

# Chi possiede veramente gli oggetti digitali?

di Jacopo Franchi

03-03-2025

Jacopo Franchi - membro dell'hub di innovazione Cariplo Factory e del Digital Transformation and Wellbeing Lab dell'Università di Milano-Bicocca - riflette su come stia cambiando il rapporto tra le persone e le "cose" in seguito alla diffusione degli oggetti digitali connessi, delineando alcuni dei temi al centro del suo ultimo libro: L'uomo senza proprietà edito da Egea.

Nei primi giorni del 2025 i giornali di tutto il mondo hanno dato ampio risalto alla proposta di Apple di pagare 95 milioni di dollari di risarcimento ai clienti le cui conversazioni sono state registrate in maniera illecita a causa di errori di attivazione dell'assistente virtuale Siri. La decisione è arrivata al termine di una class action durata quattro anni e che ha avuto visibilità globale sia per l'importo elevato del risarcimento, sia perché l'azienda ha ammesso pubblicamente quello che molti sospettavano da tempo: i dispositivi digitali ci ascoltano, ci osservano e ci registrano anche quando non dovrebbero farlo. Nel caso di Apple si tratta di un numero incalcolabile di iPhone, Apple TV, Apple Watch e iPad - su cui Siri è stata installata a partire dal 2014 - che hanno registrato le conversazioni dei loro proprietari e delle persone nelle immediate vicinanze anche senza che il comando "Ehi, Siri" venisse pronunciato.

La notizia riporta d'attualità un tema controverso, che riemerge a ogni nuovo scandalo e puntualmente rientra sottotraccia a causa dell'impossibilità di poter rispondere in maniera univoca alla domanda più importante di tutte: fino a che punto è possibile "fidarsi" degli oggetti connessi? In che misura possiamo essere sicuri che il televisore "smart" del salotto, la videocamera installata nella camera dei bambini, il frigorifero o il termostato "intelligente" non siano anche strumenti di sorveglianza e violazione della vita privata? Una domanda tanto più urgente se si pensa che le conversazioni e i filmati registrati possono essere condivisi con i dipendenti dell'azienda produttrice degli oggetti connessi, come si legge nella denuncia presentata da un ex operatore di Siri alla procura di Parigi.

In questo articolo proveremo a fornire una visione d'insieme delle principali variabili in gioco, nella consapevolezza che quello che è veramente in gioco non è solo la riservatezza - per quanto importante - delle singole conversazioni private dei clienti Apple, quanto la persistenza o meno di luoghi virtuali e fisici che possano essere considerati totalmente "privati" e inviolabili dall'esterno.

Gli italiani acquistano sempre più oggetti connessi, ma restano indietro nello sviluppo delle competenze digitali di base

Dati alla mano, la digitalizzazione degli oggetti della vita quotidiana è una tendenza entrata nella fase matura anche nel nostro Paese: secondo i dati elaborati dall'Osservatorio Internet of Things del Politecnico di Milano sono oltre 140 milioni gli oggetti connessi alla Rete, in crescita del 9% anno su anno. Ogni italiano possiede, in media, più di due oggetti connessi e ciascuno di questi è dotato di microfoni, rilevatori di movimento, posizione, telecamere e sensori che lo rendono in grado di tenere traccia di ogni variazione nell'ambiente circostante. Quante sono, in questo scenario in piena trasformazione, le "Siri" difettose? Non lo sappiamo, e l'incapacità di stimare questi rischi potenziali per la sicurezza e la privacy delle persone è un primo segnale di attenzione.

Non abbiamo idea, semplicemente, di quanti siano gli oggetti connessi presenti nelle case e nei

---

luoghi di lavoro ancora in condizioni di massima sicurezza, e quanti siano invece quelli compromessi, non aggiornati, protetti da una password debole, o che trasmettono i loro dati verso Paesi non sicuri. Non lo sappiamo, e non rassicura il fatto che i livelli di competenze digitali di base degli italiani siano costantemente al di sotto delle medie europee e di qualsiasi soglia che si potrebbe considerare "accettabile" in una valutazione dei rischi sistemici. Secondo l'indice Digital Economy and Society, più di metà della popolazione non è in grado di utilizzare prodotti e servizi digitali con un livello adeguato di competenze, pur acquistando e consumando in maniera crescente proprio quei prodotti e servizi di cui ignora il funzionamento e le vulnerabilità. Le tante "Siri" difettose installate nei televisori, negli smart speaker, negli smartphone possono continuare a registrare indisturbate anche perché la maggior parte dei loro utilizzatori ignora del tutto questa possibilità, al punto da tenerle costantemente accese e pronte all'ascolto.

Meno privacy in cambio di più servizi: fino a che punto le leggi che dovrebbero tutelarci ci proteggono davvero?

