica.

Il terzo è creare condizioni che consentano al tribalismo di svilupparsi naturalmente. Ad esempio prendere gruppi di persone affini e dare al loro legame una natura tribale. Accade nello sport, ma anche in politica è sempre più frequente.

Fox News di certo conosce le ricerche che dimostrano come da un senso di minaccia scaturiscano maggiore sostegno a chi è all'interno del gruppo e maggior paura di chi è all'esterno. Quando Fox diffonde notizie come "gli immigrati vi stanno rubando il lavoro",[4] "questa città è in mano alla criminalità",[5] "l'Isis minaccia gli americani"[6] o "i democratici vi toglieranno le armi",[7] non cerca solo di portare avanti determinati temi, ma cerca anche di polarizzare le opinioni degli spettatori.

Data analytics e automazione sono sempre più abili a hackerare il senso d'identità delle persone. Il tribalismo è a tal punto potente e polarizzante che hackerarlo – soprattutto con la velocità e la precisione consentite dai computer – può avere effetti sociali dirompenti, che si tratti di un esplicito obiettivo di hacking sociale informatico (come nel caso dei russi) o che sia l'effetto collaterale di

una AI che non si cura delle conseguenze delle proprie azioni (come gli algoritmi che regolano le pagine consigliate sui social media).

1. Bruce Schneier (3 aprile 2000), “The difference between feeling and reality in security”, *Wired*, www.wired.com/2008/04/securitymatters-0403.
2. Bruce Schneier (17 maggio 2007), “Virginia Tech lesson: Rare risks breed irrational responses”, *Wired*, www.wired.com/2007/05/securitymatters-0517.
3. Nate Silver (1 febbraio 2010), “Better to be strong and wrong – especially when you’re actually right”, *FiveThirtyEight*, https://fivethirtyeight.com/features/better-to-be-strong-and-wrong.
4. *Fox News* (26 gennaio 2017), “The truth about jobs in America”, The O’Reilly Factor (transcript), www.foxnews.com/transcript/the-truth-about-jobs-in-america.
5. Audrey Conklin (21 febbraio 2022), “Homicides, rapes in Atlanta soar despite other decreasing violent crime”, *Fox News*, www.foxnews.com/us/homicides-rapes-atlanta-soar-2022.
6. Ronn Blitzer (26 ottobre 2021), “Top Pentagon official confirms ISIS-K could have capability to attack US in ‘6 to 12 months’”, *Fox News*, www.foxnews.com/politics/pentagon-official-isis-k-us-attack-6-to-12-months.
7. Tucker Carlson (9 aprile 2021), “Biden wants to take your guns, but leave criminals with theirs”, *Fox News*, www.foxnews.com/opinion/tucker-carlson-biden-gun-control-disarm-trump-voters.

CAPITOLO 48

Difendersi dagli hack cognitivi

La community dei *pick-up artist* è un movimento di uomini che elaborano e condividono tecniche manipolative per sedurre le donne. È più antica di internet, ma grazie alla rete è riuscita a rafforzarsi e diffondersi. Molte delle tecniche che propone ricordano gli hack cognitivi, come ad esempio il *negging*, un complimento ambiguo finalizzato a minare la sicurezza di chi lo riceve e a farle ricercare l'approvazione del manipolatore. Che schifezza. Non so se il negging o gli altri loro hack funzionino davvero. Gli uomini che ne discutono online raccontano un mare di aneddoti per vantarsi, ma è difficile distinguere tra bugie e metodi scientifici da quattro soldi. Leggendo invece quel che raccontano le donne oggetto di questi tentati hack, una cosa è chiara: il miglior modo di difendersi è essere preparati in anticipo. Se conosci la tecnica del negging la sai riconoscere.

La conoscenza preventiva accelera la regressione verso la media. Molti hack cognitivi infatti funzionano meglio all'inizio e peggio una volta che le persone imparano come fronteggiarli. Alla loro prima apparizione, nel 1994, i banner pubblicitari avevano un tasso di *click-through* del 49%, sceso oggi a meno dell'1%. Anche le pubblicità pop-up hanno seguito lo stesso declino, una volta diventate tanto onnipresenti quanto insopportabili. Probabilmente anche microtargeting, drip pricing, falsi account Facebook e tutte le altre cose delle quali ho parlato negli ultimi capitoli andranno incontro alla stessa sorte. Queste tattiche perdono di efficacia non appena ci diventano familiari.

La conoscenza preventiva ha però dei limiti.[1] Ci sono molti hack cognitivi che funzionano perfino quando sappiamo che ci stanno manipolando. Quando riesci a manipolare una persona fino a convincerla di qualcosa, tenderà a restare salda in quelle convinzioni anche di fronte alla prova che si sta sbagliando. In concreto, per hackerare la disponibilità dell'utente a separarsi dal proprio denaro

le aziende spesso offrono periodi di prova gratuiti, seguiti da abbonamenti mensili a pagamento. Puntano sul fatto che gli esseri umani si fidano troppo della propria memoria e della propria capacità di gestire il tempo, sapendo che anche chi è consapevole di perdere la cognizione del tempo, spesso continua comunque a pagare servizi che si era ripromesso di cancellare.

Un altro modo per difendersi è dichiarare illegali determinate pratiche manipolatorie. Ad esempio, l'Australia ha stabilito che il prezzo complessivo deve essere sempre comunicato, per prevenire il drip pricing. La Federal Trade Commission richiede che le caratteristiche di un prodotto esaltate da una pubblicità abbiano una "giustificazione ragionevole". È inoltre possibile rendere certi hack meno efficaci, e pertanto meno pericolosi, togliendo loro la possibilità di operare il microtargeting, prendendo di mira alcuni individui in particolare. Una pubblicità elettorale che si deve rivolgere a tutti non potrà infatti sfruttare molti hack cognitivi per i suoi loschi scopi.

Inevitabilmente, anche le nuove regole vengono hackerate. Per quanto supervisione e trasparenza siano necessarie per combattere gli hack ingannevoli, non bastano. A complicare il tutto, c'è il fatto che è difficile spiegare cosa ci sia di "sbagliato" in questi hack, che causano danni astratti, a lungo termine o difficili da comprovare.

Gli hack cognitivi puntano sugli aspetti più profondi e pervasivi della mente umana, dall'istinto di sopravvivenza alla volontà di affermare il nostro status sociale. Possono essere usati contro chiunque. Per proteggerci dagli hack cognitivi, ci serve una difesa a tutto campo a livello sociale: dall'educazione alle leggi fino alle soluzioni tecnologiche, soprattutto online. Le tecnologie digitali sono sempre più al centro della nostra attenzione e l'hacking cognitivo si impone grazie alle macchine. I programmi informatici non sono più solo strumenti nelle mani di hacker umani, ma divengono a loro volta hacker autonomi e potentissimi. Diviene pertanto fondamentale comprendere come i nostri prodotti digitali siano in grado di hackerarci se vogliamo difenderci dalla manipolazione.

1. Leah Savion (gennaio 2009), “Clinging to discredited beliefs: The larger cognitive story”, *Journal of the Scholarship of Teaching and Learning* 9, n. 1, https://files.eric.ed.gov/fulltext/EJ854880.pdf.

CAPITOLO 49

Una gerarchia dell'hacking

Nessun sistema esiste in completo isolamento. Fa sempre parte di una gerarchia. Facciamo un esempio: una persona vuole rubare del denaro tramite una transazione bancaria online. Può dunque hackerare il sito della banca. Oppure può hackerare il browser del cliente della banca. O ancora può hackerare il sistema operativo o l'hardware del cliente. Sono tutti hack che possono portare allo stesso risultato, soldi gratis, e hanno lo stesso obiettivo, il furto. Un altro esempio: una persona vuole pagare meno tasse. Come ormai sappiamo, può hackerare la normativa fiscale e scovare nuovi loophole. Se ha soldi e potere a disposizione, può però salire di livello e hackerare il processo legislativo usato per creare la normativa fiscale. Può addirittura salire ancora di livello per hackerare il processo di applicazione della legislazione in generale o quello di riscossione, facendo in modo che le autorità fiscali non abbiano abbastanza personale per fare i controlli (l'hacking del processo di attuazione è un altro modo per sovvertire l'intento di un sistema). Può salire perfino di tre livelli e hackerare il processo politico usato per eleggere i legislatori. Può salire di quattro livelli e hackerare l'ecosistema mediatico usato per discutere del processo politico. Può salire di cinque livelli e hackerare i processi cognitivi innescati dall'ecosistema mediatico nel dibattito politico per eleggere i legislatori che creano il sistema fiscale che apre o chiude i loophole. Oppure può perfino *scendere* di un livello per cercare vulnerabilità ed exploit nel modulo per la dichiarazione dei redditi.

Sto cercando di spiegare che ogni sistema si situa in una gerarchia di ampiezza crescente, nel quale il sistema superiore governa il sistema sottostante, e che gli hack possono prendere di mira ogni livello. L'hacking sfrutta una gerarchia di sistemi in interrelazione reciproca. Potrà esserci un sistema difficile da scalfire o manipolare, ma in quel caso si potrà puntare ai sistemi superiori che lo governano

o a quelli inferiori che ne implementano le regole.

Nel contesto tecnologico, il passaggio da un livello all'altro è più difficile. Il fatto che ci siano vulnerabilità in Microsoft Windows non significa che sia possibile hackerare il processo di assunzione della Microsoft Corporation per rendere il sistema operativo ancor più vulnerabile. Nei sistemi sociali, il passaggio è invece più semplice, soprattutto per chi è ricco e influente. Per Jeff Bezos non è stato un problema comprare la casa più grande di Washington per ricevere i deputati e cercare di influenzarli.[1] O comprare il *Washington Post*, uno dei giornali più rispettati degli Stati Uniti. Può anche pagare tutti i programmatori che vuole perché progettino qualsiasi software lui voglia.

Ci sono hack che funzionano simultaneamente a più livelli. Nel 2020 abbiamo visto il caso di Ghostwriter, un collettivo[2] – probabilmente di origine russa – in grado di violare il sistema di content management di molti siti di notizie di Paesi dell'Europa dell'Est, con lo scopo di postare articoli fake. In questo caso un classico hack informatico via internet è andato di pari passo con un hack della fiducia che sfruttava la reputazione di quei siti.

È più facile mettere una patch a un livello basso che a uno più alto. Una vulnerabilità della TurboTax può essere riparata in pochi giorni, mentre possono volerci anni per riparare una vulnerabilità dell'intero sistema fiscale. Le vulnerabilità cognitive possono durare per generazioni (per quanto le tattiche per sfruttarle debbano cambiare strada facendo).

Per questo gli hack cognitivi sono i più pericolosi. Governano tutte le nostre azioni, individuali e collettive, e pertanto tutti i nostri sistemi sociali. Chi può hackerare la mente umana, può impiegare le sue tecniche su elettori, impiegati, imprenditori, amministratori, politici e anche sugli altri hacker, spingendoli a cambiare i loro sistemi a suo piacimento.

I pericoli dell'hacking cognitivo sono sempre più diffusi. Le menti umane non sono i soli sistemi cognitivi dei quali dobbiamo preoccuparci. Oggi servizi pubblici, transazioni d'affari e perfino le fondamentali interazioni sociali vengono mediati da sistemi digitali che fanno previsioni e prendono decisioni, proprio come gli esseri

umani, ma lo fanno in modo più veloce e sistematico, e senza averne la piena responsabilità. Le macchine decidono per noi con sempre maggior frequenza, ma il loro modo di pensare è diverso dal nostro. L'interazione delle nostre menti con queste intelligenze artificiali è il futuro dell'hacking, un futuro emozionante e pericoloso, che si tratti di economia, di diritto o di qualunque altra cosa.

1. Sam Dangremond (4 aprile 2019), "Jeff Bezos is renovating the biggest house in Washington, D.C.", *Town and Country*, www.townandcountrymag.com/leisure/real-estate/news/a9234/jeff-bezos-house-washington-dc.
2. Lee Foster *et al.* (28 luglio 2020), "'Ghostwriter' influence campaign: Unknown actors leverage website compromises and fabricated content to push narratives aligned with Russian security interests", *Mandiant*, www.fireeye.com/blog/threat-research/2020/07/ghostwriter-influence-campaign.html.

PARTE SETTIMA
L’HACKING DEI SISTEMI DI AI

CAPITOLO 50

Intelligenza artificiale e robotica

L'intelligenza artificiale (AI) è una tecnologia dell'informazione. Si basa su software, si serve dei computer ed è già parte integrante del nostro tessuto sociale, in modi dei quali siamo più o meno consapevoli. Hackererà la nostra società come non mai.

Lo farà da due punti di vista molto diversi. Uno: i sistemi AI verranno usati per hackerarci. Due: i sistemi AI a loro volta diventeranno hacker. Troveranno le vulnerabilità dei sistemi sociali, economici e politici e le sfrutteranno con velocità e abilità senza precedenti, con effetti di portata inaudita. La differenza non starà nelle dimensioni, ma nel tipo di hacking. Rischiamo che in futuro i sistemi AI hackerino altri sistemi AI, e che gli umani diventino solo possibili vittime collaterali delle loro azioni.

Potrà sembrarvi un'esagerazione, ma quello di cui parlo non richiede alcuna tecnologia fantascientifica. Non sto postulando alcuna "singolarità" nella quale il loop di apprendimento della AI diviene tanto veloce da superare la comprensione umana. Perché si verifichino gli scenari che prospetto non serve nessun genio del male. Non sto parlando di androidi intelligenti come Data di Star Trek, R2-D2 di Star Wars o Marvin della Guida galattica per autostoppisti. Non ci sarà bisogno di sistemi AI malvagi come Skynet di Terminator, Ultron degli Avengers o degli agenti del mondo di Matrix. Per alcuni degli hack che descriverò non serviranno nemmeno particolari passi avanti della ricerca. Saranno più semplici da effettuare man mano che le tecniche AI diventeranno più sofisticate, ma già oggi possiamo vederli in azione. Si tratta di hack ai quali arriveremo naturalmente, quando le AI saranno più abili ad apprendere, capire e risolvere i problemi.

Definizione: AI /ā-ī/ (sostantivo):
1. (abbrev.) Artificial Intelligence, Intelligenza artificiale.

2. Un computer in grado (in senso lato) di percepire, pensare e agire.
3. Termine ombrello che copre una vasta gamma di tecnologie per il decision-making in grado di simulare il pensiero umano.

Questa non è una definizione canonica, ma definire che cos'è la AI non è semplice. Nel 1968, lo scienziato informatico Marvin Minsky descrisse la AI come "la scienza per far fare alle macchine cose che se fatte dagli esseri umani richiederebbero l'uso dell'intelligenza".[1] Patrick Winston, un altro pioniere della AI, l'ha invece definita come una forma di "computazione che rende possibile percepire, ragionare e agire".[2] La versione del 1950 del test di Turing, il cosiddetto imitation game, era incentrata su un ipotetico programma informatico che gli umani non avrebbero saputo distinguere da un essere umano. Devo sottolineare la differenza tra la AI specializzata, detta anche narrow, "ristretta", e la AI generale. Quest'ultima è quella che vediamo nei film, una AI in grado di percepire, pensare e agire in modo generico e molto umano. Nel caso sia più intelligente degli esseri umani, viene chiamata "superintelligenza artificiale". Associata alla robotica ci dà l'androide, dall'aspetto più o meno simile a quello di un essere umano. I robot che nei film cercano di distruggere l'umanità rientrano tutti più o meno nella AI generale.

