LA CULTURA DELLA PRIVACY

Le aziende del Web e gli enti governativi analizzano sempre più informazioni sulle nostre vite. Si è pensato finora di rispondere con l'approvazione di nuove leggi sulla privacy o con qualche forma di pagamento in cambio dei nostri dati. Ciò che occorre, invece, è una soluzione sul fronte culturale e sociale, perché la democrazia stessa è a rischio.

Evgeny Morozov

Nel 1967, "The Public Interest", la gloriosa rivista che ospitava i dibattiti colti in ambito politico, pubblicò un interessante contributo di Paul Baran, uno degli artefici del metodo di trasmissione dei dati, la cosiddetta commutazione di pacchetto. Il breve saggio, intitolato *The Future Computer Utility*, avanzava l'ipotesi che in un futuro non lontano alcuni grandi computer centralizzati si sarebbero occupati di «elaborare l'informazione [...] allo stesso modo in cui viene "lavorata" e venduta l'elettricità».

Sono passati alcuni decenni e il cloud computing ha dato corpo alle previsioni di Baran. Ma l'ingegnere polacco naturalizzato statunitense è stato talmente previdente da intuire che i nuovi servizi computerizzati avrebbe richiesto sistemi di regolamentazione *ad hoc*.

Baran ha lavorato per dieci anni alla RAND Corporation – non certo un fortino del pensiero marxista – ponendosi interrogativi sulle quote di mercato in mano alle aziende private che offrivano servizi computerizzati, richiedendo l'intervento statale. Baran chiedeva anche politiche che offrissero «la massima protezione al diritto di privacy dell'informazione».

Un'analisi lucida, diretta al cuore della questione; il tecnofuturismo era già in crisi dai blocchi di partenza.

Tutte le soluzioni finora proposte sono insufficienti

A leggere l'articolo di Baran (uno dei tanti sul futuro dei servizi computerizzati apparsi in quegli anni) ci si rende conto che le discussioni sui confini della privacy hanno una radice lontana nel tempo. Non sono solo la conseguenza della vendita da parte di Zuckerberg dei nostri profili e della sua anima alla NSA. Il problema è stato previsto da subito, ma assai poco si è fatto per risolverlo.

Quasi tutti gli impieghi previsti da Baran dell'*utility computing* rientrano nell'ambito commerciale. Ordini di capi d'abbigliamento, pagamento di fatture, ricerca di spettacoli d'intrattenimento: non è l'Internet delle "comunità virtuali" e dei "cittadini della rete", i cosiddetti *netizen*. Baran immaginava semplicemente che i computer in rete permettessero di fare cose realizzabili anche senza le reti: shopping, intrattenimento, ricerca. Ma anche: spionaggio, sorveglianza, voyeurismo.

Se la "rivoluzione dei computer" di Baran non sembra granché rivoluzionaria, ciò è in buona parte dovuto al fatto che lo studioso non poteva immaginare che questa tecnologia avrebbe capovolto dalle fondamenta le società capitaliste e l'amministrazione burocratica, immutabile nei secoli. A partire dal 1990, invece, molti accaniti sostenitori della tecnologia digitale l'hanno vista in termini del tutto diversi. Hanno ritenuto che la diffusione delle reti di computer e il rapido declino dei costi delle comunicazioni rappresentassero un nuovo stadio dello sviluppo umano. A loro parere, il livello di sorveglianza alimentato dagli attentati dell'11 settembre del Duemila, la colonizzazione degli spazi digitali da parte di Google, Facebook e i big data hanno rappresentato delle anomalie che potevano venire evitate o limitate. Un po' come riscrivere il passato, cancellando i decenni persi e ritornando alla spinta utopica degli anni Ottanta e Novanta con leggi più rigorose, un controllo più stretto degli utenti e strumenti più avanzati per decodificare i dati.

Una diversa lettura della storia recente dovrebbe portare a una nuova agenda per il futuro. Il sentimento diffuso di emancipazione legato all'informazione, che molte persone ancora ascrivono agli anni Novanta, è stato probabilmente il frutto di una allucinazione prolungata nel tempo. Il capitalismo e l'amministrazione burocratica hanno facilmente retto il passo con il nuovo regime digitale, adeguandosi ai flussi informativi e sfruttando la crescente automatizzazione. Le diverse legislazioni, i mercati o le tecnologie non ostacolano la richiesta di dati, in quanto tutti e tre giocano un ruolo centrale nel sostenere il capitalismo e l'amministrazione burocratica. Qualcos'altro è mancato: la politica.

