Il mercato d

Evgeny Morozov, Frankfurter Allgemeine Zeitung, Germania. Foto di Robert Schlaug

In un mondo in cui i dati sono merce, non c'è legge che possa difendere la libertà di internet. Serve una visione più nitida dell'apocalisse che ci attende, scrive Evgeny Morozov

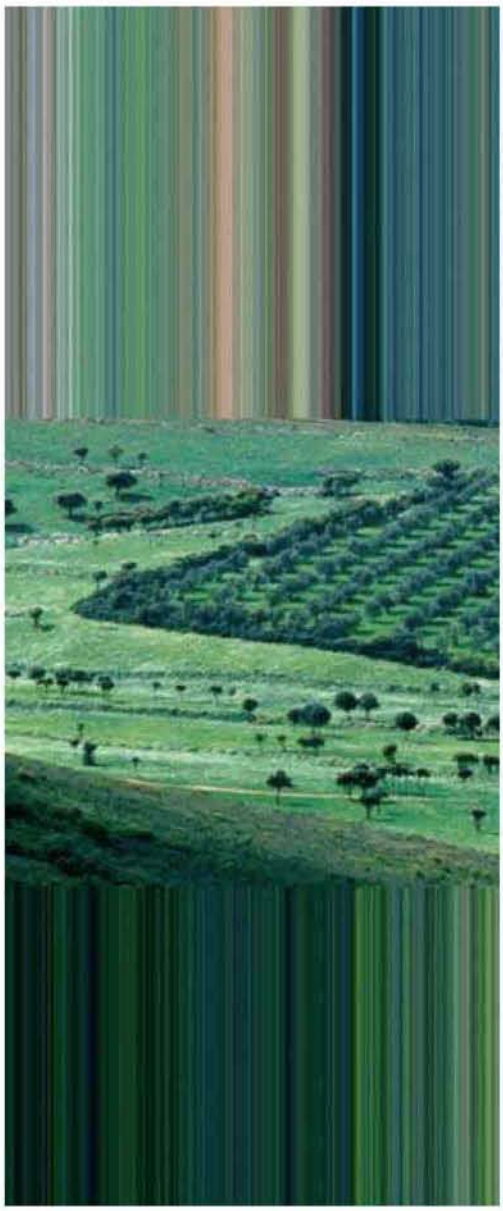
Edward Snowden ha messo a nudo il vero problema degli Stati Uniti. Questa superpotenza ossessiva e malata non riesce a pronunciare l'unica frase assolutamente necessaria per poter andare avanti: "Mi chiamo America e sono dipendente dai dati". Per le spie statunitensi i *big data* sono come il crack: bastano poche dosi per diventare dipendenti. Sì, all'inizio c'è un'illusione di grandezza e onnipotenza narcisistica – "Guardateci, con tutti questi dati possiamo scongiurare un altro 11 settembre" – ma una mente più lucida si accorge subito che la capacità di giudizio è gravemente alterata. Scongiurare un altro 11 settembre? Sul serio? Ma se due ragazzini maniaci dei social network riescono a far saltare in aria la maratona di Boston! Tutti questi dati, tutti questi sacrifici, per cosa?

Non possiamo ignorare la dipendenza americana dalla sorveglianza. È una realtà, ha delle conseguenze, e il mondo farebbe bene a mandare gli Stati Uniti in un centro di disintossicazione dai *big data*. Ma c'è anche altro che dovremmo imparare dal caso Snowden. Ha sgonfiato una serie di miti solo marginalmente legati alla sorveglianza, che riguardano invece i presunti vantaggi di un'infrastruttura digitale decentrata e gestita su base commerciale, la condizione attuale della geopolitica mediata tecnologicamente e l'esistenza di un mondo autonomo chiamato "ciberspazio". Dobbiamo valutare attentamente dove siamo e riflettere su dove presto ci ritroveremo, soprattutto se non riusciamo ad affrontare – giuridicamente, ma soprattutto intellettualmente – le tentazioni del consumismo informativo.

Primo: molti europei si stanno finalmente rendendo conto, con assoluto sgomento, che il termine *cloud* è solo un eufemismo per "un bunker buio nell'Idaho o nello Utah". Se lo scrittore argentino Jorge Luis Borges fosse vissuto più a lungo, avrebbe certamente scelto un server, e non una biblioteca, come ambientazione per le sue storie surreali.