Sono state effettuate molte ricerche sulla realizzazione pratica della AI generale, oltre alle ricerche teoriche su come progettare questi sistemi in modo che non facciano quello che non vogliamo, come distruggere l'umanità. Sono studi affascinanti, che spaziano dall'informatica alla sociologia e alla filosofia, ma probabilmente solo tra qualche decennio troveranno un'applicazione pratica.[3] Voglio invece soffermarmi sulla AI specializzata, quella che sta venendo sviluppata proprio ora.

L'AI specializzata viene progettata per un compito specifico, come controllare un'automobile a guida autonoma. Sa come sterzare, come seguire il codice stradale, come evitare gli incidenti e come comportarsi in caso di eventi inattesi, quale l'irrompere sulla strada di un pallone tirato da un bambino. Le AI specializzate dispongono di molte conoscenze basandosi sulle quali possono prendere decisioni, ma solo nel loro ambito limitato di competenza.

I ricercatori AI dicono scherzando che quando qualcosa funziona smette di essere una AI, ma diviene semplicemente software. Non è certo uno scenario allegro per i ricercatori AI, visto che presuppone che i soli progressi che contano sono i fallimenti. In questa battuta c'è però un seme di verità. AI è un termine fuorviante che vien dalla fantascienza: una volta divenuto realtà, smette di essere fuorviante. Un tempo presumevamo che per leggere una radiografia servisse un tecnico – un essere umano con la giusta formazione e le necessarie credenziali professionali – ma abbiamo imparato che le sue mansioni possono essere svolte anche da un computer.

Dobbiamo tenere ben presente una cosa: i sistemi per il decision-making si posizionano su un continuum, che spazia dal semplice termostato elettromeccanico, in grado di regolare il funzionamento di un sistema di riscaldamento in base alla temperatura, fino a un androide da fantascienza. Quel che può essere definito AI spesso dipende dalla complessità dei compiti svolti e dall'ambiente in cui questo avviene. Il termostato svolge un compito semplicissimo che deve tenere conto di un singolo aspetto dell'ambiente circostante. Non ha nemmeno bisogno di un computer. Un moderno termostato digitale potrebbe percepire se qualcuno è entrato nella stanza e presumere quanto calore sarà necessario in base alle previsioni meteo, oppure tenere conto del consumo cittadino e dei costi al secondo. Un termostato AI del futuro magari potrà perfino comportarsi come un premuroso maggiordomo, qualunque valore potremo dare a questa espressione nel contesto della regolazione della temperatura.

Meglio non preoccuparci troppo delle definizioni, non è quel che ci interessa in questo contesto. Oltre al decision-making, le caratteristiche rilevanti dei sistemi AI sulle quali mi soffermerò sono l'autonomia (la capacità di agire in modo indipendente), l'automazione (la capacità di agire in base a risposte prestabilite a trigger specifici), e l'agency fisica (la capacità di alterare l'ambiente fisico circostante). Un termostato non ha autonomia, e la sua automazione e agency fisica sono limitate. Un sistema che prevede la possibile recidiva di un condannato non ha alcuna agency fisica, ma si limita a dare consigli a un giudice. Un'automobile a guida

autonoma ha un po' di tutte e tre le cose. Anche R2-D2, anche se per qualche motivo i suoi progettisti hanno evitato di farlo parlare in modo intellegibile.

> Definizione: Robot /'rō-'bät/ (sostantivo):
> 1. Oggetti fisici in grado di percepire, pensare e agire all'interno del proprio ambiente tramite movimenti fisici.[4]

Nella cultura popolare troviamo un'infinità di miti sulla robotica, ma la realtà è molto meno scintillante. Come nel caso della AI, il termine si presta a molte definizioni. Nei film e in tv, la robotica comprende un ampio spettro di abilità fisiche e intellettive. Anche in questo caso, preferisco concentrarmi sulle tecnologie più vicine e concrete. Per quel che ci interessa, la robotica è caratterizzata da autonomia, automazione e agency fisica di alto livello, ovvero "autonomia cyber-fisica", tecnologia AI all'interno di oggetti in grado di interagire col mondo in modo materiale e diretto.

1. Marvin Minsky (1968), “Preface”, in *Semantic Information Processing*, MIT Press.
2. Patrick Winston (1984), *Artificial Intelligence*, Addison-Wesley.
3. Il futurologo Martin Ford ha somministrato un questionario a ventitré ricercatori di primo piano del settore AI, chiedendo loro quando la costruzione di una AI generalizzata raggiungerà il 50% di possibilità. Le loro risposte hanno variato tra il 2029 e il 2200, e la risposta media è stata “nel 2099”, un modo indiretto per dire “entro la fine del secolo”. Martin Ford (2018), *Architects of Intelligence: The Truth About AI from the People Building It*, Packt Publishing.
4. Kate Darling (2021), *The New Breed: What Our History with Animals Reveals about Our Future with Robots*, Henry Holt.

CAPITOLO 51

Hackerare le AI

I sistemi AI sono programmi informatici, eseguiti da computer, in genere collegati in grandi reti. Sono pertanto vulnerabili agli stessi tipi di hacking degli altri computer. Esistono però vulnerabilità specifiche dei sistemi AI, in particolare quelle dei sistemi di *machine learning* (ML). Il ML è un sottoinsieme delle AI, con un ruolo preponderante nei sistemi di AI pratici. Nei sistemi ML, i "modelli" vuoti, dopo essere stati alimentati con una quantità enorme di dati, ricevono istruzioni per trovare da soli soluzioni ai problemi. Alcuni attacchi al ML prevedono il furto dei *training data* usati per addestrare il sistema ML, o il furto del modello ML sul quale è basato il sistema. Altri hack cercano invece di configurare il sistema ML per fargli prendere decisioni sbagliate o comunque non buone.

Quest'ultima categoria, nota come *adversarial machine-learning*, è di fatto un insieme di hack. A volte è necessario analizzare a fondo il sistema ML per comprenderne tutte le funzioni e trovare i punti deboli da attaccare. Ad esempio, si può ingannare un sistema ML dandogli una serie di input architettati con grande attenzione. Nel 2017, i ricercatori del Mit hanno progettato una tartaruga giocattolo in modo che una AI per classificare le immagini la ritenesse un fucile. Altri esempi: sono stati applicati adesivi dall'aspetto apparentemente innocuo su un segnale stradale di stop per far credere alla AI che fosse un segnale di limite di velocità, o sono stati messi su una strada adesivi per indurre un'automobile a guida autonoma a tuffarsi nel traffico. Questi sono esempi teorici: i ricercatori sono riusciti a far sbagliare le auto, ma da quanto sappiamo nessuno ha ancora usato l'adversarial ML per spingere un'automobile a guida autonoma a fare un'incidente.

Non è detto che un ML del genere debba avere cattive intenzioni né che possa esistere solo nel contesto limitato di un laboratorio. Progetti simili stanno cercando ad esempio di hackerare i sistemi di

riconoscimento per permettere ai dimostranti di tenere manifestazioni senza paura di venire identificati dalla polizia.

Possiamo immaginare che in futuro le compagnie di assicurazioni si serviranno delle AI per decidere quali polizze autorizzare. Un medico potrebbe allora impiegare un hack per fare in modo che un suo paziente bisognoso di un farmaco o di una cura particolare possa assicurarsi.

Un altro tipo di hack mira a dare a un sistema ML input specifici per cambiare il sistema stesso. Nel 2016 Microsoft provò a utilizzare il chatbot Tay su Twitter. Il suo stile colloquiale era stato modellato sui pattern linguistici di una teenager e si riteneva che sarebbe diventato più articolato attraverso le interazioni con le altre persone, apprendendo il loro modo di conversare. Nel giro di ventiquattr'ore, un gruppo su un forum di 4Chan organizzò una controffensiva. I partecipanti inondarono il sistema di tweet razzisti, misogini e antisemiti, trasformando Tay in una razzista, misogina e antisemita. Tay aveva imparato da loro e, senza capirci niente, aveva ripetuto a pappagallo tutte quelle sconcezze.

I sistemi AI sono programmi informatici, per questo non c'è motivo di credere che saranno immuni agli stessi hack che sfruttano le vulnerabilità degli altri programmi. Le ricerche sul cosiddetto "adversarial ML" sono ancora agli albori, perciò non possiamo sapere se questi attacchi potranno colpire nel segno senza troppe difficoltà o quanto potranno essere efficaci le contromisure. Stando alla storia dell'hacking informatico, nell'immediato futuro dei sistemi AI non mancheranno vulnerabilità che sarà possibile sfruttare. I sistemi AI sono inoltre parte degli stessi sistemi socio-tecnici già visti nel corso del libro, pertanto non mancherà nemmeno chi cercherà di hackerarli per i propri scopi personali.

I risultati sono invece facilmente prevedibili. Incidenti automobilistici. Una tartaruga scambiata per un fucile. Tay che parla come un nazista razzista e misogino. Sono cose che accadranno, e alle quali si spera che potremo porre rimedio tramite patch ai sistemi ML, per farli di nuovo funzionare come vogliamo.

Il continuum degli hack immaginabili va da quelli più evidenti a quelli invisibili. Questi ultimi mi preoccupano di più. Magari le auto

non andranno a sbattere, ma potrebbero fare qualche bizza. Magari i chatbot non diventeranno nazisti in piena regola, ma potrebbero propendere leggermente per un certo partito politico. Gli hacker potrebbero trovare una frase da inserire nelle domande d'ammissione al college per poter essere inseriti in una categoria migliore. Se i risultati sono impercettibili e non conosciamo l'algoritmo, come potremo sapere che stanno avvenendo?

CAPITOLO 52

Il problema della spiegabilità

Nella *Guida galattica per gli autostoppisti*, una razza di esseri iper-intelligenti e pan-dimensionali costruisce il computer più potente dell'universo, Deep Thought (Pensiero profondo), per rispondere alla domanda definitiva sulla vita, l'universo e tutto il resto. Dopo 7,5 milioni di anni di computazione, Deep Thought spiega che la risposta è 42.[1] Non è in grado però di spiegare il perché, né di dire quale sia la domanda.

Questo è in sintesi il problema della spiegabilità. I moderni sistemi di AI sono essenzialmente scatole nere. I dati entrano da una parte e dall'altra esce una risposta. Può essere impossibile capire come il sistema sia arrivato a tale conclusione, anche per il progettista, perfino esaminando il codice. I ricercatori non sanno con precisione come un sistema AI per classificare le immagini riesca a distinguere una tartaruga da un fucile e ancor meno perché possa confonderli. Nel 2016, il programma AI AlphaGo vinse una sfida in cinque partite[2] contro uno dei migliori giocatori di Go del mondo, Lee Sedol, sconvolgendo allo stesso tempo il mondo delle AI e quello dei giocatori di Go. AlphaGo fece la sua mossa più celebre durante la seconda partita: la mossa trentasette. Difficile spiegarla senza addentrarci nella strategia del gioco, basti dire che si trattava di una mossa che un umano non avrebbe mai scelto. Un perfetto esempio di AI che pensa in modo diverso.

Le AI non risolvono i problemi come gli esseri umani. I loro limiti sono diversi dai nostri. Prendono in considerazione più soluzioni possibili di quante ne possiamo valutare noi. Cosa ancor più importante, cercano tipi diversi di soluzioni. Esplorano vie che noi non consideriamo, più complesse di quelle che noi in genere prendiamo in esame. (Da tempo si dice che al momento di gestire simultaneamente una serie di dati, i nostri limiti cognitivi si attestano "al magico numero sette, più o meno due".[3] Un sistema di

AI non ha neanche lontanamente limitazioni del genere).

Nel 2015, un gruppo di ricerca inserì in un sistema AI chiamato Deep Patient i dati medici di circa 700mila soggetti, per verificare se fosse in grado di prevedere l'insorgere di malattie. Il risultato fu un successo a tutto campo. Sorprendentemente, Deep Patient riuscì con successo ad anticipare una serie di disturbi psichiatrici quali la schizofrenia. Per i medici invece è praticamente impossibile prevedere l'insorgere di un primo episodio psicotico. Tutto perfetto, il problema è che Deep Patient non fornisce alcuna spiegazione su come formuli diagnosi e previsioni e i ricercatori non hanno alcuna idea di come arrivi alle sue conclusioni. Un medico può scegliere di fidarsi o di ignorare il computer, ma non può chiedere altre informazioni.

Non è uno scenario ideale. Un sistema AI non dovrebbe solo sfornare una risposta, ma anche giustificarla, spiegarla in un modo comprensibile agli esseri umani. È necessario per poterci fidare delle decisioni del sistema AI e per assicurarci che non sia stato hackerato per prendere decisioni basate su un bias. Una spiegazione ragionevole ha un valore intrinseco, a prescindere dal fatto che migliori o meno l'accuratezza di una previsione; è per questo che in un giusto processo viene richiesto di giustificare le sentenze.

I ricercatori si stanno dando da fare per arrivare a una AI spiegabile. Nel 2017, la Defense Advanced Research Projects Agency (Darpa) ha lanciato un fondo per la ricerca di 75 milioni di dollari, per finanziare una decina di programmi che si occupano di questo problema. I progressi non mancheranno, ma di fondo sembra esserci un trade-off tra efficienza e spiegabilità, tra efficienza e sicurezza e tra spiegabilità e privacy. Le spiegazioni sono una scorciatoia cognitiva usata dagli umani, e si conformano ai processi decisionali umani. Le decisioni delle AI potrebbero semplicemente non essere riconducibili a spiegazioni comprensibili dagli umani, e costringere i sistemi AI a spiegarsi potrebbe limitarli, penalizzando la qualità delle loro decisioni. Non è chiaro dove ci condurrà la ricerca. Nel breve periodo, la AI diventerà sempre più insondabile, di pari passo con la sempre maggiore complessità dei suoi sistemi: diventerà progressivamente sempre meno "umana" e meno spiegabile.

In alcuni contesti, potrebbe non importarcene poi molto della spiegabilità. Se i dati dimostreranno che una diagnosi di Deep Patient è più accurata di quella di un medico umano mi affiderò alle sue cure anche se non saprà darmi spiegazioni. Allo stesso modo potrei fidarmi di un sistema AI che mi dice dove scavare per cercare il petrolio o che mi segnala quali parti di un aereo sono a maggior rischio di malfunzionamento. Potrei invece rifiutare il responso di un sistema AI che decide quali studenti, tra quelli che hanno fatto domanda per il college, andrà meglio negli studi, oppure di un sistema che valuta le possibilità di insolvenza nella decisione di accendere un mutuo prendendo in considerazione anche gli stereotipi razziali, o ancora di un sistema che concede la libertà vigilata ai detenuti prevedendo se saranno o meno recidivi.