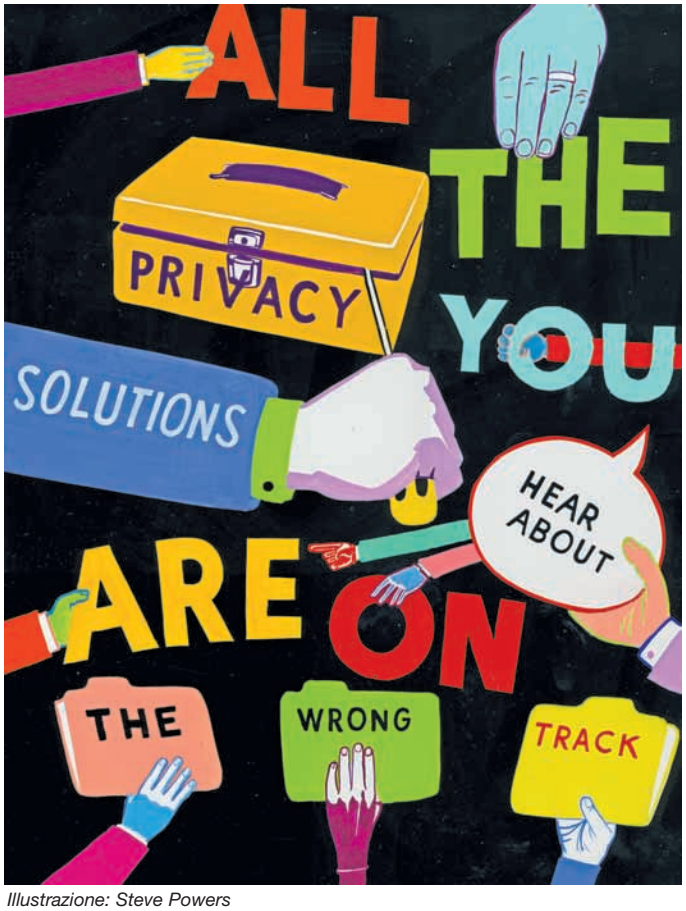

Illustrazione: Steve Powers

Qualsiasi intervento può minare la democrazia

Prendiamo in esame i sintomi del malessere attuale. Effettivamente gli interessi commerciali delle aziende tecnologiche e le finalità politiche degli enti governativi hanno trovato un punto di convergenza: la raccolta e la rapida analisi dei dati degli utenti. Google e Facebook sono "costrette" ad accumulare sempre più dati per aumentare le vendite degli spazi pubblicitari. Gli enti governativi hanno bisogno degli stessi dati – raccolti direttamente o in collaborazione con le aziende tecnologiche – per perseguire i loro scopi programmatici.

Molti di questi programmi fanno riferimento alla sicurezza nazionale. Ma questi dati si possono utilizzare in molte altre maniere, mettendo a rischio la privacy degli utenti. Il governo italiano, per esempio, si sta affidando al redditometro, un accertamento sintetico di tipo induttivo, che analizza le entrate e le modalità di spesa per segnalare come potenziale evasore fiscale chi spende più di quanto dichiara di reddito. Una volta che i pagamenti mobili avranno rimpiazzato quasi del tutto le transazioni in contante – con Google e Facebook come intermediari – i dati raccolti da queste aziende saranno indispensabili per i controlli fiscali. Allo stesso tempo, gli esperti legali stanno studiando come sfruttare il *data mining* al fine di definire contratti "su misura", che tengano conto di personalità, caratteristiche, comportamenti passati dei contraenti, permettendo di ridurre le anomalie presenti in questi settori.

Su un altro fronte, tecnocrati come Cass Sunstein, ex amministratore dell'Office of Information and Regulatory Affairs della Casa Bianca e uno dei principali sostenitori del *nanny statecraft*, un "manuale" sul tipo di misure che il governo può intraprendere per influenzare il comportamento dei cittadini, sperano che la raccolta e l'analisi rapida dei dati individuali possa aiutare a risolvere problemi quali l'obesità, il cambiamento climatico, l'alcolismo. Un nuovo libro di tre studiosi universitari inglesi – *Changing behaviours: on the rise of the psychological state* – presenta una lunga lista delle azioni intraprese in Gran Bretagna, in cui sono operative unite governative ispirate dal lavoro di Sunstein, che agiscono sulla leva comportamentale per favorire le iniziative senza scopo di lucro.

