THE IMAGE BANK/GETTY

La corsa sfrenata a mettere internet in tutte le cose

Fahrad Manjoo, The New York Times, Stati Uniti

Automobili, serrature, lenti a contatto, vestiti, tostapane, frigoriferi, acquari, giocattoli, lampadine: gli oggetti d'uso quotidiano sono pronti a diventare "intelligenti"

Più di quarant'anni fa Bill Gates e Paul Allen fondarono la Microsoft con l'idea di portare un computer su ogni scrivania. Nessuno li prese sul serio, di conseguenza pochi cercarono di fermarli. Così, prima che qualcuno potesse accorgersene, il danno era fatto: non c'era quasi più nessuno che non avesse il sistema operativo Windows, e i governi dovettero affrontare il difficile compito di arginare il monopolio della Microsoft. È una storia che si ripete spesso nell'industria della tecnologia. Pionieri audaci puntano un obiettivo irraggiungibile (Mark Zuckerberg vuole connettere tutti) e il fatto che i loro piani siano improbabili gli permette di agire indisturbati. Quando poi ci rendiamo conto delle conseguenze delle loro azioni sulla società è troppo tardi per tornare indietro.

Sta succedendo di nuovo. Negli ultimi anni le grandi aziende hanno messo gli occhi su un nuovo obiettivo. Promettono vantaggi straordinari e benefici inimmaginabili per la nostra salute e la nostra felicità. C'è solo un piccolo inconveniente, di cui non parlano quasi mai: se le loro innovazioni si diffonderanno senza l'intervento o la supervisione dei governi, rischiamo di esporre il mondo a una serie di attacchi alla sicurezza e alla privacy. E indovinate un po'? Nessuno sta facendo molto per evitarlo. Il nuovo obiettivo del settore tecnologico non è mettere un computer su ogni scrivania, ma qualcosa di più ambizioso: mettere un computer dentro ogni cosa.

Automobili, serrature di casa, lenti a contatto, vestiti, tostapane, frigoriferi, robot industriali, acquari, giocattoli sessuali, lampadine, spazzolini da denti, caschi per le moto: questi e altri oggetti di uso quotidiano sono tutti pronti a diventare "intelligenti". Centinaia di piccole startup stanno contribuendo a realizzare questo obiettivo, che il linguaggio del marketing ha ribattezzato "internet delle cose". Ma come sempre succede nel mondo della tecnologia, il movimento è capeggiato da giganti come Amazon, Apple e Samsung.

Ciberufficio nazionale

A settembre Amazon ha presentato un forno a microonde che risponde ai comandi vocali di Alexa, il suo assistente digitale. Il forno costerà sessanta dollari, ma Amazon metterà in vendita separatamente anche il microchip che connette il forno all'assistente vocale. In questo modo altre aziende po-

tranno usare la connettività di Alexa per i loro elettrodomestici, come ventilatori, tostapane e caffettiere. E questa settimana Facebook e Google hanno presentato i loro *hub* domestici, che permettono di guardare video e fare altri trucchi digitali con un comando vocale.

Molti di questi apparecchi potrebbero essere liquidati come sciocchezze destinate a fallire. Ma tutte le invenzioni tecnologiche più importanti all'inizio sembravano una cosa da poco, e le statistiche dimostrano che il mercato dell'internet delle cose sta crescendo velocemente. È quindi più prudente prepararsi al peggio, ovvero al fatto che la digitalizzazione di ogni cosa non è solo possibile ma probabile, e che è arrivato il momento di rendersi conto del pericolo.

"In genere non sono pessimista, ma di questi tempi è difficile non esserlo", ha detto Bruce Schneier, un consulente alla sicurezza autore del libro *Click here to kill everybody* (Clicca qui per uccidere tutti). Secondo Schneier, gli interessi economici e tecnici del settore dell'internet delle cose non coincidono con quelli della privacy e della sicurezza. Mettere un computer in ogni cosa significa trasformare il mondo intero in una minaccia alla sicurezza informatica. Dopo le falle e i sabotaggi che hanno colpito Facebook e Google nelle ultime settimane, è chiaro che anche le grandi aziende devono fare i conti con il problema della sicurezza. In un mondo robotizzato un attacco hacker non metterebbe in pericolo solo i nostri dati, ma anche le nostre case, le nostre vite e perfino la sicurezza nazionale.

Schneier è convinto che solo l'intervento dei governi può salvarci da questo scenario. Auspica un ripensamento del sistema che regola la sicurezza informatica, qualcosa di simile alla riforma del sistema di sicurezza nazionale che il governo statunitense fece dopo gli attentati dell'11 settembre 2001.