A qualcuno andranno bene perfino sistemi AI che prenderanno decisioni importanti senza dare la minima spiegazione. È una cosa soggettiva, e probabilmente la vedremo in modo diverso una volta che le AI saranno inserite a pieno nel processo decisionale. C'è invece chi si oppone già da ora a una AI inspiegabile.

Il Future of Life Institute e altri ricercatori AI rilevano come la spiegabilità sia cruciale[4] soprattutto per i sistemi in grado di "fare danni", avere "un effetto significativo sugli individui" o "influenzare, la vita, la qualità della vita o la reputazione di qualcuno". Il rapporto *AI in the UK* sostiene[5] che non bisognerebbe impiegare un sistema AI che ha "un impatto rilevante sulla vita di un individuo" senza dare "una spiegazione piena e soddisfacente" del suo processo decisionale.

Io ritengo che a distinguere una AI che ci deve delle spiegazioni da una che non deve spiegarci nulla sia l'equità. Dobbiamo assicurarci che i sistemi AI non siano razzisti, sessisti, abilisti o discriminatori in modi imprevisti. Senza spiegabilità, rischiamo di ottenere risultati non dissimili a quelli del sistema AI di Amazon per esaminare le domande di lavoro. Il sistema era stato addestrato usando dieci anni di dati aziendali sulle assunzioni; l'industria tecnologica è però dominata dagli uomini, pertanto il sistema AI aveva imparato a essere sessista, e a dare minore rilevanza a un curriculum nel quale compariva la parola "femminile" o il nome di un'università frequentata da sole donne (ecco un caso in cui il futuro che vogliamo

non dovrà somigliare al passato).

Questo atteggiamento ingiusto e pieno di pregiudizi ha spinto i dirigenti di Amazon ad abbandonare il sistema non appena si sono resi conto di che cosa *stava* accadendo.[6] Si sono trovati di fronte a un problema difficile, forse insormontabile, dovuto all'esistenza di molte definizioni di equità, spesso in contraddizione tra loro:[7] quel che è "giusto" in un contesto non sempre lo è in un altro. Per determinare le ammissioni è più equo un sistema *gender blind*, che riconosce il genere, un sistema che corregge volutamente i bias sul genere preesistenti, uno che assegna i posti in proporzione ai generi, oppure uno che offre pari opportunità ai diversi generi e alle persone transgender e non binarie?

Saremo in grado di esaminare meglio il processo decisionale se il sistema AI è in grado di fornire spiegazioni, quando sono in ballo questioni come un'assunzione o la concessione della libertà vigilata. Significa che siamo più propensi a fidarci di quel sistema quando le questioni sono socialmente più sfumate di un responso del tipo "queste lastre indicano un tumore"?

Ma del resto, anche le decisioni umane non sono sempre del tutto spiegabili. A volte diamo spiegazioni che sono più che altro giustificazioni a posteriori, come confermano anche alcune ricerche. Forse non dobbiamo fare altro che guardare i risultati. Quando un tribunale stabilisce che un distretto di polizia si è comportato in modo razzista, non lo fa perché ha guardato nella testa dei poliziotti o ha chiesto loro di giustificare il proprio comportamento. Lo fa guardando le conseguenze delle loro azioni.

1. Douglas Adams (1978), *The Hitchhiker's Guide to the Galaxy*, BBC Radio 4.
2. Cade Metz (16 marzo 2016), "In two moves, AlphaGo and Lee Sedol redefined the future", *Wired*, www.wired.com/2016/03/two-moves-alphago-lee-sedol-redefined-future.
3. George A. Miller (1956), "The magical number seven, plus or minus two: Some limits on our capacity for processing information", *Psychological Review* 63, n. 2, http://psychclassics.yorku.ca/Miller.
4. J. Fjeld *et al.* (15 gennaio 2020), "Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principled AI", Berkman Klein Center for Internet and Society, https://cyber.harvard.edu/publication/2020/principled-ai.
5. Select Committee on Artificial Intelligence (16 aprile 2018), "AI in the UK: Ready, willing and able?", House of Lords, https://publications.parliament.uk/pald201719/ldselect/ldai/100/100.pdf.
6. Jeffrey Dastin (10 ottobre 2018), "Amazon scraps secret AI recruiting tool that shows bias against women", *Reuters*, www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.
7. David Weinberger (ultimo accesso 11 maggio 2022), "Playing with AI fairness", *What-If Tool*, https://pair-code.github.io/what-if-tool/ai-fairness.html; David Weinberger (6 novembre 2019), "How machine learning pushes us to define fairness", *Harvard Business Review*, https://hbr.org/2019/11/how-machine-learning-pushes-us-to-define-fairness.

CAPITOLO 53

Umanizzare la AI

I sistemi di intelligenza artificiale cambieranno la nostra vita a livello personale e sociale. Ho già parlato d'ingegneria sociale. I tentativi di phishing più riusciti – quelli che fanno perdere molto denaro alle aziende e ai singoli individui – verranno personalizzati. Chi lavora alla tesoreria di un'azienda potrebbe ricevere email da qualcuno che si finge un Ceo e che chiede un trasferimento di valuta: un trucco che potrebbe rivelarsi molto efficace, soprattutto se accompagnato da un audio o da un video. Le AI potranno automatizzare la customizzazione degli attacchi di phishing, consentendo ai truffatori di inviare email o vocali studiati appositamente per i singoli obiettivi.

Subire l'inganno di una AI non è per forza peggio di essere truffati da un essere umano. Il vero pericolo sta nella velocità e nella portata degli inganni che una AI può architettare. Gli hack cognitivi sono ancora piuttosto rozzi: finti articoli di giornale o provocazioni in grado di buggerare solo i più ingenui o disperati. La AI potenzialmente è in grado di attuare hack cognitivi microtargettizzati: personalizzati, ottimizzati e inviati singolarmente. Alcuni vecchi stratagemmi come la "truffa all'americana" (*pigeon drop*) sono hack cognitivi su misura.

Le campagne pubblicitarie sono hack cognitivi su grande scala. Le tecniche AI hanno il potenziale per mescolare caratteristiche di entrambe le tecniche.

Da tempo attribuiamo caratteristiche umane ai programmi informatici. Negli anni Sessanta, il programmatore Joseph Weizenbaum creò un rudimentale simulatore di conversazione chiamato Eliza, che imitava i modi di uno psicoterapeuta.[1] Weizenbaum si stupì di come le persone, seppur consapevoli di parlare con un ottuso programma informatico, gli confessassero i propri segreti più intimi. La segretaria di Weizenbaum gli chiese addirittura di uscire dalla stanza per poter parlare con Eliza in

privato. Oggi ci capita di essere gentili con assistenti vocali come Alexa e Siri,[2] come se a loro importasse qualcosa di come ci poniamo. Siri si lamenta perfino dei nostri modi troppo bruschi – "Non è molto gentile da parte tua" – ma solo perché è stata programmata per farlo. Molti altri esperimenti sono approdati agli stessi risultati. I soggetti di una ricerca hanno valutato meno criticamente la performance di un computer quando dovevano usare quello stesso computer per dargli i voti: non volevano urtarne la sensibilità.[3] In un altro esperimento, quando un computer raccontava a uno dei soggetti dello studio qualche sua "informazione personale" evidentemente fittizia, il soggetto rispondeva condividendo a sua volta qualche dettaglio intimo.[4] Da tempo la forza della reciprocità è ben nota a psicologi e a chi cerca di usarla come hack, l'ennesimo hack cognitivo che può servirsi della AI per moltiplicarsi come non mai.

La robotica rende gli hack che sfruttano la AI ancor più efficaci. Gli esseri umani hanno sviluppato scorciatoie cognitive estremamente funzionali per riconoscere le altre persone. Vediamo volti ovunque: bastano due puntini su una linea orizzontale e ci sembra di osservare un volto. Per questo perfino le illustrazioni più semplici sono tanto efficaci: se qualcosa ha un volto, dev'essere una creatura dotata di volontà, emozioni e qualunque cosa in genere associata ai volti reali. E se quel qualcosa parla, o ancor meglio ci parla, crederemo che sia dotato di finalità, desideri e capacità di agire. Dategli due sopracciglia, e resistere sarà ancor più difficile.

I robot non fanno eccezione. Ci sono persone che hanno quasi un rapporto umano coi propri aspirapolvere, e si lamentano se la ditta invece di riparare i "loro" Roomba propone di sostituirli. Un colonnello dell'esercito americano ha cercato di impedire che un robot a forma di insetto per scovare le mine antiuomo continuasse a farsi male un'esplosione dopo l'altra.[5] A Harvard un robot ha citofonato agli studenti e li ha convinti a farlo entrare nel dormitorio fingendo di essere lì per consegnare il cibo. Boxie, un robot parlante con la faccetta buffa sviluppato dai ricercatori del Mit, ha persuaso invece alcuni soggetti a rispondere a domande intime semplicemente chiedendoglielo in modo gentile.

Parte del nostro modo di rispondere ai robot somiglia a come ci

rapportiamo all'aspetto e al comportamento dei bambini. I bambini hanno la testa più grande in proporzione al corpo, occhi più grandi in proporzione alla testa e ciglia più lunghe in proporzione agli occhi. Le loro vocine sono acute. Tutte queste cose ci fanno venir voglia di proteggerli. Da tempo immemore i creativi ne approfittano per realizzare opere in grado di intenerirci. I bambolotti sono pensati per innescare una risposta amorevole. I personaggi dei cartoni animati sono spesso fatti così, pensiamo a Betty Boop (anni Trenta) e Bambi (1942). Gli occhi del personaggio principale del film con attori reali *Alita: Angelo della battaglia* (2019) sono stati ingranditi al computer. Nel 2016, il Georgia Institute of Technology ha pubblicato uno studio sulla fiducia degli umani in un robot non antropomorfo che li aiutava a uscire da un edificio, con indicazioni come "passa di qui per arrivare all'uscita".[6] Inizialmente, i partecipanti interagivano col robot in una situazione normale e la performance del robot era volutamente scadente. In seguito, gli umani dovevano decidere se seguire o no i consigli del robot in una condizione di emergenza simulata: tutti i ventisei partecipanti hanno seguito le indicazioni del robot, anche se poco prima avevano visto coi propri occhi che non era un navigatore particolarmente bravo. Si fidavano della macchina in modo impressionante: il robot li ha indirizzati verso una stanza buia che non sembrava avere uscite, eppure quasi tutti ci sono entrati, invece di mettersi in salvo uscendo da dove erano entrati. I ricercatori hanno condotto esperimenti simili con altri robot apparentemente difettosi. Anche in questo caso i soggetti hanno seguito le istruzioni dei robot in condizioni d'emergenza, senza affidarsi invece al buonsenso. A quanto pare, i robot riescono naturalmente ad hackerare la nostra fiducia.

I robot antropomorfi sono dunque una tecnologia che ci persuade sfruttando le nostre emozioni e la AI li renderà ancor più accattivanti. La AI può imitare gli esseri umani o perfino gli animali, pertanto per inventare nuovi hack sfrutterà i meccanismi usati dagli umani per rapportarsi al prossimo. Come ha scritto nel 2010 la psicologa Sherry Turkle: "Quando i robot cercano il contatto visivo riconoscono le voci, riproducono i gesti umani, sono in grado di tirare i nostri fili darwiniani e attuare comportamenti che

riconduciamo a discernimento, volontà ed emozioni”.[7] Esatto: ci hackerano il cervello.

La AI ci spingerà non solo a trattarla come trattiamo le persone, ma si comporterà anche in modi studiati appositamente per ingannarci. Si servirà di hack cognitivi.

1. Joseph Weizenbaum (gennaio 1966), “ELIZA: A computer program for the study of natural language communication between man and machine”, *Communications of the ACM*, https://web.stanford.edu/class/linguist238/p36-weizenabaum.pdf.
2. James Vincent (22 novembre 2019), “Women are more likely than men to say ‘please’ to their smart speaker”, *Verge*, www.theverge.com/2019/11/22/20977442/ai-politeness-smart-speaker-alexa-siri-please-thank-you-pew-gender-sur.
3. Clifford Nass, Youngme Moon e Paul Carney (31 luglio 2006), “Are people polite to computers? Responses to computer-based inter-viewing systems”, *Journal of Applied Social Psychology*, https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1559-1816.1999.tb00142.x.
4. Youngme Moon (marzo 2000), “Intimate exchanges: Using computers to elicit self-disclosure from consumers”, *Journal of Consumer Research*, www.jstor.org/stable/10.1086/209566?seq=1.
5. Joel Garreau (6 maggio 2007), “Bots on the ground”, *Washington Post*, www.washingtonpost.com/wp-dyn/content/article/2007/05/05/AR2007050501009_pf.html.
6. Paul Robinette *et al.* (marzo 2016), “Overtrust of robots in emergency evacuation scenarios”, 2016 ACM/IEEE International Conference on Human-Robot Interaction, www.cc.gatech.edu/~alanwags/pubs/Robinette-HRI-2016.pdf.
7. Sherry Turkle (2010), “In good company”, in Yorick Wilks (a cura di), *Close Engagements with Artificial Companions*, John Benjamin Publishing.

CAPITOLO 54

Quando AI e robot ci hackerano

Durante le elezioni Usa del 2016, circa un quinto dei tweet d'argomento politico sono stati postati da bot. La cifra è salita a un terzo in Gran Bretagna, lo stesso anno, prima del voto per la Brexit. Un rapporto dell'Oxford Internet Institute del 2019 ha riscontrato che in almeno cinquanta Paesi i bot sono stati usati per diffondere propaganda.[1] In genere si è trattato di semplici programmi che ripetevano slogan a pappagallo. Ad esempio, nel 2018, dopo l'omicidio di Jamal Khashoggi, sono stati postati 250mila tweet filo-sauditi "Riponiamo la nostra fiducia nel principe Mohammed bin Salman". Nel 2017, la Federal Communications Commission ha permesso per un certo periodo al pubblico di intervenire circa una possibile revoca della *net neutrality*, ricevendo ben ventidue milioni di commenti. 1,3 milioni di questi commenti particolarmente aggressivi erano stati generati a partire dallo stesso template, cambiando qualche parola per farli sembrare unici. Bastava però anche un'occhiata veloce per individuarli.

Trucchi del genere diventeranno sempre più sofisticati. Già da anni i programmi AI creano articoli su sport e finanza per organizzazioni reali come la Associated Press. Si tratta di argomenti limitati, e pertanto è stato semplice adattarli alle AI. Oggi però la AI viene usata anche per articoli di taglio più generico. Esistono sistemi per la creazione di testi come Gpt-3 di Open AI[2] ai quali basta ricevere qualche fatto come input per scrivere un articolo; il problema è che questi sistemi possono anche essere addestrati a suon di bugie per scrivere fake news.

È facile immaginare come la AI guasterà il dibattito politico. Già oggi è in grado di scrivere lettere personalizzate a giornali e figure politiche, lasciare commenti su forum e siti d'informazione, o perfino discutere sui social media. Quando questi sistemi impareranno a usare ancor meglio la nostra lingua, sarà addirittura più difficile

distinguerli da persone reali e smascherare tattiche che un tempo non ci avrebbero messo in difficoltà.