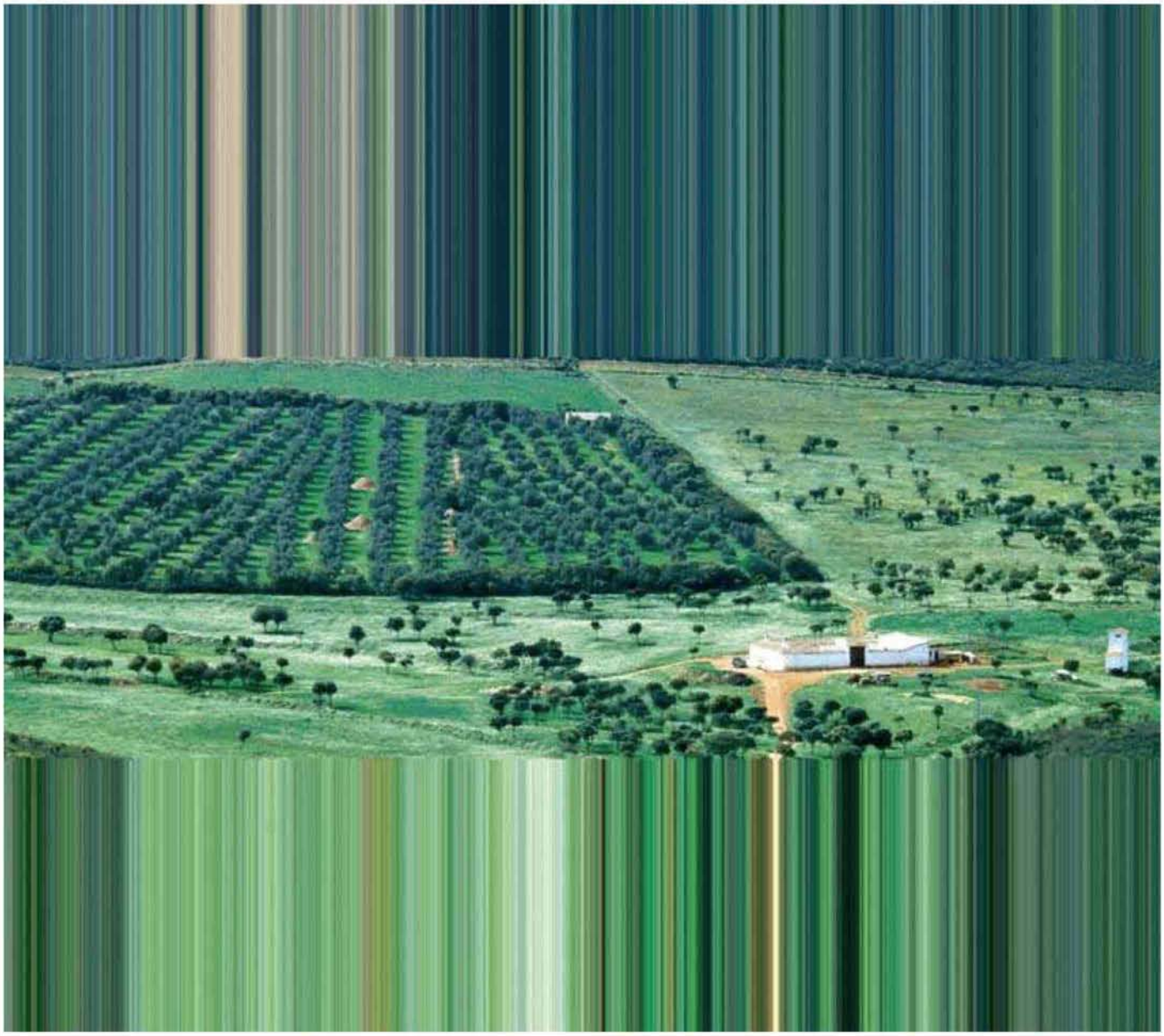
Secondo: dopo il caso Snowden idee che un tempo sembravano assurde improvvisamente appaiono sagge. Solo qualche mese fa prendevamo in giro iraniani, russi e cinesi che, con la loro sfiducia automatica per tutto ciò che è americano, parlavano il bizzarro linguaggio della "sovranità dell'informazione". Cosa? Gli iraniani vogliono realizzare un sistema di posta elettronica nazionale per ridurre la loro dipendenza dalla Silicon valley? Un'idea inutile e insensata agli occhi di molti europei, che la giudicavano uno stupido spreco di risorse: come potrebbe competere con Gmail, con le sue videochat accattivanti e la sua immediatezza? Gli europei ci hanno provato a lanciare un loro motore di ricerca, ma è stato un fallimento. Una cosa è costruire aeroplani in grado di competere con i Boeing, un'altra è realizzare un sistema di posta. L'Europa non ci riuscirebbe mai, figuriamoci l'Iran!

Qualche settimana fa, però, l'Iran ha lanciato un sistema di posta elettronica nazionale. Chi è che ride adesso? Certo, l'Iran vuole la sua posta elettronica anche per poterla censurare e per spiare i suoi cittadini.



Ma ha capito perfettamente la geopolitica: affidarsi interamente alle infrastrutture di comunicazione straniere non è un buon sistema per rafforzare la propria sovranità. Se non vuoi che un altro paese gestisca il tuo sistema di posta, perché cedere il controllo delle comunicazioni elettroniche?

ella privacy



Terzo: la sensazione di vittoria assoluta provata dalla società civile negli Stati Uniti e in Europa in seguito al fallimento del programma Tia era stata prematura. Il Tia (Total information awareness) era un tentativo di instaurare una sorveglianza globale finanziato dall'agenzia per la ricerca e lo sviluppo del dipartimento della difesa degli Stati Uniti. Ma era troppo grande, troppo appariscente e troppo dipendente dalla burocrazia pubblica. Sono passati dieci anni e oggi abbiamo un sistema molto più agile e snello, più decentrato, gestito dal settore privato e reso possibile da un contratto sociale tra la Silicon valley e Washington: la Silicon valley gestisce, aggiorna e monetizza l'infrastruttura digitale, ma Washington può usarla a richiesta. Tutti si specializzano e tutti ci guadagnano.

Ecco gli Stati Uniti di oggi nel pieno del loro splendore: quello che non si può otte-

nere con leggi discutibili si ottiene grazie alla privatizzazione, ma con un grado molto minore di vigilanza e di controllo pubblico. Dalla sanità alle carceri fino alle milizie da inviare nelle zone di guerra, tutto è gestito privatamente. È questo il modello di partenariato pubblico-privato scelto oggi da molte infrastrutture statunitensi. Le comunicazioni non fanno eccezione. Il decentramento è liberatorio solo quando non c'è un attore principale che può accaparrarsi tutti i benefici una volta entrata in funzione la rete. Se questo attore esiste – nel nostro caso è l'Nsa – decentramento è un termine vuoto. Chi ha il potere ottiene di più e più in fretta, pagando meno per il privilegio.