Grazie agli smartphone o a Google Glass, ci viene segnalato ogni volta che stiamo per fare qualcosa di stupido o dannoso. Non sempre veniamo a conoscenza del perché l'azione che stavamo intraprendendo era sbagliata, in quanto gli algoritmi di sistema eseguono i loro calcoli "morali" in piena autonomia. I cittadini svolgono il ruolo di macchine informative che alimentano il complesso tecnoburocratico con i loro dati. E perché non dovrebbero farlo se viene promesso loro in cambio un fisico più snello, l'aria meno inquinata o una durata maggiore della vita (senza malattie)?

Questa logica della prevenzione non è differente da quella adottata dalla NSA nella sua battaglia contro il terrorismo: anticipare i problemi invece di fronteggiarne le conseguenze. Anche se si legano le mani alla NSA – con combinazioni più accurate di sistemi di supervisione, leggi più rigide sull'accesso ai dati o nuove tecnologie di decrittazione – si rimane scoperti con la caccia all'informazione portata avanti da altri enti statali. Le loro giustificazioni appaiono valide. Su problemi quali l'obesità o il cambiamento climatico – che i responsabili politici si affrettano a definire vere e proprie bombe a orologeria – si argomenta che un deficit parziale di democrazia vale bene i vantaggi che ne derivano.

Le conseguenze di questo deficit ci portano però a uno scenario diverso: la nuova infrastruttura digitale, alimentata dai contributi in tempo reale volontariamente forniti dai cittadini, permette ai tecnocrati di prendere decisioni politiche al di fuori dell'agone politico, con tutte le conseguenze spiacevoli che ne possono derivare. Di fatto si sostituisce la macchinosa procedura di confronti laceranti, contrattazioni e accordi della vita politica con l'efficienza e la linearità dell'amministrazione fondata sui dati.

Questo fenomeno ha un nome all'apparenza inoffensivo: "regolamentazione algoritmica", come è stata definita da Tim O' Reilly, fondatore della O'Reilly Media e importante voce intellettuale di Silicon Valley. In altre parole, le democrazie avanzate dal punto di vista della circolazione dell'informazione hanno raggiunto un punto in cui si cercano di risolvere i problemi pubblici senza spiegare nulla ai cittadini. Ci si appella semplicemente al loro tornaconto personale, proponendo delle contropartite mirate, per molti aspetti irresistibili.

La privacy non è un fine in sé, ma uno strumento

Un altro monito dal passato. Nel 1985, Spiros Simitis, uno dei principali esperti di privacy della Germania – allora commissario per la protezione dei dati dello stato federale di Assia – era ospite della facoltà di giurisprudenza dell'University of Pennsylvania. La sua conferenza verteva sullo stesso argomento che aveva sollevato

le preoccupazioni di Baran: l'automazione dei sistemi di elaborazione dei dati. Ma Simitis non perse di vista la storia del capitalismo e della democrazia, inquadrando i cambiamenti tecnologici in una cornice più vasta.

Simitis si rese conto che la privacy non è un fine di per sé, ma uno strumento per perseguire un particolare ideale di democrazia politica, in cui i cittadini sono indotti a essere qualcosa di più che soddisfatti fornitori di informazioni a tecnocrati onniscienti e inappuntabili: «Quando la privacy è smantellata, vengono meno sia le possibilità di fare scelte politiche, sia le opportunità di proporre e mantenere un determinato stile di vita».

Tre tendenze tecnologiche rafforzavano l'analisi di Simitis. In primo luogo, egli notava che già in quel periodo ogni sfera dell'interazione sociale era mediata dalla tecnologia dell'informazione. Lo studioso di privacy metteva in guardia «dal reperimento intensivo di dati personali di lavoratori, contribuenti, pazienti, clienti di banca, titolari di assegni assistenziali o automobilisti». Le conseguenze erano che la perdita di privacy non rappresentava un incidente di percorso di qualche malcapitato, ma un problema di tutti.

In secondo luogo, le nuove tecnologie come le smartcard e il videotex non avevano solo reso possibile «registrare e ricostruire le attività individuali nel minimo dettaglio», ma anche normalizzare l'idea stessa di sorveglianza, trasferendola all'interno della quotidianità. In terzo luogo, l'informazione personale raccolta da queste nuove tecnologie stava permettendo alle istituzioni sociali di rinforzare gli standard di comportamento, mettendo in atto «strategie manipolative di lungo termine mirate a plasmare le condotte individuali».