In un recente esperimento, alcuni ricercatori hanno risposto a un appello del governo che chiedeva opinioni al pubblico sul tema Medicaid,[3] e hanno postato mille commenti scritti con una AI per la *text generation*. Sembravano tutti diversi, e scritti da persone che difendevano posizioni specifiche. Gli amministratori di Medicaid.gov ci sono cascati e hanno accolto quei contributi come fossero il frutto di preoccupazioni reali. In seguito i ricercatori hanno chiesto di rimuovere quei commenti, in modo di non creare bias nel dibattito politico, ma altri non si sarebbero comportati in modo tanto etico.

Queste tecniche vengono già usate in tutto il mondo per influenzare le attività politiche. Una campagna di propaganda online ha usato ritratti generati dalla AI per creare falsi giornalisti. La Cina ha bombardato di testi generati artificialmente la campagna elettorale taiwanese del 2020. La tecnologia deep-fake – tecniche AI per creare video realistici di eventi mai accaduti, spesso mettendo in bocca a persone vere frasi che non avrebbero mai detto – è stata usata in Paesi come Malesia, Belgio e Usa.

Da questa tecnologia deriva il *persona bot*, una AI che si presenta come un essere umano su social media o altri gruppi online. Questi bot hanno un passato, una personalità, un modo tutto loro di comunicare. Non fanno costantemente propaganda e riescono così ad aggirarsi in gruppi di vario tipo: giardinaggio, lavoro a maglia, trenini ecc. Si comportano come normali membri di queste comunità, postando commenti e discutendo di vari temi. Sistemi come Gpt-3 permettono alle AI di fare incetta di contenuti e conversazioni relative a un tema, per dare ai bot una parvenza di competenza. Poi, di tanto in tanto, la AI si finge tutta preoccupata e posta un contenuto d'argomento politico, magari linkando un articolo su un infermiere che ha avuto una reazione allergica al vaccino per il Covid-19. Oppure fa sapere a tutti quel che il suo sviluppatore pensa delle ultime elezioni, del razzismo o di qualunque argomento divisivo. Un singolo bot non può certo cambiare l'opinione pubblica, ma se invece di uno ce ne fossero migliaia? O milioni?

È quella che si chiama “propaganda informatica”, qualcosa che cambierà per sempre il nostro modo di vedere la comunicazione. La AI ha il potenziale per diffondere all’infinito la disinformazione. Può anche distruggere il dibattito all’interno di una community. Nel 2012, Kate Darling, esperta di etica robotica, ha condotto un esperimento con un giocattolo, un dinosauro animatronico di plastica chiamato Cleo[4] in grado di dare diverse risposte al contatto fisico. Dopo aver fatto giocare con Cleo i partecipanti a un convegno scientifico, ha chiesto loro di “farle del male” in vari modi. Alle persone era però bastato giocare con Cleo qualche minuto per sviluppare una forte empatia e per questo si sono rifiutate di obbedire, anche se Cleo non avrebbe sentito dolore. È una risposta profondamente umana. Per quanto possiamo sapere a livello intuitivo che Cleo è solo un dinosauro di plastica, il fatto che avesse il volto grande e il corpo piccolo ci fa pensare a un bambino. E il suo nome ci dice che è femmina! E guarda come risponde alle nostre carezze! Non riusciamo a non considerarla una creatura dotata di emozioni e ci sentiamo in dovere di non farle provare dolore.[5] Può sembrare una reazione positiva, ma che cosa succede se quel simpatico robottino guarda i suoi padroni umani coi suoi occhioni e chiede loro di acquistarle l’ultimo aggiornamento del suo software?

Siamo inclini a commettere errori di categorizzazione e a trattare i robot come creature viventi, dotate di volontà e sensibilità e pertanto offriamo il fianco alla loro manipolazione. I robot ci possono convincere a fare cose che altrimenti non faremmo. Oppure possono spaventarci e spingerci a non agire. In un esperimento, un robot si è dimostrato in grado di esercitare la *peer pressure*, la pressione sociale, sulle persone che partecipavano allo studio,[6] portandole ad assumersi rischi maggiori. Quanto tempo dovrà passare prima che un sex robot al culmine del piacere ci spinga a qualche acquisto online?

La AI diventerà sempre più brava a persuaderci a fare cose del genere. I ricercatori sono già al lavoro su AI che rilevano le nostre emozioni analizzando scrittura ed espressioni del volto o monitorando respiro e battito del cuore. Spesso sbagliano, ma la tecnologia li aiuterà a migliorare. E ben presto le AI diventeranno più

brave delle persone. Sarà così possibile una manipolazione più precisa, e come ho già detto, più adattabile ai singoli individui.

Aibo è un cane robot lanciato da Sony nel 1999. Fino al 2005 l'azienda ogni anno ha presentato un nuovo modello migliorato, ma negli anni a venire ha smesso di fornire assistenza per quelli già venduti. Gli Aibo erano piuttosto rudimentali a livello informatico, ma la gente si affezionava comunque. In Giappone, c'è chi ha fatto fare il funerale al proprio Aibo.

Nel 2018, Sony ha cominciato a vendere Aibo di nuova generazione. La loro particolarità non è tanto che i progressi del software li facciano assomigliare di più a dei cuccioli reali, ma il fatto che ora per funzionare richiedano di immagazzinare dati in un cloud. A differenza di quanto accadeva in passato, Sony può pertanto modificare o perfino "uccidere" a distanza qualunque Aibo. Il costo del cloud è di 300 dollari l'anno. Se Sony avesse voluto massimizzare i propri ricavi avrebbe potuto offrirlo gratuitamente per i primi tre anni e poi – una volta sviluppato un legame emotivo tra padrone e cucciolo – richiedere una somma molto più alta. Potremmo chiamare questa tattica "trappola emotiva".

AI e robot autonomi si occuperanno sempre più di mansioni reali, hackerando la fiducia degli umani in questi sistemi. Le conseguenze saranno costose e pericolose, ma non dimentichiamoci che sono gli umani a controllare le AI. Tutti i sistemi AI sono progettati e finanziati da umani che vogliono manipolare altri umani in un modo specifico e per un determinato scopo. Quando si tratta di hackerare le nostre emozioni, aziende potentissime come Sony sanno dimostrarsi molto lungimiranti, con grossi investimenti in tecnologia e ricerca. Se non cercheremo di frenare i loro hack con norme e regole, presto le persone comuni si troveranno a fronteggiare AI dalle capacità letteralmente sovrumane che agisce per conto dei loro potenti padroni.

1. Samantha Bradshaw e Philip N. Howard (2019), "The global disinformation order: 2019 global inventory of organised social media manipulation", *Computational Propaganda Research Project*, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.
2. Tom Simonite (22 luglio 2020), "Did a person write this headline, or a machine?", *Wired*, www.wired.com/story/ai-text-generator-gpt-3-learning-language-fitfully.
3. Max Weiss (17 dicembre 2019), "Deepfake bot submissions to federal public comment websites cannot be distinguished from human submissions", *Technology Science*, https://techscience.org/a/2019121801.
4. Kate Darling (2021), *The New Breed: What Our History with Animals Reveals about Our Future with Robots*, Henry Holt.
5. Woodrow Hartzog (4 maggio 2015), "Unfair and deceptive robots", *Maryland Law Review*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2602452.
6. Yaniv Hanoch et al. (17 maggio 2021), "The robot made me do it: Human–robot interaction and risk-taking behavior", *Cyberpsychology, Behavior e Social Networking*, www.liebertpub.com/doi/10.1089/cyber.2020.0148.

CAPITOLO 55

Computer e AI stanno accelerando l'hacking della società

L'hacking è antico come il mondo. Nella storia non c'è sistema che non sia stato hackerato: con l'invenzione del computer è stato inventato anche l'hacking informatico. I computer si prestano all'hacking meglio di qualunque altra cosa, a causa della loro complessità e delle loro interfacce programmabili. Oggi molti prodotti di consumo – auto, dispositivi elettronici, telefoni – sono controllati dai computer. Tutti i nostri sistemi sociali – finanziario, fiscale, normativo, elettorale – sono sistemi sociotecnici complessi che coinvolgono computer, reti, persone e istituzioni, e pertanto sono facilmente hackerabili.

L'informatica cambia però la forma dell'hacking. Soprattutto con l'uso delle tecniche di AI, accelera l'hacking lungo quattro dimensioni: velocità, grandezza, portata e complessità.

La velocità è facile da capire: i computer sono molto più rapidi degli esseri umani. Non hanno bisogno di dormire, non si annoiano, non si distraggono. Se programmati a dovere, fanno meno errori degli esseri umani. Di conseguenza, i computer eseguono i compiti in modo più efficiente degli umani;[1] uno smartphone impiega una piccola porzione dell'energia e del tempo che servirebbero a un essere umano per eseguire correttamente un calcolo matematico. Rendendo più agevoli questi compiti meccanici, i computer trasformano alcuni hack da praticamente assurdi ad assurdamente pratici.

Lo stiamo già constatando coi nostri occhi. Un servizio gratuito basato su AI, Donotpay ("Non pagare"), automatizza il processo di contestazione delle multe per divieto di sosta,[2] aiutando a non pagare centinaia di migliaia di sanzioni in città come Londra o New York. Donotpay ha anche ampliato il servizio e dà una mano a richiedere i rimborsi alle compagnie aeree colpevoli di ritardi sui voli e a cancellare una serie di servizi e sottoscrizioni.

La AI rende inoltre più facile fare esperimenti: i computer possono provare in un lampo innumerevoli varianti di un prodotto per trovarne la migliore. Gli sviluppatori web si servono spesso dei test A/B, mostrando diverse versioni di un prodotto a vari utenti per verificare l'efficacia del loro web design. Ad esempio, la versione A può presentare un pulsante "Clicca qui" più grande della versione B; in un caso del genere, il sito raccoglie i dati e sceglie automaticamente la versione che riceve più click. I test automatizzati A/B[3] permettono agli sviluppatori di testare simultaneamente combinazioni complesse di una serie di variabili (dimensioni, colore, posizionamento, font), consentendo una quantità senza precedenti di hack ulteriormente personalizzabili – con l'ausilio dei big data – in base alle specifiche abitudini e preferenze degli utenti. La capacità di simulare migliaia di variazioni di un hack permette inoltre di ampliare la portata degli hack eseguibili, sia legalmente, a livello commerciale, sia illegalmente.

Passiamo dunque alla questione della grandezza delle AI, che ad esempio cambiano radicalmente un'attività umana dalla storia lunghissima come la compravendita di azioni, apportandole nuove caratteristiche impreviste e non volute. I sistemi AI riescono a svolgere attività umane su una scala mai sperimentata prima.

Probabilmente quegli stessi bot che abbiamo appena visto verranno usati anche sui social media. Saranno in grado di occuparsi all'istante del tema del momento, mandando un'infinità di messaggi. Se avranno briglia sciolta, potrebbero soffocare ogni reale dibattito online.[4] Influenzeranno artificialmente la nostra idea di che cosa sia normale e di quali siano le opinioni più diffuse, con ricadute non solo nei social media ma in ogni piazza, in ogni salotto. Una manipolazione tale non giova certo al mercato delle idee di qualunque sistema politico. La democrazia, come abbiamo già detto, per funzionare a dovere ha bisogno di informazione, scelta e agency. I bot possono privare i cittadini sia dell'informazione sia dell'agency.

La portata delle AI è destinata ad aumentare. La potenza dei computer non farà che crescere, proprio come il numero di decisioni – sempre più importanti – che si vedranno delegare. Gli hack di questi sistemi saranno pertanto in grado di causare danni più diffusi,

con un potenziale distruttivo in grado di mettere in pericolo l'intero sistema sociotecnico, a prescindere dalle intenzioni degli hacker.

La AI inevitabilmente esaspererà queste tendenze. Già oggi i sistemi AI prendono decisioni in grado di influenzare le nostre vite, che riguardino piccole questioni quotidiane o grandi problemi. Ci danno indicazioni mentre guidiamo, dettandoci la strada passo passo. Ci impediscono di ottenere un mutuo o la libertà vigilata. Selezionano i candidati a un posto di lavoro, gli studenti che vogliono entrare in un college e chi ambisce a un ruolo nella pubblica amministrazione. Scelgono dove investire e aiutano i giudici anche in caso di reati penali. Decidono quali notizie vedremo sui social media, se vedremo i banner elettorali di un candidato o di un altro e quali persone e argomenti cercheranno di attirare la nostra attenzione. Individuano obiettivi militari. In futuro, le AI potrebbero consigliare alle persone più ricche quali personaggi politici finanziare. Potrebbero stabilire chi ha il diritto di voto. Partendo da un'idea di società, potrebbero delineare le politiche fiscali e selezionare le persone meritevoli di ricevere il welfare.

L'hacking di questi sistemi causerà danni sempre maggiori (l'abbiamo già visto con i *flash crash*, i crolli improvvisi del mercato azionario).[5] Per di più, non avremo modo di conoscere nel dettaglio la progettazione, la realizzazione e l'uso di questi sistemi.

Infine, i progressi delle AI – computer sempre più rapidi e potenti, reti sempre più complesse – aumenteranno i casi in cui le macchine sostituiranno gli umani: i computer saranno infatti in grado di mettere in atto strategie complesse e inattese, per noi inarrivabili.

Molti algoritmi vanno già oltre la comprensione umana, sia che servano a suggerirci che film guardare sia che ci facciano da consulenti negli investimenti o che ci sfidino a una partita di Go. È una tendenza destinata a crescere, forse in modo esponenziale, quando gli algoritmi cominceranno a programmare altri algoritmi.

Con l'ascesa della AI, l'hacking informatico diviene uno dei sistemi più potenti per hackerare la società. Quando tutto è computer, il software controlla ogni cosa. Immaginiamo un hacker all'interno di una rete finanziaria, che altera il flusso monetario. O all'interno di un database giudiziario, che apporta piccoli ma importanti cambiamenti

a leggi e sentenze (qualcuno se ne accorgerà o ne saprà abbastanza da verificare quale fosse la legge originale?).

Pensiamo a un hacker che modifica da dentro l'algoritmo di Facebook e cambia le regole che stabiliscono a quali post spetti la preminenza nel feed, chi potrà far sentire la sua voce e chi dovrà ascoltarla. I programmi informatici gestiscono la nostra quotidianità, come lavoriamo, come spendiamo i nostri soldi, come parliamo, come ci organizziamo: è la tecnologia che assurge al ruolo di policymaker. La tecnologia ci dona tanta libertà, ma nelle mani di un hacker può divenire un'architettura impareggiabile per il controllo della società.

Tutti questi sistemi sono vulnerabili all'hacking;[6] le ricerche ci dicono che i sistemi di machine learning possono essere compromessi in modo impossibile da individuare. E gli effetti di questi hack sulla società non faranno che aumentare.