L'asilo di Snowden

Quarto: l'idea che la digitalizzazione abbia dato inizio a un mondo nuovo dove le vecchie, sagge regole della realpolitik non valgono più si è dimostrata una sciocchezza. Non esiste un mondo a sé che genera un nuovo tipo di potere "digitale". C'è un solo mondo e un solo potere, con gli Stati Uniti al timone. L'amministratore delegato di Google, Eric Schmidt, e il direttore di Google Ideas Jared Cohen, un ex alto funzionario del dipartimento di stato passato a Google, hanno avuto la sfortuna di pubblicare un libro pronto ad assicurarci che non era più così – *La nuova era digitale* (Rizzoli Etas 2013) – appena pochi mesi prima delle rivelazioni di Snowden. Sono rari i libri che invecchiano così rapidamente. Provate a cercare il capitolo sui "richiedenti asilo internet": "Un dissidente che non può vivere liberamente sotto un'internet autoritaria e che si vede negare l'accesso alle reti di altri stati sceglierà di chiedere asilo fisico in un altro paese per avere la libertà virtuale in internet", sostengono gli autori. "Ottenere l'asilo virtuale potrebbe essere un primo passo importante verso l'asilo fisico, un segno di fiducia senza un impegno totale".

L'assoluta ingenuità di affermazioni come questa – basata sul presupposto che in qualche modo si possa "vivere" online così come si vive nel mondo fisico, e che la politica virtuale segua una logica diversa dalla politica tradizionale – è illustrata dal caso di Edward Snowden, un uomo con una nobile missione e pessime capacità di pianificazione dei viaggi. Se era un "asilo virtuale" che stava cercando, poteva godersi la sua dose di "libertà virtuale" all'aeroporto Sheremetevo di Mosca. Ma chissà perché sembra che la "libertà virtuale" non gli bastasse e non gli è venuto in mente (forse non aveva ancora letto il libro?) di

Il mito secondo cui esiste uno spazio virtuale e autonomo dove è possibile avere più privacy dalle istituzioni sociali e politiche è morto

richiedere "l'asilo virtuale". Il presidente boliviano Evo Morales, costretto ad atterrare in Austria perché sospettato di trasportare Snowden nel suo aereo, si sarebbe fatto una bella risata se gli fosse capitata tra le mani una copia della *Nuova era digitale* in una libreria dell'aeroporto di Vienna. Forse, se solo Morales avesse twittato di più, tutto questo non sarebbe successo.

Quinto: il vecchio e radicato mito secondo cui esiste uno spazio virtuale autonomo dove è possibile avere più privacy e indipendenza dalle istituzioni sociali e politiche è morto. Per capire perché, basta guardare la nota diffusa dalla Microsoft quando il Guardian ha rivelato che l'Nsa probabilmente intercettava le chat e le videochiamate di Skype (Skype è di proprietà della Microsoft). Nella mancata smentita della Microsoft si nasconde una frase molto particolare. Per giustificare la necessità di rendere compatibili i suoi prodotti digitali con le esigenze delle agenzie di sicurezza, il vicepresidente della Microsoft, Brad Smith, scrive che "in prospettiva, con l'aumentare delle comunicazioni audio e video via internet, è chiaro che i governi saranno interessati a usare (o a introdurre) strumenti giuridici al fine di garantirsi l'accesso a questo tipo di contenuti per indagare su crimini o per contrastare il terrorismo. Riteniamo pertanto che tutte le chiamate, sia via internet sia da rete fissa o mobile, avranno livelli simili di privacy e sicurezza". Rileggiamolo: un importante dirigente della Microsoft sostiene che rendere meno sicure le nuove forme di comunicazione è inevitabile, e probabilmente è anche un bene. Per gran parte degli anni novanta, tutti hanno creduto che la digitalizzazione avrebbe aperto la strada alla cosiddetta "convergenza", sicuramente un'ottima cosa per quanto riguarda la sicurezza. Il ragionamento era questo: passando a un'unica rete, le precedenti forme di comunicazione (il caro vecchio telefono e simili) diventeranno sicure come la posta elettronica cifrata. In realtà siamo andati nella direzione opposta. Quello che abbiamo oggi è sì un'unica rete, ma la sicurezza e la privacy sono tornate al livello della rete telefonica. È il telefono, non la posta elettronica cifrata, il nostro comune denominatore per quanto riguarda la sicurezza, almeno in termini di capacità di intercettazione. La convergenza c'è stata, ma, miracolosamente, le tecnologie sono riuscite a convergere sull'opzione meno sicura e più facile da sorvegliare.

Tutto questo ha implicazioni disastrose per chi vive in una dittatura. Quando la Microsoft e altre aziende tecnologiche cominciano a realizzare un software progettato per essere vulnerabile, incoraggiano i già vastissimi piani di spionaggio dei governi autoritari. Quello che né l'Nsa né i politici sembrano capire è che, in materia di infrastrutture digitali, la politica interna