Le istituzioni moderne hanno tratto profitto da questa situazione. Le compagnie assicurative possono predisporre programmi personalizzati a costi ridotti per venire incontro alle esigenze di pazienti, ospedali e industria farmaceutica. La polizia può utilizzare i database e una gamma di "profili di mobilità" per identificare potenziali criminali e localizzare i sospetti. Gli enti di assistenza sociale sono in grado di smascherare rapidamente i comportamenti fraudolenti.

Ma in che modo queste tecnologie ci coinvolgono in quanto cittadini, vale a dire come soggetti che interpretano e cercano di modificare il mondo intorno a loro, non solo in qualità di consumatori o clienti che si limitano a sfruttarne i vantaggi?

Stiamo perdendo la battaglia su tutti i fronti, sosteneva Simitis. Invece di acquisire più conoscenze su come vengono prese le decisioni politiche, aumentano le nostre incertezze; invece di fare luce sulla logica che guida i nostri sistemi burocratici e di renderla più semplice e meno kafkiana, siamo preda della confusione perché le scelte maturano in modo automatico e nessuno è in grado di comprendere come funzionano esattamente gli algoritmi alla base di questo meccanismo. Percepiamo un quadro sfuocato del modo di procedere delle nostre istituzioni. Malgrado la promessa di favorire lo sviluppo individuale, i sistemi interattivi sembrano garantire solo l'illusione di una maggiore partecipazione. Il risultato è che «i sistemi interattivi [...] danno l'idea di favorire l'attività individuale mentre in realtà non si tratta di altro che di reazioni stereotipate».

Se si pensa che Simitis parlasse di un futuro improbabile, si

Illustrazione: Jody Barton

prenda in considerazione un recente saggio sulla trasparenza dei sistemi automatici di previsione di Tal Zarsky, uno dei più autorevoli esperti mondiali di politica ed etica del *data mining*. Lo studioso nota che «il *data mining* coinvolge individui ed eventi, indicando elevati livelli di rischio, senza dire perché si è scelto quel tipo di selezione».

In questa situazione il livello di interpretabilità è una delle decisioni politiche fondamentali da prendere per dare il via libera ai sistemi di *data mining*. Zarsky vede in questo passaggio serie implicazioni per lo sviluppo della democrazia:

> *Da una ricerca di dati non spiegabile in maniera analitica potrebbero scaturire decisioni non motivabili. In questo caso, il software prenderebbe le sue decisioni di selezione sulla base di variabili multiple (anche nell'ordine di migliaia)[...]. Sarebbe difficile per il governo fornire una risposta dettagliata a qualcuno che chiedesse perché a una persona è stato riservato un trattamento particolare da un sistema di segnalazione automatizzato. L'unica cosa ragionevole che il governo potrebbe sostenere è che l'algoritmo si è basato su una lista di casi precedenti.*

Questo è il futuro verso cui ci stiamo incamminando. Tutto sembra funzionare e le cose all'apparenza vanno per il meglio, ma non sappiamo come e perché.

Anche una privacy illimitata rappresenta una minaccia

Simitis ha visto giusto. Senza lasciarsi sedurre dalle sirene dell'"era di Internet", Simitis ha avanzato una originale, anche se prudente difesa della privacy come caratteristica vitale di una democrazia autocritica; non della democrazia di qualche astratta teoria politica, ma di quella contraddittoria e turbolenta nella quale viviamo. In particolare, l'intuizione più profonda di Simitis è che la privacy può allo stesso tempo sostenere e minare alle basi la democrazia.

Tradizionalmente, la nostra risposta ai cambiamenti introdotti dalla informazione automatica è stata di vedere questi cambiamenti come un problema personale degli individui coinvolti. L'esempio tipico è rappresentato dall'articolo *The right to privacy* di Louis Brandeis e Samuel Warren, da cui è nato il concetto giuridico del diritto alla privacy. Apparso sulla "Harvard Law Review", nel 1890, vi si sosteneva «il diritto a essere lasciati soli» a vivere una vita tranquilla senza intrusioni esterne. Secondo Simitis, i due autori espressero il desiderio, condiviso da molti *self-made man* dell'epoca, «di godere, in piena autonomia e alle loro condizioni dei frutti delle loro attività economiche e sociali».

