DOPPIOZERO

Sorvegliati di tutto il mondo, unitevi!

Oliviero Ponte Di Pino 7 Gennaio 2020

Secondo Comscore, su internet la visualizzazione di una pagina dura in media 26 secondi. Il 99,8 per cento delle visualizzazioni dura meno di dieci minuti. Leggere questo articolo fino in fondo sarebbe un comportamento marginale, residuale. Per gli algoritmi è irrilevante, anomalo, forse addirittura patologico.

La logica dei signori della rete è impeccabile, efficientissima. Ma questa logica ci sta fregando, o forse ci ha già fregato. Perché accanto alla rete in cui navighiamo inconsapevoli, sono state create altre reti. Non le vediamo e proprio per questo sono ancora più importanti.

I due internet secondo Matthew Hindman

Esistono due internet, secondo Matthew Hindman, autore di *La trappola di internet* (traduzione di Daniele A. Gewurz, Einaudi, Torino, 2019, 286 pagine, 22 €). La prima è “l'internet 'di cui tutti sanno', che sta democratizzando la comunicazione e la vita economica”. L'aveva profetizzata nel 1996 John Perry Barlow in *A declaration of independence of cyberspace* (1996): la rete sarà immune a qualsiasi regola e completamente separata dal “Mondo Industriale”, destinata a diventare “la nuova casa della Mente”, in cui “qualunque cosa la mente umana possa creare può essere riprodotta e distribuita all'infinito senza alcun costo. Il trasferimento globale del pensiero non richiede più le vostre fabbriche”.

Poi c'è l'internet reale, dove “un terzo di tutte le visite web va alle prime dieci aziende” e che “consente a due aziende di controllare più della metà delle entrate pubblicitarie online” (p. 201) e il 70 per cento della pubblicità online negli USA.
Hindman, professore associato di Media and Public Affairs e consulente della

Federal Communication Commission statunitense, ha analizzato e modellizzato l'evoluzione dell'economia della rete. Le sue conclusioni sono drastiche. Il fattore decisivo per avere successo online è la *stickiness*, ovvero la capacità di un sito di attrarre e conservare i visitatori. L'obiettivo è quello che gli economisti chiamano *lock in*, che si realizza quando i costi di passaggio a un altro fornitore superano i possibili benefici.

L'errore di prospettiva è stato pensare che con il World Wide Web i costi di distribuzione delle informazioni si sarebbero azzerati: si sono solo spostati dal mondo fisico a quello virtuale. Non servono più camion, navi o aerei e fattorini, ma le *server farms* con migliaia di computer che inghiottono giganteschi flussi di energia, e sistemi di commutazione con una larghezza di banda di diversi terabyte al secondo, progettati e gestiti da un'aristocrazia di ingegneri del software. Il tutto affinato da continui e costosi test A/B per valutare le soluzioni migliori anche nei dettagli: dai titoli più efficaci ai pixel di un carattere o a una sfumatura di colore. Per quanto riguarda le notizie, la quantità vale più della qualità: “i consumatori leggono una gran quantità di contenuti mediocri e poco costosi” (p. 93). Meglio raffiche di spazzatura che reportage documentati e inchieste validate dal *fact checking*, meglio il gattino in bottiglia o il pettegolezzo sexy della recensione.


PRIVACY GIFT SHOP
ANYTHING YOU SAY OR DO CAN AND WILL BE USED AGAINST YOU IN A TARGETED ADVERTISEMENT
think privacy
A PUBLIC SERVICE ANNOUNCEMENT FROM PRIVACYGIFTSHOP.COM
©ADAM R. HARVEY 2018

Il metodo di raccomandazione/filtraggio (per consigliare un libro su Amazon, una pagina su Google, un film su Netflix, un post su Facebook, un ristorante su Tripadvisor) si è via via affinato. Inizialmente a essere privilegiati erano i contenuti *più popolari*. In una seconda fase è intervenuto il *filtraggio collaborativo* : “via via che il sistema registra una quantità maggiore di dati sui clic, le raccomandazioni si basano sempre più sul comportamento passato degli utenti e degli interessi dimostrati” (p. 69). Ha fatto progressi anche la gestione dei *contenuti*, che usa “l'analisi del testo per abbinare gli utenti con i tipi di articoli che hanno apprezzato in passato” (p. 68). Le strategie più efficaci utilizzano un modello ibrido, che combina questi tre approcci.