Da sapere
I dati di Facebook

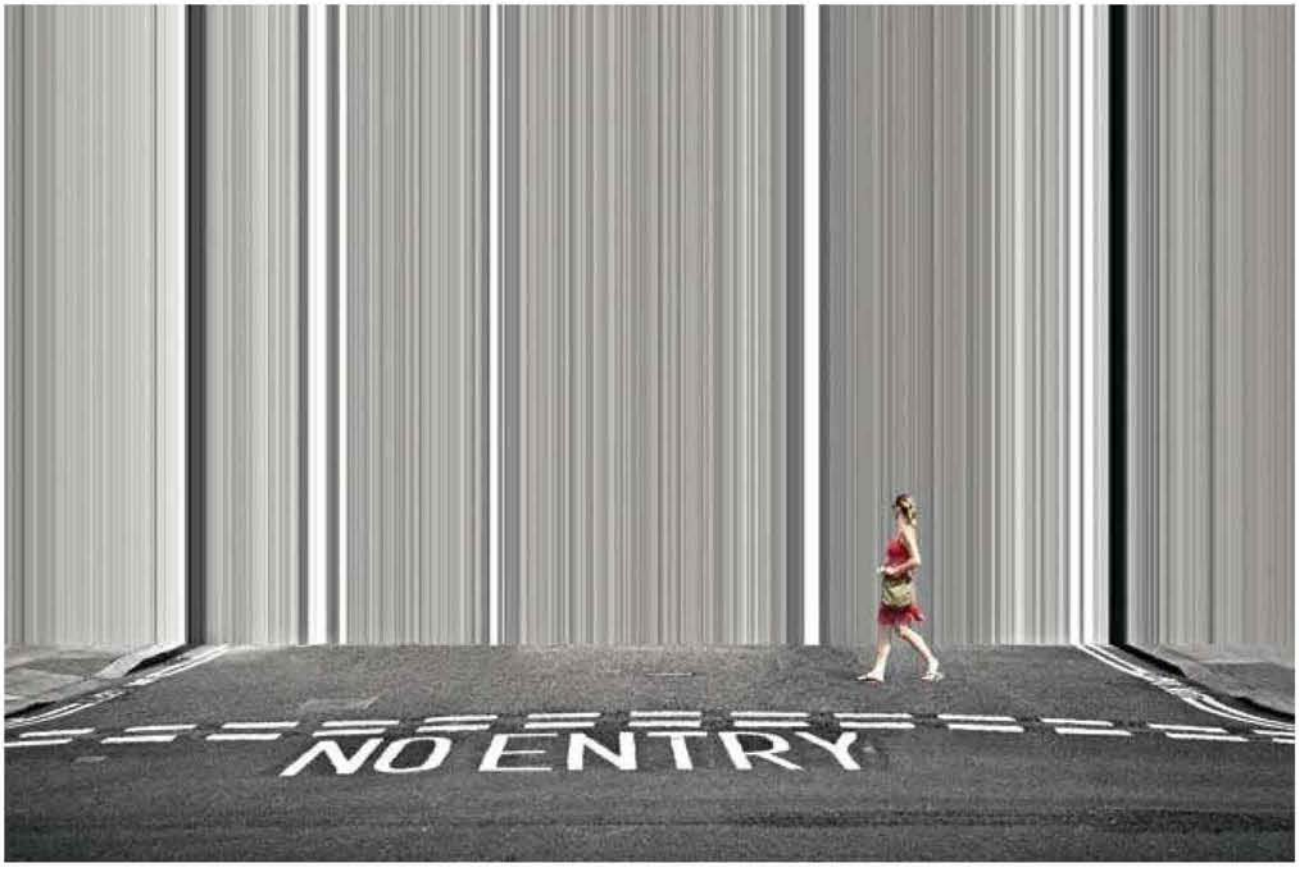
◆ Il 27 agosto Facebook ha pubblicato il suo primo rapporto sulle richieste di accesso al materiale degli utenti da parte di 74 governi di tutto il mondo. Il rapporto si riferisce ai primi sei mesi del 2013. "Siamo convinti che sia possibile proteggere i cittadini affiancando la trasparenza all'impegno degli enti governativi", ha scritto il consulente legale di Facebook, Colin Stretch. "La chiarezza di questi ultimi e la pubblica sicurezza non sono valori inconciliabili, ma ideali che possono convivere all'interno di società libere e che contribuiscono a renderci ancora più forti".

I paesi che hanno fatto più richieste di informazioni a Facebook

	Richieste totali	Account interessati	% di risposte*
Stati Uniti	11.000 - 12.000	20.000 - 21.000	79
India	3.245	4.144	50
Regno Unito	1.975	2.337	68
Germania	1.886	2.068	37
Italia	**1.705**	**2.306**	**53**
Francia	1.547	1.598	39
Brasile	715	857	33
Australia	546	601	64
Spagna	479	715	51
Polonia	233	158	9
Taiwan	229	329	84
Cile	215	340	68

Richieste per le quali sono stati rilasciati alcuni dati

FONTE: FACEBOOK



è anche politica estera: è inutile affrontarle separatamente. Vogliamo catturare tutti i terroristi prima che compiano un attentato? Benissimo, i *big data* sono qui per aiutarci. Ma non dimentichiamo che possono aiutare anche i governi della Cina e dell'Iran a catturare in anticipo i futuri dissidenti. Non possiamo costruire infrastrutture di comunicazione vulnerabili e aspettarci che siano solo i governi occidentali ad approfittarne.

La retorica della libertà

Questo ci porta alla conseguenza più problematica delle rivelazioni di Snowden. Per quanto possa essere critica la situazione in Europa, saranno gli utenti degli stati autoritari a soffrire di più. E non per la sorveglianza statunitense, ma per la censura interna. Come mai? L'aspirazione di Russia, Cina o Iran alla "sovranità dell'informazione" non è semplicemente un modo per mettere i loro cittadini al riparo dalla sorveglianza statunitense. Incoraggerebbe i governi autoritari a essere più aggressivi nel dirottare le comunicazioni pubbliche tra i cittadini – che in larga misura usano ancora Facebook e Twitter – verso degli equivalenti nazionali di questi servizi.