Un obiettivo lodevole: se non si fosse estesa questa copertura legale agli imprenditori, il moderno capitalismo americano non sarebbe mai potuto diventare così florido. Ma questo diritto, separato da qualsiasi responsabilità sociale, potrebbe anche sancire un eccessivo livello di distacco dal mondo esterno e mettere a rischio le fondamenta della democrazia che ha reso possibile il suo riconoscimento. Se tutti i cittadini esercitassero pienamente il loro diritto alla privacy, la società verrebbe privata della trasparenza informativa fondamentale non solo per il benessere dei tecnocrati, ma anche indispensabile per valutare i problemi, formarsi delle opinioni e confrontarsi (e, qualche volta, mandare a casa i tecnocrati).

Non si tratta di una questione relativa soltanto al diritto alla privacy. Per alcuni pensatori contemporanei, come lo storico e filosofo francese Marcel Gauchet, le democrazie rischiano di cadere vittime dei propri successi. Con l'istituzione di un sistema legale di diritti, che permette ai cittadini di perseguire i loro interessi privati senza riferimenti al bene pubblico, si corre il pericolo di esaurire le risorse che hanno favorito l'avvento dello stesso sistema legale.

Se tutti i cittadini rivendicano i loro diritti senza assumersi delle responsabilità, le questioni politiche che hanno caratterizzato la vita democratica nel corso dei secoli – Come si può vivere insieme? Qual è l'interesse pubblico e come interagisce con quello personale? – vengono riassorbite nei domini legali, economici e amministrativi. Il "politico" e il "pubblico" rimangono completamente fuori da questi domini; le leggi, i mercati e le tecnologie dettano i tempi dei dibattiti e delle contestazioni, con soluzioni radicali.

Ma una democrazia priva della partecipazione dei cittadini non assomiglia a una vera democrazia e potrebbe venire meno. Tutto ciò era ovvio a Thomas Jefferson che, oltre a volere che ogni cittadino «partecipasse al governo degli affari», credeva che l'impegno civile prevedesse una dialettica costante tra vita pubblica e privata. Una società che ritiene, come afferma Simitis, che l'accesso dei cittadini all'informazione «finisce dove inizia il diritto alla privacy del *bourgeois*» non sarebbe una democrazia ben funzionante. Allora l'equilibrio tra privacy e trasparenza deve venire continuamente negoziato nei periodi di rapidi cambiamenti tecnologici. Questo bilanciamento è un problema politico *par excellence*, da definire attraverso un

Illustrazione: Wes Lang

costante confronto pubblico e sempre aperto alla negoziazione. Non può venire stabilito una volta per tutte con una serie di alchimie tra teorie, mercati e tecnologie. Come ha sostenuto Simitis: «ben lontana dal venire considerata un elemento costitutivo della società democratica, la privacy appare come una contraddizione tollerata, le cui implicazioni vanno sempre riprese in considerazione».

La legge e il mercato non bastano

Negli ultimi decenni, le nostre istituzioni sono diventate sempre più dipendenti dalla mole crescente di dati. Se si trattenessero i dati e si interrompesse il ciclo informativo, probabilmente il giocattolo si romperebbe. Come cittadini ci troviamo in una condizione anomala: la ragione per cui divulghiamo i dati non è legata al nostro senso civico. In realtà, diffondiamo le nostre informazioni personali su Google o su applicazioni *self-tracking*. Ci rivolgiamo ai servizi gratuiti foraggiati dagli avvisi pubblicitari o vendiamo i nostri dati per monitorare diete e stato di forma fisica.

Già nel 1985 Simitis aveva capito che saremmo arrivati alla "regolazione algoritmica" come la stiamo conoscendo oggi e che la politica sarebbe diventata "amministrazione pubblica" che si affida al pilota automatico in modo che i cittadini possano rilassarsi e divertirsi, per venire occasionalmente "richiamati" nel caso abbiano dimenticato di comprare, per esempio, dei broccoli.

Simitis descrive la costruzione di quello che io definisco il "filo di ferro invisibile" stretto intorno alle nostre vite sociali e intellettuali. I

big data, con i diversi database interconnessi che si affidano a informazioni e algoritmi di dubbia provenienza, impongono severe costrizioni alla nostra maturazione politica e sociale. Nel 1963, il filosofo tedesco Jürgen Habermas aveva giustamente avvertito che «una civiltà sbilanciata esclusivamente sul lato tecnologico [...] è minacciata [...] dalla divisione degli esseri umani in due classi: gli "ingegneri sociali" e i "carcerati" delle istituzioni sociali chiuse».