1. Karlheinz Meier (31 maggio 2017), “The brain as computer: Bad at math, good at everything else”, *IEEE Spectrum*, https://spectrum.ieee.org/the-brain-as-computer-bad-at-math-good-at-everything-else.
2. Samuel Gibbs (28 giugno 2016), “Chatbot lawyer overturns 160,000 parking tickets in London and New York”, *The Guardian*, www.theguardian.com/technology/2016/jun/28/chatbot-ai-lawyer-donotpay-parking-tickets-london-new-york.
3. Amy Gallo (28 giugno 2017), “A refresher on A/B testing”, *Harvard Business Review*, https://hbr.org/2017/06/a-refresher-on-ab-testing.
4. Una legge dello stato della California impone ai robot di identificarsi. Renee DiResta (24 luglio 2019), “A new law makes bots identify themselves – that’s the problem”, *Wired*, www.wired.com/story/law-makes-bots-identify-themselves.
5. Laim Vaughan (2020), *Flash Crash: A Trading Savant, a Global Manhunt e the Most Mysterious Market Crash in History*, Doubleday.
6. Shafi Goldwasser *et al.* (14 aprile 2022), “Planting undetectable backdoors in machine learning models”, *arXiv*, https://arxiv.org/abs/2204.06974.

CAPITOLO 56

Quando le AI diventano hacker

Gli hacker giocano a "ruba-bandiera", una sorta di versione informatica del celebre gioco all'aria aperta. Ogni squadra difende la propria bandiera e cerca di prendere quella dell'altra squadra. È un gioco che si svolge in un ambiente controllato, ma che riflette quel che fanno gli hacker nella vita reale: scovano le vulnerabilità nei propri sistemi per ripararle e in quelli degli altri per sfruttarle.

Già a metà degli anni Novanta la competizione è diventata un classico delle convention di hacker. Oggi ci sono decine di team di tutto il mondo che, dopo essersi allenati per mesi, si fronteggiano nel corso di eventi maratona per conquistare la tanto agognata vittoria. Per gli appassionati, non c'è divertimento maggiore (che non sia illegale).

La Darpa Cyber Grand Challenge, tenutasi nel 2016, è stata un evento del genere, destinato però alle AI, al quale hanno preso parte cento squadre.[1] Dopo i gironi di qualificazione, le sette finaliste si sono scontrate alla Def Con di Las Vegas, in un ambiente appositamente progettato con un *custom software* mai analizzato o testato prima. Le AI avevano a disposizione dieci ore per trovare le vulnerabilità delle altre AI e sfruttarle, oltre che per mettere le patch alle proprie ed evitare che gli avversari ne approfittassero. Il vincitore è stato il sistema Mayhem, creato da un team di esperti di sicurezza informatica di Pittsburgh. Questi stessi ricercatori hanno poi messo in vendita la loro tecnologia, che ora vanta clienti come il Dipartimento della Difesa.

Al Def Con, quello stesso anno, si è tenuto anche un "ruba-bandiera" per esseri umani, con Mahyem come unico partecipante non umano. Nel complesso è arrivato ultimo, senza però ottenere il risultato peggiore in tutte le categorie. Possiamo immaginare facilmente come potrebbe andare in futuro un confronto del genere. L'abbiamo visto con gli scacchi e col Go. Le AI migliorano di anno in

anno, di pari passo coi progressi della tecnologia. Le squadre umane invece si fermano più o meno allo stesso livello, perché gli umani son pur sempre umani, anche quando dispongono di strumenti migliori. E prima o poi la AI sconfiggerà gli umani. Secondo me ci vorranno meno di dieci anni.

Stranamente la Darpa non ha mai più riproposto competizioni di questo genere, ma da allora ne sono state organizzate molte in Cina, con tanto di eventi ibridi in cui si scontrano umani e computer. Non disponiamo di molti dettagli – si tratta infatti di eventi interni, in genere organizzati dall'esercito – ma, come possiamo immaginare, i sistemi cinesi di AI non fanno che migliorare.[2]

Ci vorrà qualche anno prima di arrivare ad AI del tutto autonome in grado di scagliare attacchi hacker, ma già oggi le tecnologie AI stanno trasformando la natura stessa dei cyberattacchi. Le AI sono particolarmente brave a scovare le vulnerabilità di un sistema. Setacciano i software una linea di codice dopo l'altra senza annoiarsi, basta che qualcuno spieghi loro come riconoscere una vulnerabilità. Bisognerà occuparsi di molti problemi specifici di alcuni domini, un tema sul quale la letteratura accademica non manca di certo e le ricerche proseguono.[3]

Sembra scontato che le AI continueranno a migliorare fino a raggiungere valori di eccellenza, con implicazioni che vanno ben oltre le reti informatiche. Le AI sapranno infatti trovare migliaia di nuove vulnerabilità in molti dei sistemi descritti in questo libro: tasse, norme bancarie, procedure politiche. Ovunque ci sia una moltitudine di regole interrelate, la AI sarà in grado di riscontrare vulnerabilità e sfruttarle. Ad esempio, già oggi le AI vengono usate per rintracciare eventuali loophole nei contratti, e in futuro diverranno sempre più abili.[4] Il successo di un hacker dipende da quanto lui conosce il sistema-target e le sue interazioni con il resto del mondo. Le AI inizialmente capiscono queste cose tramite i training data, ma l'uso consente loro di migliorare. Le AI moderne si evolvono costantemente acquisendo nuovi dati e regolando il proprio funzionamento di conseguenza. Il flusso continuo di dati continua ad addestrare la AI mentre opera e a renderla più competente. Per questo i progettisti dei veicoli a guida autonoma si vantano di quante

ore di strada hanno accumulato le loro creazioni.

La possibilità di sviluppare AI in grado di hackerare altri sistemi pone due problemi diversi ma correlati. In primo luogo, potremmo ordinare a una AI di hackerare un sistema. Qualcuno potrebbe dare in pasto a una AI tutti i regolamenti fiscali e finanziari del mondo, per creare una nuova serie di hack molto remunerativi. In secondo luogo, una AI potrebbe inconsapevolmente hackerare un sistema. Sono entrambi scenari pericolosi, ma il secondo lo è di più, perché potremmo non scoprirlo mai.

1. Jia Song e Jim Alves-Foss (novembre 2015), "The DARPA Cyber Grand Challenge: A competitor's perspective", *IEEE Security and Privacy Magazine* 13, n. 6, www.researchgate.net/publication/286490027_The_DARPA_cyber_grand_challenge_A_competitor%27s_perspective.
2. Dakota Cary (Sep 2021), "Robot hacking games: China's competitions to automate the software vulnerability lifecycle", Center for Security and Emerging Technology, https://cset.georgetown.edu/wp-content/uploads/CSET-Robot-Hacking-Games.pdf.
3. Bruce Schneier (18 dicembre 2018) "Machine learning will transform how we detect software vulnerabilities", *Security Intelligence*, https://securityintelligence.com/machine-learning-will-transform-how-we-detect-software-vulnerabilities/.
4. Redazione dell'*Economist* (12 giugno 2018), "Law firms climb aboard the AI wagon", *Economist*, www.economist.com/business/2018/07/12/law-firms-climb-aboard-the-ai-wagon.

CAPITOLO 57

Il reward hacking

Come ho già scritto, la AI non risolve i problemi nello stesso modo in cui lo farebbe un essere umano. Una AI prima o poi finisce per trovare soluzioni che gli umani non avrebbero mai potuto aspettarsi, in grado talora di sovvertire l'intento del sistema analizzato. Le AI non pensano infatti secondo implicazioni, contesti, norme e valori condivisi e dati per scontati dagli umani.

Si parla di *reward hacking* quando una AI raggiunge lo scopo in modo imprevisto e non voluto dai suoi designer.[1] Eccovi qualche esempio esplicativo:

– In una simulazione di calcio uno contro uno, invece di tirare in porta, la AI tira fuori per costringere l'avversario a effettuare la rimessa in gioco con la porta sguarnita.[2]

– Una AI riceve l'ordine di impilare alcuni mattoncini Lego. L'altezza a cui sollevarli viene misurata dalla posizione della faccia inferiore di un mattoncino. La AI impara a ribaltare il mattoncino per mettere quella faccia in alto (ovviamente, nelle istruzioni non ce n'era nessuna che impedisse di farlo).[3]

– In un ambiente simulato per creature "evolute", a una AI viene consentito di modificare le proprie caratteristiche fisiche per raggiungere meglio i propri obiettivi. Viene assegnato come obiettivo quello di attraversare un traguardo il prima possibile. Ci si aspetta che la AI scelga gambe più lunghe, muscoli più forti o una maggiore capacità polmonare. La AI decide invece di diventare così alta da attraversare il traguardo semplicemente cadendo a terra.[4]

Sono tutti hack. Possiamo magari addossarne la colpa a obiettivi e ricompense mal descritti o riscontrare che avvengono tutti in ambienti simulati, ma il punto è un altro. Le AI sono progettate per ottimizzare le loro funzioni in base a un obiettivo e per questo, in modo naturale e inconsapevole, implementano hack inattesi.

Immaginiamo un aspirapolvere robot col compito di ripulire tutto lo sporco che vede.[5] A meno che il suo obiettivo non venga specificato meglio, potrebbe decidere di disabilitare o coprire i propri sensori ottici per non vedere più alcuno sporco. Nel 2018, un programmatore dallo spirito imprenditoriale – o forse solo molto annoiato – ha cercato di fare in modo che il suo aspirapolvere robot la smettesse di sbattere contro i mobili e l'ha addestrato ricompensandolo quando non sbatteva.[6] La AI ha imparato però ad andare in retromarcia: sul retro non aveva infatti sensori che potessero rilevare eventuali urti.

Se in una serie di regole sussistono problemi, incoerenze e loophole, e se tali proprietà conducono a una soluzione accettabile secondo le regole definite, la AI prima o poi le troverà. Guardando i risultati, potremmo pensare: "Ah be', tecnicamente la AI ha seguito le regole". Avremo però la sensazione che la AI ha barato, ha aggirato il sistema, lo ha hackerato, prima di renderci conto che la nostra comprensione del contesto sociale del problema è diversa da quella della AI, come diverse sono le nostre aspettative. I ricercatori del settore parlano in questo caso di problema di *goal alignment*, allineamento degli obiettivi.

La storia di Re Mida può servirci da esempio. Il dio Dioniso gli concede un solo desiderio e Re Mida chiede che tutto quel che tocchi si trasformi in oro. Le conseguenze sono tragiche: Re Mida non può più mangiare o bere, perché tutto si è trasformato in oro, proprio come la sua amata figlia. È un problema di allineamento degli obiettivi: Re Mida ha programmato l'obiettivo sbagliato nel suo sistema di desideri.

Anche i geni della lampada sono molto precisi sulla scelta delle parole giuste per esprimere i desideri, e quando li esaudiscono si divertono a essere puntigliosi. Non c'è modo di batterli in furbizia. Qualunque cosa si desideri, il genio la farà avverare in modo da fartelo rimpiangere. Il genio riesce sempre ad hackerare il tuo desiderio.

Più in generale, nella lingua e nel pensiero umano, obiettivi e desideri non sono mai del tutto specificati.[7] Non pensiamo mai a ogni singola opzione. Non controlliamo minuziosamente ogni rischio, ogni eccezione o clausola. Non chiudiamo mai tutte le possibilità di

hacking. Non lo facciamo perché non ne siamo in grado. Qualunque obiettivo specificheremo non potrà che essere incompleto.

Nelle interazioni umane lo possiamo quasi sempre accettare, in quanto le persone comprendono i contesti e agiscono quasi sempre in buona fede. Per diventare parte della società, abbiamo acquisito nozioni condivise su come vada il mondo. Riempiamo ogni vuoto di comprensione servendoci dei contesti e del buonsenso.

La filosofa Abby Everett Jaques quando era a capo del Progetto sull'etica delle AI presso il Mit ha spiegato: immaginate che vi chieda di portarmi un caffè. Se c'è un bricco nelle vicinanze me ne verserete una tazza, altrimenti andrete a comprarmene uno al bar all'angolo. Non mi porterete un camion di chicchi da tostare. Non comprerete una piantagione di caffè in Costa Rica. Non ruberete la tazza che sta bevendo qualcuno nei paraggi. Non mi porterete un caffè preparato una settimana fa o una salviettina usata per pulire il caffè caduto sul tavolo. E non ho neanche bisogno di specificarlo. Lo sapreste e basta. Allo stesso modo, se vi chiedo di sviluppare una tecnologia che trasforma in oro le cose toccate, non la costruirete in modo da far morire di fame chi la userà. Non dovrei dirlo nemmeno, lo sapreste già.

Non possiamo specificare del tutto un obiettivo a una AI, così come la AI non sarà del tutto in grado di capirne il contesto.

Nel corso di un Ted Talk, il ricercatore AI Stuart Russell ha immaginato un assistente AI[8] che provoca un ritardo aereo perché qualcuno non arrivi puntuale a una cena. Il pubblico ha riso, ma un computer come può sapere che causare un guasto a un aereo non è il modo giusto per evitare che una persona sgradita si presenti al ristorante? Magari l'ha imparato venendo a conoscenza di alcuni passeggeri che hanno fatto lo stesso.[9] (Nel 2017 girava questa barzelletta. Jeff Bezos: "Alexa, comprami qualcosa da Whole Foods". Alexa: "Ok, compro la catena di supermercati Whole Foods").

Nel 2015, è stato scoperto che Volkswagen aveva truccato alcuni test per il controllo delle emissioni. L'azienda non aveva modificato i risultati, ma aveva progettato i computer di bordo delle proprie auto per barare. I suoi ingegneri avevano programmato il software per capire quando veniva testato, pertanto durante il test veniva attivato

il sistema di controllo delle emissioni, che veniva poi disattivato. Le performance su strada delle auto Volkswagen erano pertanto di livello superiore, peccato che – all'insaputa della Environmental Protection Agency (Epa) degli Stati Uniti – emettessero una quantità di ossido di azoto fino a quaranta volte superiore a quella consentita. In questo aneddoto non ci sono di mezzo AI – sono stati ingegneri umani a programmare dei normali computer per barare – ma ci fa capire comunque quale sia il problema. Volkswagen ha messo in atto questo trucchetto per più di dieci anni, sfruttando il fatto che i programmi informatici sono complessi e difficili da analizzare. Non è facile capire che cosa facciano, così come non è semplice guardare un'auto e comprendere come funzioni. Un hack del genere può funzionare a lungo, se i programmatori non vuotano il sacco. In questo caso, abbiamo scoperto quel che faceva Volkswagen grazie a un gruppo di scienziati della West Virginia University che ha testato le stesse auto su strada usando sistemi di rilevamento delle emissioni diversi da quelli dell'Epa. Il software era stato studiato appositamente per ingannare i sistemi Epa e così gli scienziati della West Virginia sono riusciti a misurare accuratamente le emissioni delle auto senza farsi "scoprire" dal software stesso.