I governi autoritari hanno buoni motivi per temere Twitter e Facebook, sui quali esercitano molto meno controllo. Probabilmente non è una coincidenza che LiveJournal, il social network preferito della Russia, abbia improvvisamente avuto problemi di manutenzione, e quindi sia stato inutilizzabile, proprio quando un tribunale russo ha emesso la sentenza contro Aleksej Novalnyj, il blogger e attivista che ha denunciato la corruzione di Vladimir Putin. Nonostante i timori di una possibile americanizzazione e sorveglianza generalizzata, servizi basati negli Stati Uniti come Facebook e Twitter continuano a difendere la libertà di espressione meglio delle loro controparti russe, cinesi o iraniane. Questi paesi censurano di più e, come dimostra l'esempio di LiveJournal (che appartiene a un oligarca russo), possono interrompere le comunicazioni quando lo ritengono politicamente opportuno. Un dissidente politico che dovesse scegliere se organizzare le sue proteste su Facebook o sull'equivalente russo, Vkontakte, farebbe bene a preferire Facebook. I governi dei regimi meno democratici cercheranno sicuramente di sfruttare il populismo antiamericano provocato dalle rivelazioni di Snowden per lasciare a chi protesta un'unica opzione, quella nazionale.

È questa la vera tragedia dell'*internet freedom agenda*, l'ambizione statunitense di difendere la libertà della rete: saranno i dissidenti in Cina e in Iran a pagare per l'ipocrisia che l'ha ispirata fin dall'inizio. Gli Stati Uniti sono riusciti a perseguire i loro interessi nel campo delle comunicazioni appellandosi ad alti princìpi morali e usando espressioni ambigue come "libertà di internet" per nascondere le tante e profonde contraddizioni della loro politica. In materia di "libertà di internet" – uno slogan più accattivante della "difesa della democrazia" – gli Stati Uniti godevano di una certa legittimazione quando sostenevano di non esercitare la sorveglianza che condannavano in Cina o in Iran. Allo stesso modo, in materia di attacchi informatici potevano criticare il ciberspionaggio cinese o iraniano perché assicuravano al mondo di essere estranei a questi metodi.

Entrambe le affermazioni erano palesemente false, ma finché non ci sono state le prove gli Stati Uniti hanno potuto guadagnare tempo e influenza. Quei giorni sono ormai lontani. Oggi la retorica dell'*internet freedom agenda* sembra affidabile quanto la *freedom agenda* di George Bush dopo Abu Ghraib. Washington dovrà ripensare la sua politica. Ma invece di perseguitare

Snowden dovrebbe ringraziarlo. Ha solo messo a nudo le fragili fondamenta di scelte insostenibili, costruite intorno a termini vaghi e ambigui come *internet freedom* e guerra informatica. Scelte che in ogni caso non sarebbero sopravvissute alle complessità della politica globale.

Che fare? Cominciamo dalla sorveglianza. Fino a oggi, quasi tutti i politici europei hanno puntato alla soluzione più semplice, la legge, pensando che se fossero riusciti a disciplinare le aziende statunitensi, per esempio costringendole a rivelare quanti dati forniscono all'Nsa e quando, il problema sarebbe venuto meno. È una posizione piuttosto miope e ingenua che riduce un enorme problema filosofico – il futuro della privacy – alla dimensione apparentemente gestibile delle direttive sulla conservazione dei dati. Magari fosse così semplice! Le difficoltà attuali dipendono dall'ideologia di fondo, non da politiche sbagliate né dalla loro pessima attuazione. Con questo non intendo oppormi a una maggiore regolamentazione delle aziende tecnologiche: l'Europa avrebbe dovuto imboccare questa strada una decina di anni fa, invece di farsi intrappolare dalla inebriante retorica della "nuvola informatica". Voglio sottolineare però che ci aspetta un compito molto più impegnativo a livello intellettuale.

Lo spazzolino smart

Supponiamo, per un momento, che l'Europa possa imporre tutte le leggi che vuole alle aziende tecnologiche statunitensi. È un'ipotesi estremamente improbabile vista la forza crescente delle loro lobby a Bruxelles, ma lasciamo da parte questo aspetto. Cosa succederà tra cinque anni, quando tutti gli oggetti e i dispositivi diventeranno *smart*, cioè avranno dei sensori avanzati e poco costosi, e saranno collegati tra loro e con internet? Molti oggetti di questo tipo sono già in commercio, e molti altri lo saranno presto: forchette smart che misurano la velocità con cui mangiamo, spazzolini smart che controllano quante volte ci laviamo i denti, scarpe smart che ci dicono quando sono consumate, ombrelli smart che vanno online per sapere se pioverà e ci ricordano di prenderli quando stiamo per uscire di casa. E poi, naturalmente, c'è lo smartphone che abbiamo in tasca e, presto, ci saranno gli occhiali di Google che porteremo sul naso.

Tutti questi oggetti lasciano delle tracce di dati. Basta raccogliere informazioni da diversi oggetti di questo tipo e metterle insieme per trarre le stesse deduzioni e previsioni che l'Nsa ottiene sorvegliando le nostre email o i tabulati telefonici. In altri termini, l'Nsa può sapere dove ci troviamo controllando il nostro cellulare oppure ottenendo dati dalle scarpe smart o dall'ombrello intelligente. Allo stesso modo, non sarà necessario installare una videocamera nella nostra cucina per sapere cosa abbiamo mangiato: potranno capirlo manipolando lo spazzolino smart nel bagno o il secchio della spazzatura intelligente in cucina. Se non teniamo conto di questi nuovi dispositivi, non ha molto senso costruire il sistema di posta elettronica o la rete mobile più sicuri del mondo: l'Nsa riuscirà a ottenere dati con altri mezzi, più creativi.