Quali che siano le debolezze di base di una società che ha imboccato con decisione la strada verso la connessione permanente, i vantaggi restano numerosi e innegabili. La digitalizzazione degli oggetti di uso quotidiano offre la possibilità di esercitare un controllo maggiore, anche a distanza, sulle modalità di consumo, risparmio energetico e versatilità nell'utilizzo. L'offerta di un numero maggiore di servizi a parità di numero di "cose" acquistate, i costi iniziali tutto sommato contenuti rispetto alla quantità di funzioni disponibili, l'automazione resa possibile dall'intelligenza artificiale sono fattori che spingono verso la sostituzione completa degli oggetti analogici con quelli digitali e non vi è scandalo, errore o violazione che possa impedire questa trasformazione profonda delle abitudini di consumo.

Chiariamoci: non si tratta qui di demonizzare una particolare tecnologia rispetto all'altra, né di sottovalutare la buona fede dei produttori di tecnologia nel fornire soluzioni rispettose delle leggi esistenti e non invasive della privacy individuale. È necessario, tuttavia, fermarsi un momento a riflettere se le attuali modalità di trattamento dei dati personali siano adeguate a un mondo dove i punti di connessione si moltiplicano ogni giorno, e con essi i rischi che ogni malfunzionamento possa trasformarsi in altrettante "Siri" fuori controllo. Fino a che punto una singola persona può leggere con attenzione informative privacy di decine di pagine e decidere in piena consapevolezza quali dispositivi digitali acquistare e quali autorizzazioni concedere al trattamento dei dati personali? E quali tutele hanno gli anziani o gli adolescenti nei confronti di un oggetto connesso che raccoglie continuamente i loro dati personali per via della noncuranza degli altri membri adulti della famiglia?

La sicurezza informatica in uno scenario di guerra ibrida tra Stati, persone e "cose" connesse, dove ogni oggetto è un potenziale punto di attacco

La tutela della privacy, in questo senso, potrebbe rivelarsi solo uno dei tanti rischi da affrontare in uno scenario di generale impreparazione ai problemi legati alla digitalizzazione di massa. Secondo uno studio realizzato dalle società specializzate in informatica e sicurezza, NETGEAR e Bitdefender, gli oggetti connessi a Internet ricevono una media di dieci attacchi ogni ventiquattrore, con percentuali di successo variabili. Abitudini errate che tre decenni di storia di violazioni informatiche hanno solo in parte scalfito - utilizzare password semplici, non aggiornate, non utilizzare metodi di autenticazione a più fattori, servirsi di hardware e software obsoleti e condividere le credenziali di accesso in chiaro tra più persone - possono generare pericoli che vanno ben al di là dell'integrità del singolo dispositivo. Non sono rari i casi di oggetti compromessi da cybercriminali con l'esplicito intento di raccogliere informazioni utili per attentare alla sicurezza di abitazioni, cose e persone.

In un momento storico in cui le crescenti tensioni geopolitiche si traducono in attacchi informatici che

---

puntano a generare il maggior danno possibile, approfittando delle vulnerabilità più diffuse, la sicurezza informatica non riguarda più l'integrità del singolo dispositivo o la sicurezza di una singola persona per volta. Con la guerra ibrida digitale gli oggetti connessi presenti in gran numero all'interno delle abitazioni private, o sui mezzi di spostamento più utilizzati, possono diventare bersaglio di aggressori lontani - siano essi hacker o servizi di intelligence stranieri - coscienti dello stato di incuria in cui versano le case e le barriere "digitali" di gran parte degli italiani. La cybersecurity applicata al campo degli oggetti connessi diventa così una sfida tecnologica e culturale, dove il numero di possibili punti di ingresso e manomissione tende all'infinito.

Qual è il conto finale di un'economia fondata sull'accesso ad abbonamento in luogo di un'economia fondata sul possesso degli oggetti?

Un approfondimento, infine, deve essere fatto per quanto riguarda la possibilità che le aziende, i fabbricanti e i commercianti di oggetti connessi possano impedire, del tutto o in parte, il corretto funzionamento di questi ultimi. Ogni oggetto digitale mantiene un legame di dipendenza con il proprio produttore: sia per ricevere gli aggiornamenti, sia per poter elaborare in cloud i propri dati, sia per poter fornire nuove funzionalità, più evolute di quelle previste inizialmente. Questa possibilità presenta anche un rovescio della medaglia: la capacità del produttore di poter mettere a pagamento alcune o tutte le funzionalità più avanzate, costringendo i clienti a pagare un abbonamento ricorrente e sempre più caro in luogo di una somma una tantum e definita nel momento dell'acquisto.

I costi della digitalizzazione di massa per la società nel suo insieme, da convenienti che potevano essere all'inizio, potrebbero quindi crescere nel giro di pochi anni fino a livelli difficilmente preventivabili. Gli stessi assistenti virtuali potrebbero, in futuro, diventare accessibili solo su abbonamento - come nel caso di Alexa, di cui è stata annunciata recentemente la versione Alexa+ basata sull'intelligenza artificiale -, soprattutto nel momento in cui le varie Siri dovessero diventare il principale centro di controllo vocale di tutti i dispositivi presenti in un'abitazione. Quanti abbonamenti riusciranno a sostenere, le persone comuni, per poter utilizzare quegli oggetti che pensavano di aver acquistato una volta per tutte? Quale sarà l'impatto di questa economia fondata sull'accesso ai risparmi degli italiani?