Questo invisibile filo spinato dei big data limita le nostre vite a uno spazio che potrebbe sembrare ospitale e colmo di attrattive, ma che non è stato scelto da noi e non è in nostro potere ricostruire o espandere. Il problema di fondo è che non ce ne rendiamo conto. Crediamo di essere liberi di fare qualsiasi cosa e il filo spinato rimane invisibile. L'aspetto ancora più paradossale è che non possiamo prendercela con nessuno. Di certo non con Google, Dick Cheney o la NSA. Il filo invisibile è il risultato di diverse logiche e sistemi – del capitalismo moderno, del governo burocratico, della gestione del rischio – sovralimentati dall'automazione informatica e dalla depoliticizzazione della politica.

Più informazioni riveliamo su di noi, più denso diventa il filo invisibile. Perdiamo gradualmente la nostra capacità di ragionare e di confrontarci; non capiamo più quello che ci accade intorno.

Ma non tutto è perso. Possiamo diventare consapevoli di questo filo e liberarcene. La privacy è la risorsa che ci permette di farlo e, se saremo fortunati, di trovare la strada giusta per uscirne.

Questo contesto spiega perché Simitis ha espresso una verità rivoluzionaria che non è presente nei dibattiti di oggi sulla privacy: non si avrà alcun progresso, ha detto Simitis, fino a quando la protezione della privacy «sarà equiparata al diritto individuale di decidere quando e quali dati siano accessibili». La trappola in cui cadono molti autorevoli sostenitori della privacy è pensare che garantendo all'individuo più controlli sui suoi dati – attraverso leggi più severe o un regime di proprietà più rigido – quel filo spinato invisibile diventi finalmente riconoscibile e possa venire spezzato. Non sarà così, almeno fino a quando questi dati ritornano a quelle stesse istituzioni che hanno eretto la barriera intorno a noi.

Una riflessione sulla privacy in termini etici

Se definiamo la privacy un problema di tenuta democratica, le convinzioni tradizionali appaiono inadeguate. Jaron Lanier, per esempio, nel suo libro *Who owns the future?*, sostiene di tralasciare un polo della privacy – quello legale – per focalizzarsi invece sul versante economico. «I diritti commerciali si prestano di più alle diverse situazioni della vita reale rispetto ai nuovi diritti che caratterizzano la privacy digitale», scrive Lanier. Secondo questo filone di pensiero, la trasformazione dei nostri dati in un bene da vendere permette di raggiungere due obiettivi. Innanzitutto, si riesce a controllare chi ne ha accesso; in secondo luogo, si ha un corrispettivo per la cessione dei dati.

La proposta di Lanier non è originale. In *Code and other laws of cyberspace* (pubblicato per la prima volta nel 1999), Lawrence Lessig aveva espresso il suo pieno consenso all'idea di dare vita a un regime proprietario sui dati personali. Lessig auspicava l'avvento di un "aiutante elettronico" per negoziare con i siti Web: «L'utente effettua le sue scelte una sola volta – specificando il livello di negoziazione della privacy e che cosa è disposto a cedere dei dati personali – e da quel momento in poi, quando si collega, il sito e l'aiutante negoziano. Solo se l'aiutante elettronico troverà l'accordo, il sito potrà ottenere i dati richiesti».