Le implicazioni della scelta di commercializzare i dati personali non riguardano solo i mercati e l'economia, ma anche l'etica

Potrebbe perfino comprarli. Alcuni liquidano questi timori sostenendo che le nostre comunicazioni via email sono troppo personali per essere vendute come un prodotto commerciale. È vero. Eppure non abbiamo nulla da ridire se l'algoritmo di Google setaccia le nostre email per presentarci annunci pubblicitari mirati. È questa pubblicità personalizzata, che si basa sull'analisi e la classificazione immediata e automatica, a mantenere gratuito il raffinato e costoso sistema di posta elettronica di Google. Si noti che è questo tacito accordo, in base al quale Google può usare un algoritmo per analizzare le nostre email e venderci annunci pubblicitari mirati, a rendere le nostre email gratuite e allo stesso tempo accessibili all'Nsa. Google non avrebbe problemi a crittografare i nostri messaggi in modo che i suoi stessi algoritmi non riescano a decifrarli, privando se stesso e l'Nsa di dati preziosi. Ma in questo caso non potrebbe offrirci un servizio gratuito, e chi ne sarebbe contento?

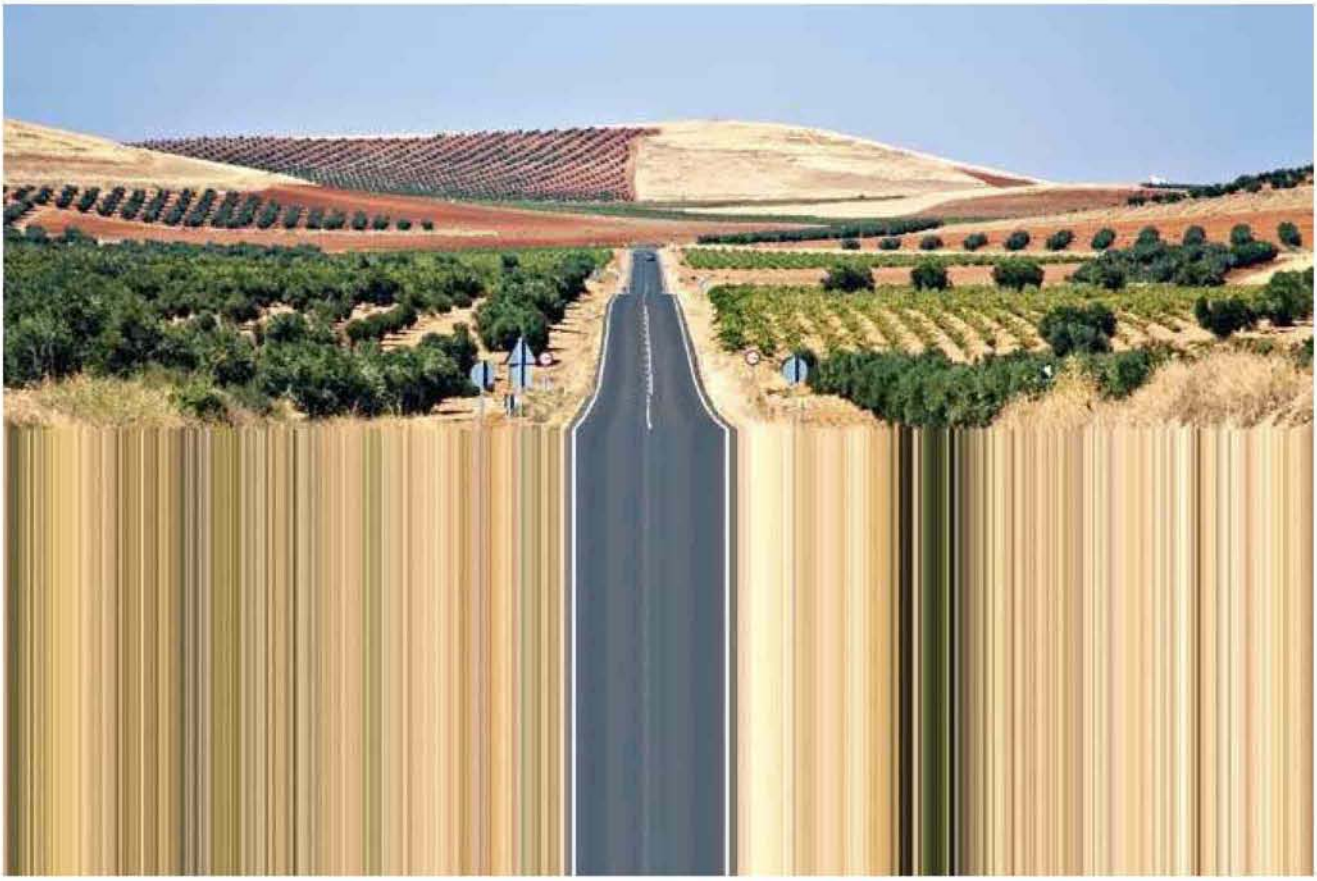
Quando i nostri dispositivi e altri oggetti analogici saranno diventati smart, il modello di Gmail si diffonderà in ogni settore. Una serie di imprese commerciali ci fornirà oggetti e dispositivi gratuiti o con un prezzo pari solo a una piccola parte del loro costo reale. In altri termini, il nostro spazzolino da denti intelligente sarà gratis, ma in cambio accetteremo che raccolga dati su come lo usiamo. Saranno questi dati a finanziare lo spazzolino. Oppure, per oggetti con schermi e altoparlanti, potremo vedere o sentire una pubblicità personalizzata che si basa sull'uso che ne facciamo, e sarà la pubblicità a coprire i costi. È il sistema già adottato da Amazon con i suoi lettori Kindle: se vogliamo un modello più economico, dobbiamo solo accettare la pubblicità sullo schermo. Il vero patto faustiano di Amazon sarebbe quello di offrirci gratis sia il lettore sia l'accesso istantaneo a tutti i libri del mondo a una sola condizione: accettare che analizzino tutte le nostre letture e ci propongano della pubblicità su misura.