Se vi chiedessi di progettare un software per il controllo del motore di un'automobile col fine di massimizzare la performance e superare comunque i test sulle emissioni, probabilmente non lo progettereste in modo fraudolento senza rendervene conto. Ma lo stesso non si può dire della AI, che non comprende istintivamente il concetto astratto di inganno. La AI penserà invece *outside the box*, in modo non scontato, proprio perché non sa nemmeno che cosa sia la "scatola" o quali limiti seguano le soluzioni trovate dagli esseri umani. Senza contare che a livello astratto non capisce neanche l'etica. Non capisce che il sistema di Volkswagen era dannoso e aggirava lo scopo del test sulle emissioni, e nemmeno che era illegale: per capirlo avrebbe dovuto essere addestrato con dati contenenti le leggi sulle emissioni. La AI può hackerare un sistema senza rendersene conto. Per via del problema della spiegabilità possiamo non accorgercene neanche noi.

A meno che i programmatori non ordinino esplicitamente al sistema di non cambiare il suo comportamento nel corso di un test,

una AI potrebbe architettare lo stesso trucchetto. I programmatori ne sarebbero soddisfatti. I contabili andrebbero in solluchero. E probabilmente nessuno se ne accorgerebbe. Certo, dopo lo scandalo Volkswagen, ormai studiato per filo e per segno, i programmatori possono decidere consapevolmente di mettersi al riparo da un simile hack. Ma non possiamo prevedere l'imprevedibile. Ricordiamoci del genio della lampada.

1. Potete trovare una serie di esempi in Victoria Krakovna (2 aprile 2018), "Specification gaming examples in AI", https://vkrakovna.wordpress.com/2018/04/02/specification-gaming-examples-in-ai.
2. Karol Kurach *et al.* (25 luglio 2019), "Google research football: A novel reinforcement learning environment", *arXiv*, https://arxiv.org/abs/1907.11180.
3. Ivaylo Popov *et al.* (10 aprile 2017), "Data-efficient deep reinforcement learning for dexterous manipulation", *arXiv*, https://arxiv.org/abs/1704.03073.
4. David Ha (10 ottobre 2018), "Reinforcement learning for improving agent design", https://designrl.github.io.
5. Dario Amodei *et al.* (25 luglio 2016), "Concrete problems in AI safety", *arXiv*, https://arxiv.org/pdf/1606.06565.pdf.
6. Custard Smingleigh (@Smingleigh) (7 novembre 2018), Twitter, https://twitter.com/smingleigh/status/1060325665671692288.
7. Abby Everett Jaques (2021), "The Underspecification Problem and AI: For the Love of God, Don't Send a Robot Out for Coffee", manoscritto inedito.
8. Stuart Russell (aprile 2017), "3 principles for creating safer AI", TED2017, www.ted.com/talks/stuart_russell_3_principles_for_creating_safer_ai.
9. Melissa Koenig (9 settembre 2021), "Woman, 46, who missed her JetBlue flight 'falsely claimed she planted a BOMB on board' to delay plane so her son would not be late to school", *Daily Mail*, www.dailymail.co.uk/news/article-9973553/Woman-46-falsely-claims-planted-BOMB-board-flight-effort-delay-plane.html; Ella Torres (18 gennaio 2020), "London man reports fake bomb threat to delay flight he was running late for: Police", *ABC News*, https://abcnews.go.com/International/london-man-reports-fake-bomb-threat-delay-flight/story?id=68369727; Peter Stubley(16 agosto 2018), "Man makes hoax bomb threat to delay his flight", *Independent*, www.independent.co.uk/news/uk/crime/man-late-flight-hoax-bomb-threat-gatwick-airport-los-angeles-jacob-meir-abdellak-hackney-a8494681.html; Reuters (20 giugno 2007), "Woman delays Turkish plane with fake bomb warning", www.reuters.com/article/us-turkey-plane-bomb-idUSL2083245120070620.

CAPITOLO 58

Come difenderci dagli hacker della AI

Gli hack più evidenti non ci preoccupano. Se il sistema di un'automobile a guida autonoma decide che il modo migliore per andare più veloce possibile è girare in tondo, i programmatori se ne accorgono e modificano di conseguenza la sua AI. Un veicolo che fa una cosa del genere non passerebbe mai il collaudo. Dobbiamo però tenere gli occhi aperti: ci sono hack dagli effetti più sfumati. Pensiamo ai motori di raccomandazione[1] – la prima generazione di hack delle AI – e a come siano in grado di spingerci verso i contenuti più estremi. Non era per questo che erano stati progettati: questa proprietà è emersa naturalmente con l'uso. I sistemi agivano, osservavano i risultati, e si modificavano di conseguenza, decidendo che era meglio rifare quelle cose che avevano aumentato il coinvolgimento degli utenti. Gli algoritmi di raccomandazione di YouTube e Facebook hanno imparato che i contenuti più estremi suscitano reazioni viscerali, che spingono le persone a passare più tempo su una piattaforma. Per attuare questo hack non è servita una persona malintenzionata: anche un sistema automatizzato piuttosto rudimentale è riuscito ad arrivarci da solo, mentre quasi nessuno di noi se ne accorgeva.

Allo stesso modo, nel 2015, una AI ha imparato da sola a giocare a Breakout, un videogioco degli anni Settanta. Alla AI non è stato detto niente delle regole e delle strategie che governavano il gioco. Le sono stati invece dati i controlli e l'istruzione che sarebbe stata ricompensata nel caso avesse ottenuto il punteggio più alto possibile. Non ci interessa che abbia imparato a giocare: nessuno si aspettava che non ci riuscisse. Molto più interessante è però che abbia scoperto, e ottimizzato come nessun umano era mai riuscito a fare, la tattica del *tunneling* attraverso una colonna di mattoncini per far rimbalzare la palla sul muro.

I ricercatori AI conoscono bene tutte queste cose, e in tanti stanno

cercando di capire come difendersi dal reward hacking e dall'hacking degli obiettivi. Una soluzione è quella di far capire i contesti alle AI. I ricercatori non devono preoccuparsi solo del problema del goal alignment, ma anche di quello del *value alignment*, l'allineamento di valori, per creare AI che rispecchino i valori umani. Le soluzioni possono prendere due direzioni opposte. Possiamo specificare esplicitamente i valori relativi a un contesto. Una soluzione già fattibile, ma che ci espone a tutti gli hacking appena descritta. Oppure possiamo creare AI in grado di apprendere i nostri valori, osservando come agiscono gli umani o desumendoli da tutto quel che abbiamo scritto, e che costituisce la nostra storia, letteratura, filosofia ecc. Potrebbero volerci molti anni, ma sarà probabilmente una caratteristica della AI generale. Gran parte delle ricerche attuali oscillano tra questi due estremi.

Possiamo immaginare facilmente quali problemi potrebbero derivare da una AI che si allinea da sola ai valori degli esseri umani osservandoli direttamente o studiandone la storia. Ai valori di chi dovrà rifarsi? A quelli di un uomo somalo? O a quelli di una donna di Singapore? Deve fare una media dei due, qualunque cosa significhi? I valori degli umani spesso si contraddicono, e molte volte noi stessi non li rispettiamo. I valori di un singolo individuo possono essere irrazionali, immorali o basati su convinzioni erronee. Storia, letteratura e filosofia sono piene di cose irrazionali, immorali o sbagliate. Non siamo sempre all'altezza dei nostri ideali.

Per difendersi dall'hacking, il modo più efficace è identificare le vulnerabilità e mettere delle patch prima che vengano sfruttate per sovvertire i sistemi. Le tecnologie AI possono esserci di grande aiuto, anche perché sono in grado di operare a velocità sovrumana. Pensiamo ai computer. Quando le AI saranno in grado di scovare nuove vulnerabilità nel software, le sfrutteranno tanto il governo quanto i criminali, fino ai semplici appassionati di hacking. Le potranno usare per compromettere le reti informatiche di tutto il mondo, mettendoci tutti in pericolo.

La stessa tecnologia però potrà aiutarci a difenderci, visto che una vulnerabilità, una volta scoperta, può essere sanata per sempre. Proviamo a immaginare come un'azienda di software potrebbe

implementare un rilevatore di vulnerabilità. Potrebbe inserirlo nel processo di sviluppo per individuare ed eliminare le vulnerabilità prima di mettere un software sul mercato. Attacco e difesa avrebbero a disposizione la stessa tecnologia, ma la difesa potrebbe impiegarla per rendere più sicuri i propri sistemi in modo permanente. Possiamo immaginare un futuro nel quale le vulnerabilità del software saranno acqua passata: "Vi ricordate agli albori dell'informatica, quando gli hacker sfruttavano le vulnerabilità di un sistema per hackerarlo? Che periodo assurdo…".

Naturalmente, il periodo di transizione non sarà facile. Magari in un primo tempo verrà messo al sicuro il nuovo codice, ma non il *legacy code*. Gli AI tool esamineranno il codice già in uso, al quale spesso non sarà possibile applicare patch. In casi del genere, saranno gli hacker a sfruttare a proprio vantaggio i rilevatori automatici di vulnerabilità. Nel lungo periodo, se ne avvantaggerà però soprattutto la difesa.

Lo stesso vale per quando le AI cominceranno a trovare hack nei sistemi sociali. Verranno alla luce vulnerabilità politiche, economiche e sociali, pronte a essere sfruttate nell'interesse di chi controlla tali AI. Le pubblicità su misura saranno più efficaci e ci sarà qualcuno pronto a pagare di più per servirsene. Le AI troveranno nuovi loophole nel sistema fiscale e lo faranno perché dietro ci sarà qualcuno desideroso di pagare meno tasse.

In genere l'hacking rafforza le strutture di potere preesistenti. La AI sarà una nuova freccia al loro arco, a meno che non impareremo a porre rimedio agli squilibri di potere meglio di come facciamo oggi.

Come nel caso precedente, le stesse tecnologie potranno essere però usate anche per difendersi.[2] Gli hacker AI troveranno magari migliaia di vulnerabilità nel sistema fiscale, ma con le AI si potrà evitare a priori che ci siano falle nelle nuove norme o proposte di legge. Tutto potrebbe cambiare. Immaginiamo di testare una nuova legge fiscale con questo sistema. Potrebbe farlo tanto un parlamentare, quanto un'organizzazione a difesa dei contribuenti o un giornalista. Certo, non significa automaticamente che tutto sarebbe risolto (ricordiamoci che mettere le patch alle vulnerabilità è tutt'altro problema), ma almeno se ne discuterebbe. In teoria,

pertanto, si potrebbero applicare le giuste patch prima che qualcuno se ne approfitti. Anche in questo caso, il periodo di transizione sarà rischioso, per via di tutte le leggi e regole passate. Ma ancora una volta, sul lungo periodo, le AI per scovare le vulnerabilità favoriranno la difesa.

Ci sono aspetti positivi e negativi in tutto questo. La società potrà usare le AI in modo che i potenti non hackerino i suoi sistemi, ma la conseguenza più probabile è un maggior controllo sociale. Sarà più difficile cambiare la società: non dimentichiamoci che la struttura di potere è sempre cruciale.

1. Zeynep Tufekci (10 marzo 2018), “YouTube, the great equalizer”, *New York Times*, www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html; Renee DiResta (11 aprile 2018), “Up next: A better recommendation system”, *Wired*, www.wired.com/story/creating-ethical-recommendation-engines.
2. Per esempio, Gregory Falco *et al.* (28 agosto 2018), “A master attack methodology for an AI-based automated attack planner for smart cities”, *IEEE Access* 6, https://ieeexplore.ieee.org/document/8449268.

CAPITOLO 59

Gli hacker AI del futuro

Possiamo immaginare un hacking interamente affidato alla AI? Dipende dal sistema.

Perché una AI cominci anche solo a ottimizzare una soluzione, o addirittura a svilupparne una nuova, è necessario formalizzare tutte le norme di un ambiente in modo comprensibile da un computer. Bisogna stabilire determinati scopi, che nel gergo dell'intelligenza artificiale sono dette "funzioni-obiettivo". La AI ha bisogno di una sorta di feedback sul suo operato per poter migliorare la propria performance. A volte è semplice. Pensiamo a un gioco come il Go. Regole, obiettivo e feedback – hai vinto o perso? – vengono specificati in modo preciso, e non c'è niente di esterno che possa creare confusione. La AI Gpt-3 può creare testi coerenti perché il suo "mondo" è fatto solo di testo. Ecco perché la maggior parte degli esempi di goal e reward hacking provengono da ambienti simulati. Sono artificiali e limitati, e tutte le norme vengono specificate alla AI.

Quel che conta è la quantità di ambiguità di un sistema. Possiamo immaginare di addestrare una AI con tutte le leggi fiscali del mondo, riconducibili a una serie di formule per determinare quante tasse bisogna pagare. Esiste perfino un linguaggio di programmazione, chiamato Catala, ottimizzato per scrivere le leggi. Ma la legge contiene comunque alcune ambiguità, che sono difficili da riprodurre in un codice: per la AI questo rappresenta un problema. Gli avvocati tributaristi non perderanno il lavoro tanto presto.

Gran parte dei sistemi umani sono perfino più ambigui. Difficile immaginare una AI in grado di inventarsi hack sportivi attuabili nel mondo reale come la curvatura dei bastoni da hockey. Una AI, per ideare una cosa del genere, non dovrebbe solo capire le regole del gioco, ma anche la fisiologia umana, l'aerodinamica di bastone e disco ecc. Non è impossibile, ma di certo è più difficile che inventare una nuova mossa per il gioco del Go.

L’ambiguità latente dei sistemi sociali complessi ci consente una difesa a breve termine contro l’hacking AI. La AI comincerà a inventare hack sportivi solo quando gli androidi cominceranno a praticarli, o quando verrà sviluppata una AI generale in grado di capire come si intersecano i diversi contesti del mondo reale. E lo stesso si può dire degli hack del gioco d’azzardo o del processo legislativo (una AI avrebbe potuto scoprire da sola il gerrymandering?). Passerà molto tempo prima che le AI possano simulare il modo in cui le persone lavorano, da sole e in gruppo, e riuscire pertanto a trovare nuovi modi per hackerare il processo legislativo.

Ma per quanto il problema di un mondo pieno di hacker AI sia ancora fantascientifico, vale comunque la pena di prenderlo in considerazione. Non è una stupidaggine. La AI sta progredendo a tutta velocità, con balzi sorprendenti e difficili da prevedere. Credevamo che alcuni progressi sarebbero stati facili, e invece tardano ad arrivare. Quando nei primi anni Ottanta andavo al college ci avevano detto che un computer non avrebbe mai imparato a giocare a Go: era troppo difficile, non tanto per una questione di regole, ma per l’enorme numero di mosse possibili. Oggi le AI sono invece in grado di giocare a Go a livello dei grandi maestri.

Per questo, anche se le AI potranno diventare un vero problema solo in futuro, dobbiamo preoccuparcene già oggi. Dobbiamo cominciare a cercare soluzioni etiche, applicabili e comprensibili, e dobbiamo sbrigarci: l’unica cosa certa della AI è la sua capacità di essere sempre più rapida delle nostre attese.