Nella lotta per la *stickiness* un piccolo vantaggio porta nel lungo periodo a “enormi differenze nel numero di visitatori” (p. 61). Le economie di scala favoriscono le imprese maggiori e creano monopoli, esattamente come era successo alla fine dell'Ottocento con i *robber barons*, gli odiati signori dell'acciaio e delle ferrovie. In rete trionfano i giganti. Oggi “internet non è affatto un ecosistema, ma un paio di monoculture commerciali” (p. 221)

Contro chi continua a considerare la rete il Paradiso dell'innocenza egualitaria, le analisi di Hindman dimostrano che negli USA, mentre i giornali locali “di carta”, una delle spine dorsali della democrazia americana, chiudono uno dopo l'altro, le nuove testate online restano marginali.

Oltre a sottrarre pubblicità ai media tradizionali, Facebook e Google hanno affinato meccanismi “personalizzati” che promettono agli inserzionisti un'efficacia molto maggiore. Gli algoritmi usati dai giganti dei web funzionano per sei ordini di ragioni:

“i sistemi di raccomandazione possono aumentare notevolmente il pubblico”;

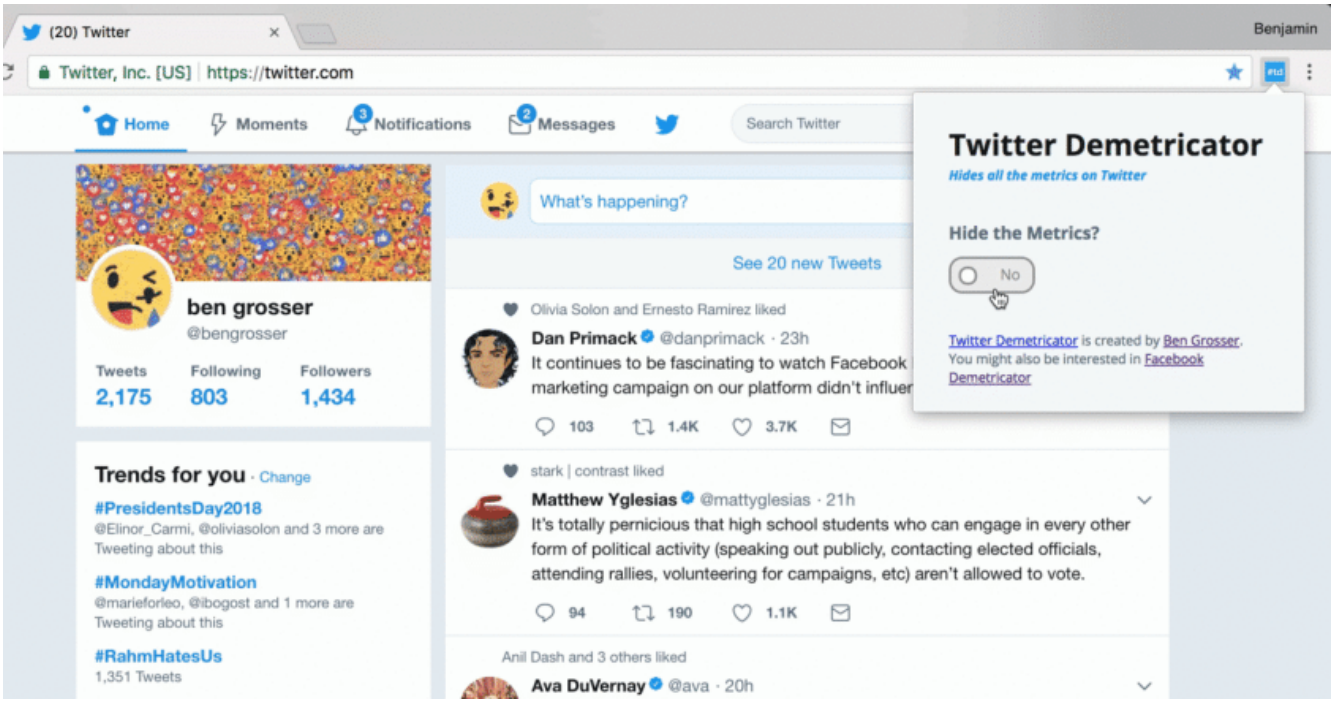
e “favoriscono le aziende digitali con ampi contenuti”;