Seguendo un modello leggermente modificato – già disponibile grazie a diverse startup note come *personal data lockers*, archivi dati personali – possiamo fare soldi vendendo noi stessi i nostri dati, e non solo quelli dello spazzolino, ma di ogni oggetto intelligente che usiamo: l'automobile, la scrivania, il secchio dell'immondizia. Una startup, Miinome, vi permette perfino di fare soldi mettendo online il vostro codice genetico: ogni volta che una società lo consulta – magari per personalizzare la pubblicità o per usarlo in un esperimento di *big data* – ricevete una piccola somma.

Sostanzialmente, la possibilità di inserire un sensore e un collegamento internet in qualunque cosa, compreso il corpo umano, consente di mercificare tutto e di attribuire un prezzo alle informazioni che se ne ricavano. I sensori e la connettività permanente contribuiscono a creare nuovi mercati nel campo dell'informazione, permettendo ai cittadini di monetizzare l'autosorveglianza.

Leggi inutili

Se questo è davvero il futuro verso cui ci stiamo dirigendo, è chiaro che le leggi non ci saranno di grande aiuto, perché i cittadini sceglierebbero volontariamente questo tipo di transazioni, così come già oggi scegliamo un servizio di posta elettronica gratuito (ma controllabile) e lettori di ebook più economici (ma finanziati dalla pubblicità). Le spie dell'Nsa avranno due possibilità: chiedere dati alle aziende che costrui-



scono questi oggetti intelligenti oppure acquistarli sul mercato, visto che i dati finiranno con l'essere commercializzati da noi cittadini. In altre parole, quello che oggi viene raccolto grazie a mandati e ordini di tribunale potrebbe essere ottenuto con semplici transazioni commerciali.

I politici convinti che le leggi possano fermare la mercificazione delle informazioni si illudono. Questa mercificazione non avviene contro la volontà dei cittadini comuni, avviene perché è proprio questo che vuole il cittadino-consumatore comune. Nessuno è costretto a usare Gmail o il Kindle: lo facciamo volontariamente. Lasciate perdere le leggi: è solo con l'attivismo politico e con una robusta critica intellettuale dell'ideologia del "consumismo informativo" che possiamo riuscire ad allontanare l'inevitabile catastrofe.

Da dove può partire questa critica? Consideriamo quello che in un primo momento potrebbe sembrare un parallelo bizzarro: il cambiamento climatico. Per buona parte del novecento abbiamo creduto di pagare un prezzo giusto per i nostri consumi energetici e che esistesse solo il paradigma consumistico "sono libero di usare tutta l'energia che posso pagare". In base a questo paradigma, non ci sono questioni etiche legate ai nostri consumi energetici: la logica del mercato ha sostituito la moralità, ed è stato proprio questo a consentire alti tassi di crescita economica e la proliferazione di dispositivi che hanno trasformato le nostre case in paradisi elettronici che ci liberano da faticosi lavori domestici. Ma come abbiamo scoperto nell'ultimo decennio, questo modo di pensare si fondava sulla grande illusione che il prezzo dell'energia fosse equo e che noi pagassimo la nostra giusta quota.

Ma ovviamente non abbiamo mai pagato il prezzo giusto per i nostri consumi energetici, perché non abbiamo mai considerato la possibilità che la vita sulla Terra potrebbe finire anche se pareggiassimo tutti i nostri rendiconti finanziari. Perciò oggi la decisione di quale macchina guidare o di quanta luce avere in salotto non è condizionata solo dalla nostra capacità di pagare l'elettricità, è anche una decisione etica che ciascuno prende personalmente. Il punto è che, grazie anche alle fortunate campagne del movimento ambientalista, una serie di decisioni puramente razionali e basate sul mercato tutt'a un tratto hanno assunto una rilevanza politica che ci ha dato macchine progettate in modo diverso, luci che si spengono automaticamente se la stanza è vuota, eccetera. Ha anche prodotto cittadini incoraggiati, almeno in teoria, che non si preoccupano solo di quanto costa la bolletta della luce.

Questo parallelo con la condivisione delle informazioni potrebbe apparire bizzarro, ma in realtà non è così strano. Oggi la decisione di comprare uno spazzolino intelligente con un sensore incorporato, e di vendere i dati che genera, ci viene presentata come una scelta puramente commerciale che riguarda solo noi. In realtà è così solo perché non riusciamo a immaginare un disastro informativo con la stessa facilità di una catastrofe ambientale. Non siamo più capaci di immaginare utopie negative, e la colpa in parte è dei nostri intellettuali tecnofili, innamorati della Silicon valley e di termini alla moda come "innovazione". Ma il fatto che la catastrofe sia lenta e non si presti facilmente a una vivida visualizzazione non significa che sia meno grave.

Il fattore etico

Quello che ci serve è una visione più nitida e cruda dell'apocalisse informativa che ci attende in un mondo dove i dati personali sono commercializzati come il caffè o qualunque altra merce. Prendiamo per esem-

pio la tesi secondo cui cedere i nostri dati in cambio di un tangibile vantaggio commerciale è conveniente. Poniamo che installiate un sensore nell'auto per dimostrare alla vostra assicurazione che guidate con maggiore prudenza dell'autista medio previsto dalla polizza standard. Ottimo: se siete più prudenti della media pagherete meno. Ma il problema della media è che metà della popolazione è sempre al di sotto del punto di riferimento. Inevitabilmente, che voglia farsi sorvegliare o meno, questa metà sarà costretta a pagare di più, perché se i più bravi di noi accetteranno di registrare i propri comportamenti, gran parte delle istituzioni sociali arriverà alla conclusione (piuttosto logica) che chi rifiuta di farlo ha qualcosa da nascondere. Perciò le implicazioni della scelta di commercializzare i dati personali non riguardano solo i mercati e l'economia, riguardano anche l'etica. Se la decisione di cedere i miei dati personali per un po' di soldi peggiora la situazione di qualcun altro e lo priva di opportunità, allora devo prendere in considerazione anche un fattore etico, l'economia non basta.