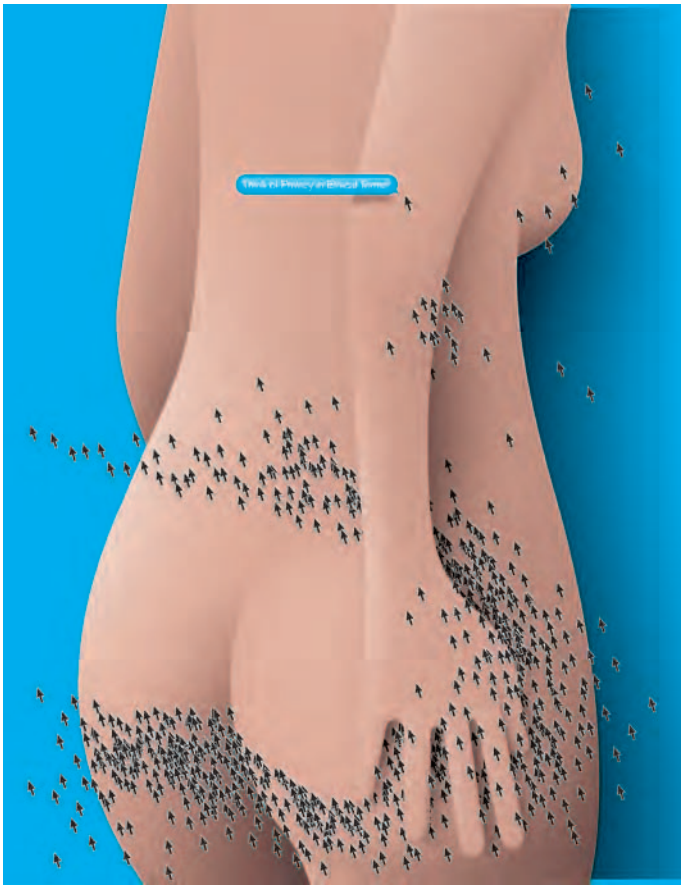

Illustrazione: Felix Pfäffli

É facile vedere dove potrebbe portarci questo ragionamento. Molti di noi possiedono applicazioni personalizzate per smartphone che registrano le informazioni relativamente a chi incontriamo e i luoghi che visitiamo, aggiornando costantemente il valore del nostro portfolio personale di dati. Il processo sarebbe estremamente dinamico: quando passeremo vicino a una gioielleria, il negozio sarà probabilmente disposto a pagare di più per sapere quando è il compleanno di nostra moglie, rispetto a quanto pagherebbe questa informazione se fossimo seduti davanti alla TV nel soggiorno della nostra abitazione.

In realtà, il regime proprietario può rafforzare la privacy. Se i consumatori vogliono un buon ritorno economico dal loro portfolio di dati, devono assicurarsi che queste informazioni non siano disponibili da qualche parte. Allora, o le "danno in noleggio" come fa Netflix con i film, o le vendono a patto che vengano utilizzate o rivendute solo dietro il rispetto di condizioni rigidissime. Alcune aziende offrono già dei *data lockers,* vale a dire contenitori protetti di dati, per facilitare scambi in sicurezza.

Pertanto, se si vuole difendere il "diritto alla privacy" per il proprio tornaconto personale, la trasformazione dei dati in un bene commerciabile può rimuovere le preoccupazioni. L'NSA avrebbe ancora ciò che le interessa; ma se il problema è la paura dell'utente che la sua informazione privata sia vulnerabile e fuori controllo, un

modello commerciale agile, accoppiato a un regime rigido di gestione dei diritti digitali, è in grado di fornirgli le giuste garanzie.

Intanto, gli enti governativi continuano a "imbonirci" per raccogliere i dati, disposti anche a pagare un piccolo prezzo o a promettere una detrazione fiscale per ottenere quello che vogliono dal cittadino, anche con l'aiuto dei dati del suo smartphone. I consumatori vincono, gli imprenditori vincono, i tecnocrati vincono. La privacy viene in qualche modo preservata. Allora, chi è che perde in questa situazione? A leggere Simitis, la risposta è chiara: la democrazia.

Non si tratta solo dell'invisibile filo spinato che continua a circondarci. Ci sono anche delle implicazioni sul piano della giustizia e dell'uguaglianza. Per esempio, la mia decisione di divulgare le informazioni personali, anche solo alla mia compagnia assicurativa, avrà inevitabilmente delle ricadute su altre persone, molte delle quali in condizioni meno privilegiate delle mie. Chi sostiene che la registrazione dei dati sul suo stato di salute o sulla locazione è una scelta individuale dalla quale può tirarsi fuori in qualsiasi momento, ha poca conoscenza del funzionamento delle istituzioni. Una volta che il sistema di automonitoraggio viene adottato da un discreto numero di persone – molte delle quali ricevono una qualche forma di ricompensa per farlo – coloro che si rifiuteranno di registrare i loro dati non saranno visti come persone che agiscono in piena autonomia, ma saranno considerati dei devianti con qualcosa da nascondere. La loro assicurazione avrà costi più alti. Da questo punto di vista, la nostra decisione di automonitorarci non si può ridurre a un semplice vantaggio economico. Inevitabilmente, subentrano delle considerazioni di ordine morale. Voglio realmente condividere i miei dati e prendere un coupon di cui posso fare a meno se questa mia azione può costringere qualcuno che magari sta già facendo più lavori per mantenersi a pagare di più? Queste riflessioni morali perdono di peso se la decisione finale viene delegata a un "aiutante elettronico".

Pochi di noi si pongono problemi morali quando si tratta di condividere i dati, ma la situazione potrebbe cambiare. Prima che la questione ambientale esplodesse, quasi nessuno ci pensava due volte per prendere l'automobile invece dei servirsi del trasporto pubblico. Prima che il commercio equo e solidale si imponesse all'attenzione globale, nessuno avrebbe pagato di più un caffè *fair trade*.