“avvantaggiano le imprese con hardware migliore e personale più qualificato”;

e “favoriscono le imprese con più dati”, ovvero “i siti più popolari e più frequentati”;

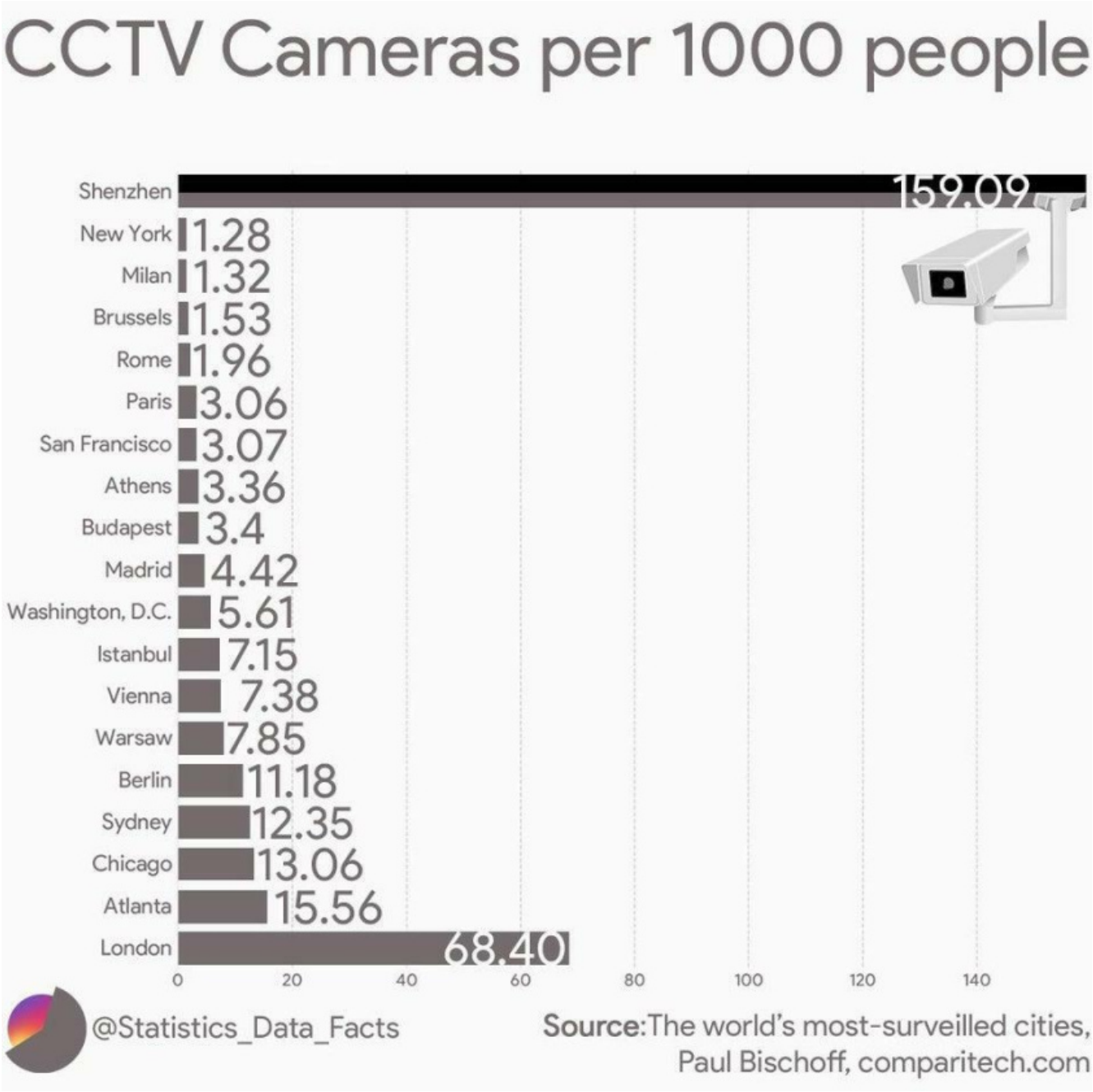
“i sistemi di personalizzazione promuovono il *lock-in*”;