Inoltre sostiene la necessità di una nuova agenzia federale negli Stati Uniti, il National cyber office, che dovrebbe studiare, spiegare e coordinare una risposta alla minacce poste dall'onnipresenza di internet. "Non mi viene in mente nessun settore che negli ultimi cento anni abbia migliorato la sua sicurezza senza che lo stato lo abbia obbligato a farlo", ha scritto. Ma ammette anche che un intervento pubblico è improbabile. "Nella nostra società, dove tutti danno per scontato che lo stato deve intervenire il meno possibile, non vedo chi potrebbe limitare le tendenze espansionistiche delle grandi aziende", sostiene. Queste tendenze sono ormai evidenti. In passato era difficile connettere a internet i dispositivi domestici, ma negli ultimi anni i costi e le difficoltà tecniche si sono notevolmente ridotti. Microcomputer come Arduino possono essere usati per rendere "smart" praticamente ogni oggetto domestico. Sistemi come quello proposto da Amazon promettono di accelerare ulteriormente lo sviluppo dell'internet delle cose.

A corto di popcorn

In una conferenza stampa organizzata a settembre, un ingegnere di Amazon ha mostrato con quale facilità un produttore di ventilatori potrebbe crearne uno che sfrutta le caratteristiche del microchip di Amazon, noto come Alexa connect kit. Il kit, che Amazon sta testando insieme ad alcune aziende produttrici, verrebbe collegato al sistema di controllo del ventilatore durante l'assemblaggio. Il produttore dovrebbe anche scrivere alcune linee di codice: nel caso del ventilatore, appena mezza pagina.

Questi dispositivi non hanno gli stessi standard di sicurezza a cui siamo abituati

Non serve altro. Gli elementi digitali del ventilatore (compresa la sicurezza e l'archiviazione nel cloud) sono tutti gestiti da Amazon. Se viene comprato su Amazon, il ventilatore si connette immediatamente con la rete domestica e comincia a ubbidire agli ordini impartiti all'assistente digitale. Basta collegarlo e accenderlo.

Tutto questo sembra confermare la tesi di Schneier, ovvero che il costo di aggiungere una dimensione informatica agli oggetti sarà così basso che per i produttori risulterà logico collegare ogni tipo di dispositivo a internet. In alcuni casi porterà dei vantaggi, per esempio sarà possibile ordinare al microonde di scaldare il pranzo. A volte porterà opportunità di guadagno: il microonde di Amazon ordinerà per noi i popcorn quando cominceranno a finire.

A volte questi apparecchi sono usati per scopi commerciali o di sorveglianza, come i televisori smart che tracciano quello che guardiamo per vendere pubblicità. Anche se i vantaggi sono limitati, creano una certa logica di mercato. Prima o poi – e non manca molto – gli oggetti che non si connettono a internet saranno meno numerosi di quelli in grado di farlo.

Il problema, tuttavia, sarà che il modello economico dei dispositivi connessi a internet spesso non permette gli aggiornamenti di sicurezza a cui siamo abituati per dispositivi più tradizionali. La Apple ha interesse a fornire aggiornamenti di sicurezza e a mantenere protetti i nostri iPhone perché costano molto e il futuro dell'azienda dipende anche dalla sua capacità di tenerci lontani dai pericoli digitali.

Ma i produttori di elettrodomestici a basso costo non hanno competenze simili né gli stessi incentivi a procurarsele. È per questo che finora l'internet delle cose è stato sinonimo di scarsissima sicurezza. Ed è per questo che l'anno scorso l'Fbi ha dovuto mettere in guardia i genitori dai pericoli dei giocattoli connessi a internet e che Dan Coats, il direttore dei servizi di sicurezza statunitensi, ha definito i dispositivi intelligenti una minaccia crescente alla sicurezza nazionale.

Un rappresentante di Amazon mi ha detto che la sicurezza diventerà un elemento costitutivo delle sue tecnologie. Il connect kit, ha dichiarato l'azienda, permette ad Amazon di controllare la sicurezza digitale di un apparecchio. Ed è molto probabile che il livello di sicurezza di Amazon sia più alto di quello della maggior parte dei produttori di elettrodomestici.

L'Internet of things consortium, un'organizzazione che rappresenta decine di aziende, non ha risposto a una richiesta di chiarimenti. Schneier non considera l'intervento dello stato un rimedio per tutti i mali, ma un semplice rallentatore di velocità, un modo per permettere agli esseri umani di rimanere al passo con i progressi tecnologici. La regolamentazione e la supervisione dello stato rallentano l'innovazione, ed è uno dei motivi per cui il settore tecnologico non le ama. Ma quando si parla di pericoli globali indefiniti, prendersi un minuto per valutare la situazione non è una cattiva idea.

Connettere ogni cosa potrebbe portare grandi vantaggi alla società. Ma i pericoli potrebbero essere altrettanto grandi. Perché non muoversi quindi con prudenza verso un futuro così incerto? ◆ *ff*