La cessione di sovranità sulle cose e le leggi europee che provano, pezzo dopo pezzo, a porre un argine a possibili abusi e mancanze dei produttori

L'aspetto più difficile da accettare, probabilmente, sarà proprio questo legame di dipendenza tra le cose e i loro produttori: troppe consuetudini si sono accumulate nel corso del tempo perché sia semplice accettare il fatto che le "nostre" cose, purtroppo, non ci apparterranno mai più come prima. Per poter utilizzare un oggetto digitale nel pieno delle sue funzionalità sarà sempre necessario poter contare su una connessione alla Rete stabile, sulla disponibilità di aggiornamenti forniti dal produttore, sull'autorizzazione all'accesso tramite credenziali riconosciute dal dispositivo, quando non dalla presenza stessa di un server remoto su cui elaborare la maggior parte dei dati necessari al funzionamento. Basterà poco, basterà il venir meno di uno solo di questi supporti vitali per disattivare anche gli oggetti più costosi, o andare incontro a una serie rovinosa di vulnerabilità e malfunzionamenti.

La legge, in tutto questo, segue a distanza e cerca di anticipare i grandi cambiamenti in atto nella società, alla ricerca di un equilibrio sempre più difficile da trovare tra la possibilità di sviluppare nuove modalità di consumo e profitto e la tutela dei diritti fondamentali delle persone, soprattutto di quelle più fragili. Per far fronte all'insieme di casistiche fin qui sommariamente descritte sono già entrati o entreranno in vigore, nell'arco di alcuni anni, una serie di regolamenti pensati per essere sufficientemente flessibili alle novità che ci attendono: e così se il Regolamento Generale sulla

---

Protezione dei Dati (GDPR) rimane dal 2018 - anno dell'effettiva entrata in vigore - il punto di riferimento per quanto riguarda il trattamento dei dati personali, il Cyber Resilience Act dovrebbe garantire a partire dal 2027 una serie di requisiti minimi di sicurezza per gli oggetti digitali, come l'obbligo di aggiornamenti del software per un periodo di almeno cinque anni.

Domande ancora in attesa di risposta e il ruolo cruciale delle nuove generazioni di fronte alla scelta tra "possesso" e accesso

Anche le leggi, tuttavia, potrebbero andare incontro a una serie di mutamenti sullo scenario globale di non semplice previsione. Basti pensare al destino tuttora incerto dell'accordo tra Unione Europea e Stati Uniti relativo al trasferimento dei dati personali dei cittadini europei sull'altra sponda dell'Atlantico, già annullato in passato da una pronuncia della Corte di Giustizia europea e ora a rischio di venire nuovamente azzerato a seguito dei cambiamenti al vertice delle autorità statunitensi che si erano fatti garanti della sua applicazione. Non è possibile, oggi, tracciare un limite definito e invalicabile tra quello che gli oggetti digitali possono e non possono fare, tra le leggi che devono rispettare e le norme a rischio di venire ridimensionate, e questa incertezza di fondo ha degli effetti tanto sulla qualità e le caratteristiche dei prodotti, quanto sulla fiducia, la sicurezza, i diritti dei consumatori più esposti al rischio.

Il pericolo di una ridondanza o conflittualità tra i regolamenti, e della sostanziale impossibilità per i produttori di dimensioni minori di poter sostenere i costi di un adeguamento a leggi in costante mutamento è all'ordine del giorno. Un produttore europeo di oggetti connessi che debba tenere conto contemporaneamente dei requisiti previsti dall'AI Act, degli obblighi che entreranno in vigore con il Cyber Resilience Act, delle tutele richieste dal GDPR potrebbe decidere di rinunciare in partenza a una competizione in cui parte svantaggiato rispetto alle multinazionali hi-tech, oppure sottovalutare volutamente alcuni rischi insiti nei suoi prodotti digitali potendo contare sulla relativa scarsità di controlli all'accesso sul mercato, e sulla generale ignoranza e rassegnazione della maggioranza dei suoi clienti.

Siri, anche in questo caso, ha ancora tanto da offrirci in termini di spunti di riflessione. Qual è il valore che le persone sono disposte ad assegnare alla propria privacy individuale, alla propria sicurezza, ai propri diritti come cittadini ancor prima che come consumatori? Qual è il valore che le nuove generazioni, in futuro, assegneranno al possesso di qualcosa, e che cosa invece spingerà sempre più i giovani a preferire un accesso temporaneo a rischio di venire interrotto da produttori, cybercriminali, amministratori di sistema? Qual è il risarcimento che Apple avrebbe dovuto pagare se davvero fossero state condotte indagini approfondite, e fossero emersi i contenuti completi di dieci anni di conversazioni registrate "per errore" e conservate non si sa in quali condizioni? Altre domande a cui qualcuno - fosse anche un assistente virtuale potenziato dall'intelligenza artificiale - dovrebbe cominciare a dare una risposta.