Se vogliamo andare a caccia di hack generati dalla AI, il posto migliore per cominciare è probabilmente il sistema finanziario, in quanto le sue regole sono state pensate perché fossero gestite in modo algoritmico. Gli algoritmi per il trading ad alta frequenza hanno anticipato quanto vedremo in futuro in forma molto più sofisticata. Possiamo immaginare di fornire a una AI tutte le informazioni finanziarie del mondo in tempo reale, oltre a tutte le leggi e regole a livello globale, più vari news feed e qualunque altra cosa ci possa sembrare rilevante, per poi ordinarle di ottenere “il massimo profitto legalmente lecito” o perfino “il massimo profitto

che ci permetta di farla franca". Non penso che manchi molto a una cosa del genere, e di certo ne scaturiranno nuovi hack di ogni sorta e del tutto inattesi.[1] Probabilmente alcuni di loro andranno oltre le nostre possibilità di comprensione, e pertanto non saranno mai scoperti. Sul breve termine, è più probabile che vedremo hack realizzati in collaborazione da AI e umani. Una AI potrà identificare una vulnerabilità sfruttabile, per affidarla alle "cure" di un contabile o un fiscalista molto esperto.

L'hacking è quasi sempre stato un'attività del tutto umana. Per cercare nuovi hack servono esperienza, tempo, creatività e fortuna. Tutto cambierà quando saranno le AI a darsi all'hacking. Le AI non dovranno sottostare ai limiti degli esseri umani. Non avranno bisogno di dormire. Penseranno in modo del tutto alieno. E hackereranno i sistemi come non possiamo ancora nemmeno immaginare.

Come ho detto nel capitolo 55, i computer hanno dato una spinta all'hacking su quattro dimensioni: velocità, scala, portata e complessità. La AI non farà che confermare queste tendenze.

Punto primo, la velocità. A volte gli umani impiegano mesi o anni per effettuare un hack, ma in futuro per la stessa cosa potranno volerci solo pochi giorni, ore o perfino secondi. Che succederà quando addestreremo una AI con l'intero sistema fiscale e le chiederemo di trovare tutti i modi per pagare meno tasse possibili? E nel caso una multinazionale sia in grado di analizzare e ottimizzare i sistemi fiscali di tutto il mondo? Una AI sarà in grado di capire, senza che le venga fornito l'apposito prompt, che è più conveniente fissare la propria ragione sociale in Delaware e registrare le consegne a Panama? Quante vulnerabilità – loophole – che non conosciamo sarà in grado di scoprire? Decine? Centinaia? Migliaia? Non lo sappiamo assolutamente, ma è probabile che nel giro di dieci anni lo scopriremo.

Punto secondo, la scala. Quando i sistemi AI cominceranno a scoprire gli hack, li sfrutteranno a una scala per la quale non siamo pronti. Se prenderanno di mira i sistemi finanziari, inevitabilmente ne domineranno il settore. Già oggi il mercato creditizio, le leggi fiscali e la legge in genere favoriscono i più ricchi. La AI accentuerà

questa disparità. Non saranno ricercatori con buone intenzioni a sviluppare le prime AI in grado di hackerare la finanza con scopo di lucro, ma grandi banche internazionali, hedge fund e consulenti manageriali.

In terzo luogo, la portata: alcuni sistemi sociali sono abituati ad avere a che fare con gli hack, ma hanno imparato a farlo quando gli hacker erano umani e gli hack avevano ritmi umani. Non disponiamo di alcun sistema di governance in grado di rimediare rapidamente allo sfruttamento di centinaia o migliaia di loophole fiscali appena scoperti. Non siamo in grado di mettere patch con una simile velocità. Non abbiamo saputo impedire che Facebook venisse usato per hackerare la democrazia; proviamo a immaginare come potrebbe sfruttarlo una AI. Se le AI cominceranno ad architettare hack legali e imprevisti del sistema finanziario, per l'economia mondiale potrebbero esserci conseguenze burrascose, dalle quali riprendersi non sarà né rapido né indolore.

Infine, la complessità: gli hack AI permettono strategie complesse che vanno ben oltre quel che la mente umana è in grado di immaginare senza ausili esterni. Le complesse analisi statistiche delle AI possono rivelare rapporti tra variabili sfuggiti anche ai migliori esperti, consentendo di attuare strategie in grado di sovvertire su molteplici livelli il sistema-target. Ad esempio, una AI progettata per massimizzare le percentuali di un partito politico potrebbe individuare la giusta combinazione tra variabili economiche, strategie di campagna elettorale e sfruttamento del sistema di voto, influendo sull'esito delle elezioni quel tanto che basta per trasformare una sconfitta in una vittoria; sarebbe una rivoluzione in grado di estendere all'intera democrazia le innovazioni che un software di mappatura può introdurre nel gerrymandering. Per non parlare dei trucchetti quasi impossibili da scovare che una AI potrebbe consigliarci per manipolare il mercato azionario, il sistema legislativo o l'opinione pubblica.

Con la velocità, la scala, la portata e la complessità consentite dai computer, l'hacking potrebbe diventare un problema ingestibile per la società. In una scena di *Terminator*, Kyle Reese descrive a Sarah Connor il cyborg che le sta dando la caccia: "Non si può patteggiare

con lui. Non si può ragionare con lui. Non conosce pietà, né rimorso, né paura. [...] Non si fermerà mai". Non abbiamo a che fare con veri e propri assassini cyborg, ma se la AI diverrà un hacker ostile, avremo molte difficoltà a tenere il passo della sua capacità inumana di riscontrare vulnerabilità nei sistemi.

Ci sono studiosi di AI preoccupati dalla possibilità che le intelligenze artificiali si liberino dei limiti imposti loro dagli esseri umani e prendano il dominio della società. Possono sembrare congetture assurde, ma non possiamo del tutto ignorare uno scenario simile.

Oggi e nell'immediato futuro, saranno però le persone più potenti ad attuare il tipo di hacking che stiamo descrivendo, a discapito delle persone comuni. Tutte le AI che ci circondano, sul nostro personal computer, online, o sotto forma di robot, sono programmate da qualcuno, in genere per fare i suoi interessi e non i nostri. Per quanto device connessi a internet come Alexa possano fingere di essere nostri amici fidati, non dimentichiamoci che sono stati ideati per venderci prodotti Amazon. Proprio come Amazon ci spinge a comprare i suoi prodotti e non quelli della concorrenza, anche quando sono di miglior qualità, Alexa non darà sempre la priorità a quel che è meglio per noi. Hackererà la nostra fiducia in Amazon per arricchire i suoi azionisti.

In mancanza di regolamenti significativi, possiamo fare ben poco per prevenire l'hacking delle AI. Dobbiamo accettarlo come inevitabile, e dar vita a solide strutture di controllo in grado di reagire in modo rapido ed efficace, normalizzando gli hack benefici come parte del sistema e neutralizzando quelli nocivi, che lo siano volutamente o meno.

È una sfida che ci pone questioni ancor più complesse su come la AI si evolverà e come le istituzioni potranno fronteggiarla: quali hack sono benefici? Quali sono nocivi? Chi lo decide? Se siete a favore di uno Stato poco invasivo, probabilmente approverete quegli hack in grado di ridurre il suo controllo sui cittadini. Potreste però temere un passaggio di consegne del potere dai politici ai signori della tecnologia. Se siete fautori del principio di precauzione,[2] auspicherete l'intervento di esperti che mettano alla prova i nuovi

hack prima di incorporarli nei nostri sistemi sociali, estendendo magari il principio anche a istituzioni e strutture che hanno reso possibili quegli hack.

Una domanda tira l'altra. Gli hack creati dalla AI dovranno essere governati a livello locale o globale? Saranno governati tramite un organo amministrativo o affidandosi a delle consultazioni popolari? Dobbiamo far decidere al mercato o alla società civile? (Il modo in cui stiamo applicando agli algoritmi i modelli di governance sembra indicarci il futuro). Le strutture di governo che progettiamo consegneranno a certe persone e organizzazioni il potere di decidere quali hack contrassegneranno il nostro futuro. Dobbiamo assicurarci che quel potere venga esercitato in modo saggio.

1. Hedge fund e società d'investimento stanno già utilizzando le AI per decidere come investire. Luke Halpin e Doug Dannemiller (2019), "Artificial intelligence: The next frontier for investment management firms", *Deloitte*, www.deloitte.com/content/dam/assets-shared/legacy/docs/perspectives/2022/fsi-artificial-intelligence-investment-mgmt.pdf; Peter Salvage (marzo 2019), "Artificial intelligence sweeps hedge funds", BNY Mellon, www.bnymellon.com/us/en/insights/all-insights/artificial-intelligence-sweeps-hedge-funds.html.

2. Maciej Kuziemski (1° maggio 2018), "A precautionary approach to artificial intelligence", *Project Syndicate*, www.project-syndicate.org/commentary/precautionary-principle-for-artificial-intelligence-by-maciej-kuziemski-2018-05.

CAPITOLO 60

I sistemi di governance dell'hacking

Le AI non sono ancora abbastanza sviluppate per usarle come unica difesa dall'hacking AI. È necessario invece collaborare alla creazione di strutture governative in grado di guidarci nello sviluppo e nell'impiego di questa tecnologia.

Non sappiamo però ancora come dovranno essere queste strutture, per quanto siano state avanzate diverse proposte normative. Lo scopo è affrontare i problemi posti da velocità, scala, portata e complessità consentite dalle intelligenze artificiali. Esperti e imprenditori del settore AI[1] come Nick Grossman hanno proposto che internet e le aziende basate sui big data passino dal paradigma "Regulation 1.0", che permette ogni innovazione senza richiedere alcuna assunzione di responsabilità per le eventuali conseguenze, a un paradigma "Regulation 2.0", che sottoponga le imprese a limiti e controlli rigorosi. Nel capitolo 33 abbiamo visto quale sia il miglior sistema di governance per gli hack diretti alla nostra società: un sistema di tribunali, giudici, giurie e precedenti in continua evoluzione basato sulla common law. In futuro, ogni sistema di governance per la gestione della AI dovrà essere rapido, inclusivo, trasparente e agile, come ogni buon sistema di governance moderno.

Possiamo provare a tracciare le linee di un sistema di governance in grado di difenderci dagli effetti potenziali di hack AI voluti o non voluti (in genere odio gli acronimi superflui, ma lasciate che per snellire il discorso nei prossimi paragrafi usi la sigla Hgs per abbreviare l'espressione *hacking governance system*):

– *Velocità*: la cosa fondamentale è che per tenere il passo delle accelerazioni di tecnologia e cambiamenti della società, ogni Hgs operi in modo rapido ed efficace. Quando si parla di innovazioni tecnologiche, spesso viene evocato il dilemma di Collingridge: quando una novità dirompente si è diffusa al punto che le sue conseguenze sociali sono evidenti è troppo tardi per regolarla.[2] Da

quella nuova tecnologia dipendono troppe vite, troppi posti di lavoro, e rimettere il genio nella lampada è impossibile. È un'idea insensata – l'edilizia, le ferrovie, l'alimentazione, la medicina, le fabbriche, la chimica o l'energia nucleare dimostrano il contrario – ma di certo una cosa già radicata è più difficile da regolare. Gli hack procederanno più rapidamente di quanto i governi potranno cambiare leggi e regolamenti e il passaggio dalla teoria alla pratica non farà che complicare le cose. Idealmente, un Hgs dovrebbe essere in grado di agire più velocemente di quanto un hack possa diffondersi, e sapere in men che non si dica se dovrà accompagnare quell'hack fino alla maturazione o piuttosto soffocarlo nella culla.

– *Inclusività*: per capire se un hack è benefico o nocivo, specialmente agli inizi, un Hgs dovrà includere quante più prospettive possibili, per assicurarsi di non trascurare nessuna potenziale minaccia o beneficio. Dovrà pertanto includere come minimo un team multidisciplinare molto differenziato al suo interno, in grado di esaminare gli hack da ogni punto di vista, dalla sociologia al diritto, dall'economia al design thinking o all'ecologia. Un Hgs così strutturato dovrà inoltre cercare di incorporare in modo dinamico gli input dei gruppi più marginali, in particolare delle comunità con meno rappresentanza, ma anche di ricercatori ed esperti indipendenti, accademici, sindacati, associazioni di commercianti, amministrazioni locali e gruppi della società civile. Tutti questi soggetti dovranno esprimere la loro opinione non solo nel corso di singoli incontri, ma in un dialogo continuo tra loro e con i membri dell'Hgs, in modo che le decisioni dell'Hgs al tempo stesso derivino dal dibattito pubblico e aiutino l'opinione pubblica a chiarirsi le idee. Di conseguenza, l'attivismo e le lobby potrebbero influenzare le decisioni sugli hack di politici e altri decisori esterni all'Hgs.

– *Trasparenza*: Per includere nel proprio processo decisionale il parere di esperti e società civile, l'Hgs dovrà procedere e deliberare[3] in modo pubblico e trasparente. Un Hgs opaco, aperto solo a insider e persone più competenti, taglierebbe fuori il feedback sociale necessario a capire effetti primari e collaterali degli hack. Un Hgs trasparente nelle procedure e nelle decisioni sarà invece in grado di guadagnarsi la fiducia dei cittadini, un consenso fondamentale per

avere sostegno dalla politica al momento di trovare il difficile equilibrio tra innovazione, stabilità e valori di contesto come l'equità e la correttezza.

– *Agilità*: infine, ricordiamoci che i cittadini possono cambiare orientamento politico, un hack al quale è stato dato il via libera può avere conseguenze disastrose, e studiosi e governo possono trovare modi più efficaci di regolamentare un hack; di conseguenza, ogni Hgs dovrà essere dotato dei mezzi per far evolvere rapidamente le proprie strutture, competenze e decisioni. Anche quando si hanno a disposizione gli input e le informazioni migliori, i sistemi sociali restano complessi e difficili da prevedere, e non sempre si riesce a bloccare gli hack sociali più nocivi. Quando l'Hgs troverà una patch efficace o qualche altro tipo di meccanismo di difesa, è possibile che gli hacker saranno già al lavoro su uno stratagemma per contrattaccare. Un Hgs dovrà pertanto agire secondo un modello iterativo: imparare subito dai propri errori, testare gli approcci migliori per controllare e incorporare gli hack sociali, migliorare costantemente per implementare le più efficaci tra le nuove pratiche.

In generale, sarà necessario che ogni cittadino divenga più consapevole del ruolo della tecnologia nelle nostre vite. Finora abbiamo accettato che i programmatori codificassero il mondo a loro piacimento. L'abbiamo fatto per molti motivi: non volevamo rallentare le nuove tecnologie, i legislatori non le capivano abbastanza da poterle regolare e soprattutto non se ne curavano. Le cose sono però cambiate. I sistemi informatici non influenzano più solo il mondo dei computer. Gli ingegneri che decidono come dovrà essere un computer, di fatto tratteggiano il futuro del mondo.

Un sistema giudiziario basato sulla common law è un buon punto di partenza. Non voglio minimizzare la tensione tra democrazia e tecnologia, ma non è vero che tutti possano capire la AI o contribuire a regolamentarla. D'altro canto, come scegliere tecnocrati affidabili, e come essere certi che tale fiducia sia condivisa? È un problema più ampio, e di difficile soluzione, che riguarda la governance del nostro mondo, così ricco di informazioni, così connesso e tecnologico. Un

problema che esula la portata di questo libro. Ed è anche un problema profondamente diverso dalla creazione di strutture di governo in grado di operare alla velocità dell'era dell'informazione a dispetto della sua complessità. Studiosi di diritto come Gillian Hadfield,[4] Julie Cohen,[5] Joshua Fairfield[6] e Jamie Susskind[7] si stanno occupando di questo problema generale, e di certo c'è ancora molto da fare.