Tutto questo per dire che il consumismo informativo ha profonde conseguenze politiche e morali, paragonabili al consumismo energetico per portata e significato. Intellettuali e politici dovrebbero impegnarsi per rendere più vivide e chiare queste conseguenze. Dovremmo fare di tutto per contrastare l'apparente normalità economica dello scambio di informazioni. Considerarli "solo affari" non basterà più.

La condivisione di informazioni può anche avere un florido mercato, ma non ha un inquadramento etico che la sostenga. Più di trent'anni fa, Michel Foucault aveva saputo prevedere che il neoliberismo ci avrebbe trasformati in "imprenditori di noi stessi". Ma non dimentichiamo che fare l'imprenditore ha i suoi lati negativi: come quasi tutte le attività economiche può avere effetti indesiderati, per esempio l'inquinamento. Fare gli imprenditori dello scambio di informazioni non fa eccezione.

I politici europei possono cercare di imporre tutte le leggi che vogliono, ma fino a quando il consumismo dominerà incontrastato e la gente non avrà una chiara spiegazione etica del perché non dovrebbe guadagnare vendendo i propri dati, il problema continuerà a esistere. La sorveglianza dell'Nsa, il grande fratello, Prism: sono tutte cose importanti. Ma è altrettanto importante guardare il quadro d'insieme, e in questo quadro d'insieme è il consumismo informativo a dover essere analizzato, non solo il complesso militare-industriale responsabile della sorveglianza. Fino a quando non avremo una spiegazione esauriente dei motivi per cui un dato non dovrebbe essere messo sul mercato, non potremo illuderci di proteggerlo dall'Nsa, perché, anche con una regolamentazione più severa, le agenzie di intelligence si limiterebbero a comprare sul mercato quello che oggi ottengono segretamente da programmi come Prism.

Non possiamo più trattare internet come un settore qualunque, sperando di riuscire a sviluppare una serie di competenze specifiche

La vera minaccia

Alcuni potrebbero dire: se solo avessimo un partito per le questioni digitali. Difficile fare un errore più grosso. È sbagliato pensare che tutta questa roba digitale possa essere incasellata e delegata a giovani brillanti che sanno come cavarsela. Questa "roba digitale" è di fondamentale importanza per il futuro della privacy, dell'autonomia, della libertà e della stessa democrazia: questioni che dovrebbero essere prioritarie per ogni partito politico. Per un grande partito, rinunciare alla responsabilità del "digitale" significa abdicare alla responsabilità del futuro della democrazia.

I "problemi digitali" devono coinvolgere tutti, e non essere ghettizzati nelle mani e nei programmi dei partiti pirata e di chiunque prenderà il loro posto. Non possiamo più trattare internet come una questione qualunque, sperando di riuscire a sviluppare una serie di competenze specifiche. Piuttosto, occorre che questioni più attuali – "privacy" o "soggettività" – siano in primo piano. Dimenticate gli obiettivi ambiziosi come la libertà di internet: sono un'illusione e non vale la pena cercare di raggiungerli. Dobbiamo concentrarci sulla creazione di ambienti dove la vera libertà può ancora essere coltivata e preservata.

Il tragico errore dei Pirati è stato cercare di fare troppo: volevano cambiare sia il sistema della politica sia i suoi contenuti. Un progetto così ambizioso era destinato a fallire. Inoltre, l'utilità politica di cambiare il sistema – che fosse una spinta verso una più larga partecipazione o verso una maggiore trasparenza delle procedure legislative – è tutta da discutere: le riforme promosse dai Pirati non sembravano nascere da lunghe riflessioni critiche sulle insidie dell'attuale sistema politico, ma dalla loro convinzione che il sistema stesso, incompatibile con le maggiori piattaforme digitali da Wikipedia a Facebook, dovesse essere rimodellato a loro immagine. Questa era e rimane una sciocchezza. Un parlamento è sicuramente diverso da Wikipedia, però il successo dell'enciclopedia aperta non ci dice assolutamente nulla sulla possibilità di prendere Wikipedia come modello su cui riconfigurare le nostre istituzioni (e sia chiaro: sono tutt'altro che perfetti, questi parlamenti, come ha dimostrato la crisi finanziaria). Ma l'elemento positivo dei partiti pirata è la sollecitazione a riflettere sulle questioni digitali e le loro conseguenze per il futuro della democrazia. Questa è la parte relativa al contenuto, non al sistema. È un progetto che deve continuare ma, forse, riorientarsi, passando dal perseguimento del falso obiettivo della libertà di internet alla riflessione su come salvaguardare la vera libertà. È stato un bene per la democrazia che il caso Snowden ci abbia costretto a misurarci con questi problemi. Guardiamo le cose in faccia: la maggior parte di noi preferisce non pensare alle implicazioni etiche degli spazzolini intelligenti o all'ipocrisia della retorica occidentale nei confronti dell'Iran o alle genuflessioni dei leader europei davanti alla Silicon valley e al suo linguaggio che danneggia il cervello, il siliconese. Il minimo che possiamo fare è riconoscere che la crisi è molto più profonda e ha ragioni non solo giuridiche, ma anche intellettuali. Il consumismo informativo, come il suo fratello maggiore, il consumismo energetico, è una minaccia per la democrazia molto più grave dell'Nsa. ◆ *gc*

L'AUTORE

Evgeny Morozov è un intellettuale bielorusso esperto di tecnologia e di internet che vive negli Stati Uniti. Ha scritto *L'ingenuità della rete* (Codice 2011). Il suo ultimo libro pubblicato in Italia è *Contro Steve Jobs* (Codice 2012).