Ovviamente non ci si può comportare in questo modo per tutto quello che si acquista, altrimenti non si uscirebbe mai da un negozio. Ma lo scambio di informazioni – l'ossigeno della vita democratica – dovrebbe ricadere nella categoria del "rifletti di più, non di meno". É qualcosa che non si può delegare a un "aiutante elettronico", se non si vuole privare la nostra vita della sua dimensione politica.

Sabotare il sistema non risolve il problema

Si può anche pensare di ridurre il problema della privacy alla dimensione legale. La domanda che ci si è posti negli ultimi due decenni – Come possiamo avere la sicurezza di esercitare un controllo maggiore sui nostri dati personali? – non può essere l'unica. A meno che non si riesca a comprendere passo dopo passo come l'elaborazione automatica dell'informazione favorisca e limiti la vita democratica, una risposta a questa domanda sarebbe priva di valore, specialmente se il regime democratico si riaggiorna continuamente in tempo reale sulla base delle nostre informazioni. Da un punto di vista intellettuale, il passaggio da intraprendere è chiaro: affrontare la questione non solo sui versanti economico e legale, ma anche su quello politico, collegando il futuro della privacy al futuro della democrazia in modo tale da non ridurre la privacy né ai mercati né alle leggi. Come si traduce in pratica questa indicazione di ordine teorico?

Innanzitutto, è necessario politicizzare il dibattito sulla privacy e la condivisione dell'informazione. Mettere in luce l'esistenza – e le profonde conseguenze politiche – del filo spinato invisibile potrebbe rappresentare un buon inizio. Si devono analizzare le soluzioni dei problemi a uso intensivo di dati e mostrarne il carattere a volte antidemocratico. In alcune situazioni si dovrebbero accettare più rischi, imperfezioni, improvvisazioni e inefficienze pur di mantenere vivo lo spirito democratico.

In secondo luogo, si deve imparare a sabotare il sistema, anche rifiutando in blocco l'automonitoraggio. Se rifiutare di registrare le calorie assunte o i nostri spostamenti è la sola strada per costringere i responsabili politici a mettere mano alle cause strutturali di problemi come l'obesità o il cambiamento climatico – e non limitarsi ad affrontare i sintomi con un sistema di piccole ricompense – il boicottaggio dell'informazione può essere giustificato. Non fare cassa vendendo i propri dati personali potrebbe rappresentare un atto politico, allo stesso modo di non guidare una macchina o non mangiare carne. La privacy può allora riemergere come strumento politico per mantenere vivo lo spirito della democrazia. Si difendono gli spazi privati perché si crede nella nostra capacità di riflettere sui problemi del mondo e sulle possibili soluzioni, non intendendo delegare queste facoltà ad algoritmi o cicli informativi.

In terzo luogo, i servizi digitali dovrebbero divenire più propositivi. Un sito Web non si dovrebbe limitare a chiederci di decidere chi debba vedere i nostri dati, ma rimettere in moto la nostra creatività. Invece di spingere i cittadini a salvaguardare o condividere l'informazione personale, i siti dovrebbero avere una funzione di stimolo, rivelando le dimensioni politiche nascoste delle diverse modalità di condivisione dell'informazione. Non serve un aiutante elettronico, ma un "provocatore" elettronico. Non più applicazioni che dicono quanto denaro si può risparmiare monitorando i nostri esercizi fisici, ma applicazioni che ci facciano capire quante persone perderanno l'assicurazione sanitaria se le Compagnie assicurative avranno a disposizione tanti dati come l'NSA, buona parte di cui forniti da consumatori come noi. Il risultato finale sarebbe che in poco tempo riusciremmo a riconoscere i problemi da soli, senza alcuna forma di assistenza tecnologica.

Infine, dobbiamo abbandonare i preconcetti su come i servizi digitali funzionino e si interconnettano. Altrimenti, cadremmo vittime della stessa logica che ha indotto molti sostenitori accaniti della privacy a pensare che la difesa del "diritto alla privacy" – non la battaglia per la tutela della democrazia – debba essere la linea portante della politica pubblica. Anche se molti seguaci di Internet non saranno d'accordo, ciò che accade in rete ha solo un'importanza secondaria. Come nel caso della privacy, l'obiettivo principale dovrebbe essere il destino della democrazia. ■

Evgeny Morozov è l'autore di The Net Delusion: The Dark Side of Internet Freedom *e di* To Save Everything, Click Here: The Folly of Technological Solutionism.