Per arrivare a una soluzione, anche in questo caso, bisognerà per prima cosa affrontare alcuni problemi fondamentali della nostra società. In altre parole: un hacking tentacolare e aggressivo è sintomo di un sistema fragile. I soldi danno il potere: quando un ricco infrange le regole non deve sottostare alla stessa giustizia di un povero. Se chi deve attuare le leggi non agisce in modo equo – pensiamo a quanto di rado vengano perseguiti i crimini delle grandi aziende – chi è potente non ha motivo per seguire le regole, e di conseguenza la fiducia della società nel sistema e nelle sue regole cola a picco.

Queste ingiustizie hanno effetti considerevoli. Le imprese e gli individui più privilegiati sono sottoposti a così poche regole da poter determinare in prima persona le scelte politiche, sostituendosi di fatto ai governi. Di conseguenza, le persone comuni non hanno più voce in capitolo e la democrazia muore. Forse sto estremizzando, ma non possiamo trascurare questa possibilità. Ho descritto l'interazione tra umani e sistemi informatici, e i rischi che sorgono quando i computer cominciano a svolgere il ruolo delle persone. Anche in questo caso, ci troviamo di fronte a un problema più vasto di quello degli usi propri e impropri delle AI, del quale si stanno già occupando futurologi ed esperti di tecnologia. È semplice affidarsi alla tecnologia perché ci conduca nel futuro, ma come cittadini dovremmo decidere collettivamente quale ruolo affidarle, soprattutto in un mondo nel quale sarà a disposizione di tutti.

Oggi nel mondo non esiste alcun Hgs, e nessun governo sta pensando di crearne uno. È il momento di darsi da fare.

1. Nick Grossman (8 aprile 2015), “Regulation, the internet way”, Data-Smart City Solutions, Harvard University, https://datasmart.ash.harvard.edu/news/article/white-paper-regulation-the-internet-way-660.
2. Adam Thierer (16 agosto 2018), “The pacing problem, the Collingridge dilemma and technological determinism”, *Technology Liberation Front*, https://techliberation.com/2018/08/16/the-pacing-problem-the-collingridge-dilemma-technological-determinism.
3. Stephan Grimmelikhuijsen *et al.* (gennaio 2021), “Can decision transparency increase citizen trust in regulatory agencies? Evidence from a representative survey experiment”, *Regulation and Governance* 15, n. 1, https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12278.
4. Gillian K. Hadfield (2016), *Rules for a Flat World: Why Humans Invented Law and How to Reinvent It for a Complex Global Economy*, Oxford University Press.
5. Julie E. Cohen (2019), *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press.
6. Joshua A.T. Fairfield (2021), *Runaway Technology: Can Law Keep Up?*, Cambridge University Press.
7. Jamie Susskind (2022), *The Digital Republic: On Freedom and Democracy in the 21st Century*, Pegasus.

Conclusioni

Nell'estate del 2022, mentre finivo di scrivere questo libro, mi sono imbattuto in un articolo del *Wall Street Journal* su un nuovo hack finanziario. Chi importa merci deve pagare al governo una tariffa, spesso molto alta. Esiste però un loophole,[1] la *de minimis rule*, pensata per consentire ai turisti americani di portare a casa qualche souvenir dai viaggi all'estero. Oggi gli importatori abusano di questa norma, facendo consegnare le merci provenienti dai Paesi stranieri direttamente ai clienti. "Di conseguenza, se dieci anni fa meno dell'1% delle importazioni di beni di valore dalla Cina si serviva della regola *de minimis*, oggi siamo arrivati a più del 10%". L'impatto sul gettito fiscale di questo hack è di 67 miliardi di dollari l'anno.

È facile scoraggiarsi pensando a tutti questi hack. Ci sembrano inevitabili. L'impressione è che da sempre i sistemi sociali vengano sovvertiti a vantaggio di pochi. A stento riusciamo a difenderci, e le armi a nostra disposizione sembrano del tutto inadeguate per affrontare il futuro: di certo, infatti, l'hacking della società non farà che peggiorare.

L'hacking è essenzialmente questione d'equilibrio. Da un lato innesca l'innovazione, dall'altro sovverte i sistemi, rafforza lo squilibrio di potere e può danneggiare la società. Per gran parte della nostra storia, possiamo dire che sia valsa la pena di rischiare per rinnovare. Certo, pochi privilegiati hanno hackerato i sistemi a loro vantaggio, ma del resto stavano già giocando con carte truccate, un po' di hacking non cambiava niente.

Oggi, questo equilibrio sta cambiando per due diverse ragioni, una culturale e una tecnologica.

Osserviamole più da vicino, iniziando da quella culturale. Sul lungo periodo – ragionando in termini di secoli – le nostre società sono in genere diventate più equilibrate, democratiche e giuste. L'hacking è diventato pertanto una scappatoia sempre più allettante per individui e gruppi privilegiati che volevano sovvertire il sistema a proprio vantaggio. In un sistema autocratico, un potente può infatti

ottenere quel che vuole senza ricorrere a troppi sotterfugi. Chi fa e disfa le regole senza pagarne le conseguenze non ha certo bisogno dell'hacking, che diventa invece un'opzione stuzzicante quando i sistemi economico, sociale e politico mettono i bastoni tra le ruote.

Non posso comprovarlo, ma ritengo che sia proprio a causa di questa dinamica che negli ultimi decenni l'hacking si sia tanto diffuso. È così che spiego il "capitalismo dell'ultima fase" e tutti i problemi che ne conseguono: la strada più facile, al giorno d'oggi, è scovare i loophole nei regolamenti. Quando chi dispone di mezzi e tecnologie si è reso conto di poter arricchirsi hackerando il sistema, ha investito sulle risorse e le competenze necessarie: ha imparato a sfruttare le vulnerabilità, a hackerare le gerarchie per il proprio tornaconto, a far normalizzare e legalizzare i propri hack, fino a vederli adottati dal sistema. Le disparità di reddito non hanno fatto che peggiorare la cosa. Secondo l'economista Thomas Piketty, la diseguaglianza produce un surplus di risorse per i vincitori,[2] un surplus che si può mobilitare per creare ulteriore diseguaglianza. Gran parte di quella mobilitazione consiste nell'hacking. Oggi sempre più persone dispongono delle competenze e delle risorse – e di conseguenza del potere – per hackerare il sistema. I nostri sistemi sociali subiscono il sovraccarico di hack raffazzonati, dovuti ad anni e anni di scontri per ottenere prestigio e potere. Cloud computing, media virali e AI rendono i nuovi hack sempre più accessibili e potenti, con una crescita apparentemente esponenziale di instabilità e innovazione. Per quanto le persone che se ne servono siano sempre di più, ad avvantaggiarsene sono soprattutto coloro che li ideano e li controllano.

I sistemi sociali si fondano sulla fiducia, che viene messa a dura prova dall'hacking. Se su scala ridotta il crollo della fiducia non ha poi grandi conseguenze, su larga scala può minare il funzionamento dell'intera società. Un loophole fiscale che avvantaggia solo i più ricchi crea risentimento ed erode la fiducia dell'opinione pubblica nei confronti dell'intero sistema fiscale. Siamo investiti da uno tsunami di hack, che riflettono l'attuale mancanza di fiducia, di coesione sociale e di impegno civile.

La seconda ragione è tecnologica. Certo, i nostri sistemi sociali nel

corso dei secoli sono divenuti più equi, ma il progresso non è sempre giusto o lineare. Vista da lontano la sua curva sembra in crescita costante, ma con uno sguardo più ravvicinato si nota un gran numero di alti e bassi. È un processo "rumoroso", e la tecnologia cambia la quantità di rumore. Le oscillazioni si fanno sempre più estreme, e per quanto possano non influenzare la traiettoria complessiva, hanno un impatto enorme sulle nostre vite quotidiane. È per la stessa ragione che il Ventesimo secolo è stato – statisticamente – il più pacifico della storia dell'umanità, anche se è stato teatro delle più cruente tra le guerre. Potevamo ignorare questo rumore solo quando non rischiavamo danni fatali su larga scala, vale a dire fin quando una guerra non era potenzialmente in grado di uccidere l'umanità intera oppure si limitava a coinvolgere persone e Paesi dei quali l'Occidente non si preoccupava poi molto. Oggi non ne siamo più tanto certi. Ci troviamo infatti a fronteggiare un rischio esistenziale senza precedenti. La tecnologia ingigantisce ogni cosa, e permette a danni di breve termine di trasformarsi in un danno sistemico a lungo termine. Per più di mezzo secolo abbiamo vissuto con lo spauracchio di una guerra atomica. I viaggi aerei internazionali hanno consentito a piccoli focolai locali di generare la pandemia di Covid-19, a causa della quale abbiamo perso milioni di vite umane e miliardi di dollari, con conseguenze sempre più negative per la stabilità di politica e società. Se la Terra del futuro sarà molto meno ospitale lo dovremo anche al sommarsi di cicli di retroazione e punti critici con gli effetti della tecnologia sull'atmosfera. Un singolo hack è oggi in grado di influenzare l'intero pianeta. Secondo il sociobiologo Edward O. Wilson, il problema di fondo dell'umanità è che "abbiamo emozioni paleolitiche, istituzioni medievali e una tecnologia divina".[3] Ricordate l'hack di Volkswagen per truccare i risultati ai test sull'emissione di carbonio? Se troppe aziende facessero lo stesso, la temperatura globale potrebbe salire di due gradi Celsius, rendendo impossibile la vita sulla Terra. Oppure possiamo immaginare un gruppo terroristico dell'apocalisse che hackera le strutture di comando per il lancio dei missili nucleari o attua un bio-hack per diffondere una nuova malattia. La gente morirebbe in massa, i governi crollerebbero e si innescherebbe una

spirale discendente in grado di interrompere la lunga e dolorosa marcia dell'umanità.

È per questi due motivi che oggi l'hacking rappresenta un rischio esistenziale. Possiamo hackerare sempre di più, sempre meglio, sempre più velocemente. I sistemi sociali e tecnologici si stanno trasformando in campi di battaglia in perenne mutazione, dove si fronteggiano atti sovversivi e tentativi di controffensiva. Considerando che chi è in cima alla catena alimentare potrà sempre contare su un bias a proprio favore, e che da questa tensione deriverà una nuova instabilità, saremo tutti noi a fare le spese di queste nuove forme di hacking.

Penso però che ci siano anche buoni motivi per essere ottimisti. I progressi tecnologici che hanno fatto evolvere l'hacking sono potenzialmente anche in grado di rendere il mondo un posto migliore, aiutandoci a difenderci dagli hack nocivi e scovando e diffondendo quelli benefici. Tutto sta nello scegliere il giusto sistema di governance. Difficile però farlo in fretta. Trasformare gli hack – quelli di oggi, generati dagli esseri umani, e quelli di domani, generati dalle AI – in innovazione sociale significa separare gli hack buoni da quelli cattivi, per far crescere i primi e limitare i secondi. È un compito che va ben oltre le difese dagli hack che ho descritto nel capitolo 2. Implica sistemi di governance in grado di tenere il passo di un cambiamento rapido e di soppesare interessi contrastanti e rischi, benefici e potenziale di ogni hack.

Dobbiamo dar vita a strutture di governance resilienti che possano rispondere agli hack in modo rapido ed efficace. Se impiegheremo anni ad applicare le patch necessarie alla legislazione fiscale, o se consentiremo a un hack legislativo di radicarsi al punto di essere irremovibile, tutto sarà vano. È essenziale che le regole e le leggi della società siano riparabili come i nostri computer e telefoni. In futuro, se non riusciremo ad hackerare l'hacking, a mantenerne i benefici limitandone costi e ingiustizie, la nostra stessa sopravvivenza sarà a rischio.

1. Josh Zumbrun (25 aprile 2022), “The $67 billion tariff dodge that’s undermining U.S. trade policy”, *Wall Street Journal*, www.wsj.com/articles/the-67-billion-tariff-dodge-thats-undermining-u-s-trade-policy-di-minimis-rule-customs-tourists-11650897161.
2. Thomas Piketty (2013), *Le Capital au XXIe siècle*, Seuil (ed. it. *Il capitale nel XXI secolo*, Bompiani 2014).
3. Tristan Harris (5 dicembre 2019), “Our brains are no match for our technology”, *New York Times*, www.nytimes.com/2019/12/05/opinion/digital-technology-brain.html.

Ringraziamenti

Questo libro è nato in un periodo di pandemia e grandi sconvolgimenti personali e ha risentito di entrambe le cose. Dopo aver scritto 86mila parole nel 2020, l'anno seguente le ho messe da parte – a costo di mancare la data di consegna – per ricominciare a scrivere solo nel 2022, quando, con l'aiuto di Evelyn Duffy di Open Boat Editing, ho tagliato 20mila parole e ho riorganizzato l'intero libro nella sessantina di brevi capitoli che avete appena letto (o almeno spero).

In questi due anni, moltissime persone mi hanno aiutato. Voglio ringraziare i miei assistenti di ricerca: Nicholas Anway, Justin DeShazor, Simon Dickson, Derrick Flakoll, David Leftwich e Vandinika Shukla, tutti studenti della Harvard Kennedy School che hanno collaborato con me per qualche mese, durante l'estate o per un intero semestre.

Ross Anderson, Steve Bass, Ben Buchanan, Nick Couldry, Kate Darling, Jessica Dawson, Cory Doctorow, Tim Edgar, FC (detto "freakyclown"), Amy Forsyth, Brett Frischmann, Bill Herdle, Trey Herr, Campbell Howe, David S. Isenberg, Dariusz Jemielniak, Richard Mallah, Will Marks, Aleecia McDonald, Roger McNamee, Jerry Michalski, Peter Neumann, Craig Newmark, Cirsten Paine, David Perry, Nathan Sanders, Marietje Schaake, Martin Schneier, James Shires, Erik Sobel, Jamie Susskind, Rahul Tongia, Arun Vishwanath, Jim Waldo, Rick Wash, Sara M. Watson, Tarah Wheeler, Josephine Wolff e Ben Wizner hanno letto il libro in una delle sue varie versioni, aiutandomi con commenti ai quali ho – quasi sempre – dato retta. Kathleen Seidel ha rivisto il libro nei minimi dettagli, come la mia storica assistente e copyeditor Beth Friedman.

Grazie al mio editor, Brendan Curry, e a tutto il personale della Norton che mi ha dato una mano a trasformare un manoscritto in un prodotto finito. Grazie anche alla mia agente, Sue Rabiner. Un ringraziamento anche alla mia nuova comunità, qui a Cambridge: alla Harvard Kennedy School, al Berkman Klein Center, a Inrupt (e al

progetto Solid), e a tutti i miei amici e colleghi. E infine a Tammy: grazie di tutto.