“i sistemi di suggerimenti incoraggiano la concentrazione del pubblico” (pp. 75-77).



Risultato? Se un sito raddoppia il suo pubblico, le sue entrate pubblicitarie saranno più del doppio (e i profitti cresceranno grazie alle economie di scala). Oltretutto “il pubblico dei grandi siti è molto più costante di quello dei siti più piccoli”, anche se “le fluttuazioni quotidiane del traffico rendono stabile la *struttura* del web” nel suo insieme. Ignoriamo se tra due o cinque anni Doppiozero avrà più o meno visite di oggi, ma sappiamo quante visite avrà il sito che occupa la sua posizione nella classifica del traffico. E la top ten cambierà di poco, a meno di clamorosi fallimenti (p. 106).

C'è un'altra costante, secondo Hindman: “la percentuale di pubblico che cerca le notizie rimane stabile da vent'anni al 3 per cento circa” (p. 203), limitato da una feroce *competizione per l'attenzione*. La conseguenza politica è immediata: “La nuova organizzazione politica basata sui dati beneficia di economie di scala enormi. La fortissima concorrenza per l'attenzione fa sì che sia ancora più difficile per gli attivisti su piccola scala farsi notare” (p. 208). Le vittorie elettorali di Barack Obama, Donald Trump e Boris Johnson, basate sui big data e sui meccanismi portati alla luce dallo scandalo su Cambridge Analytica, sembrano confermare questa ipotesi, anche se il successo planetario dei Fridays for Future di Greta e l'epidemia delle sardine in Italia lascia qualche speranza (anche se per certi aspetti questi due movimenti restano in una sfera pre-politica).



I due internet secondo Shoshana Zuboff

Esistono due internet anche per Shoshana Zuboff, professoressa alla Harvard Business School e autrice del poderoso *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri* (traduzione di Paolo Bassotti, Luiss, Roma, 2019, 622 pagine, 25 €).

Il “primo testo” è quello che vediamo (o meglio, quello che potremmo vedere): sono i contenuti che ciascuno di noi pubblica (gratuitamente) sui social e in rete, e le nostre interazioni di tutti i generi ormai digitalizzate, per esempio quando facciamo la spesa, paghiamo una bolletta o andiamo dal medico. Come ha spiegato Hal Varian, a lungo *chief economist* di Google, “al giorno d'oggi c'è un computer di mezzo in quasi ogni transazione […] e ora che sono disponibili, tali computer vengono utilizzati in tanti altri modi” (p. 74). In particolare servono per:

l'estrazione e l'analisi dei dati;

le nuove forme contrattuali dovute a un miglior monitoraggio (pensate alle assicurazioni...);

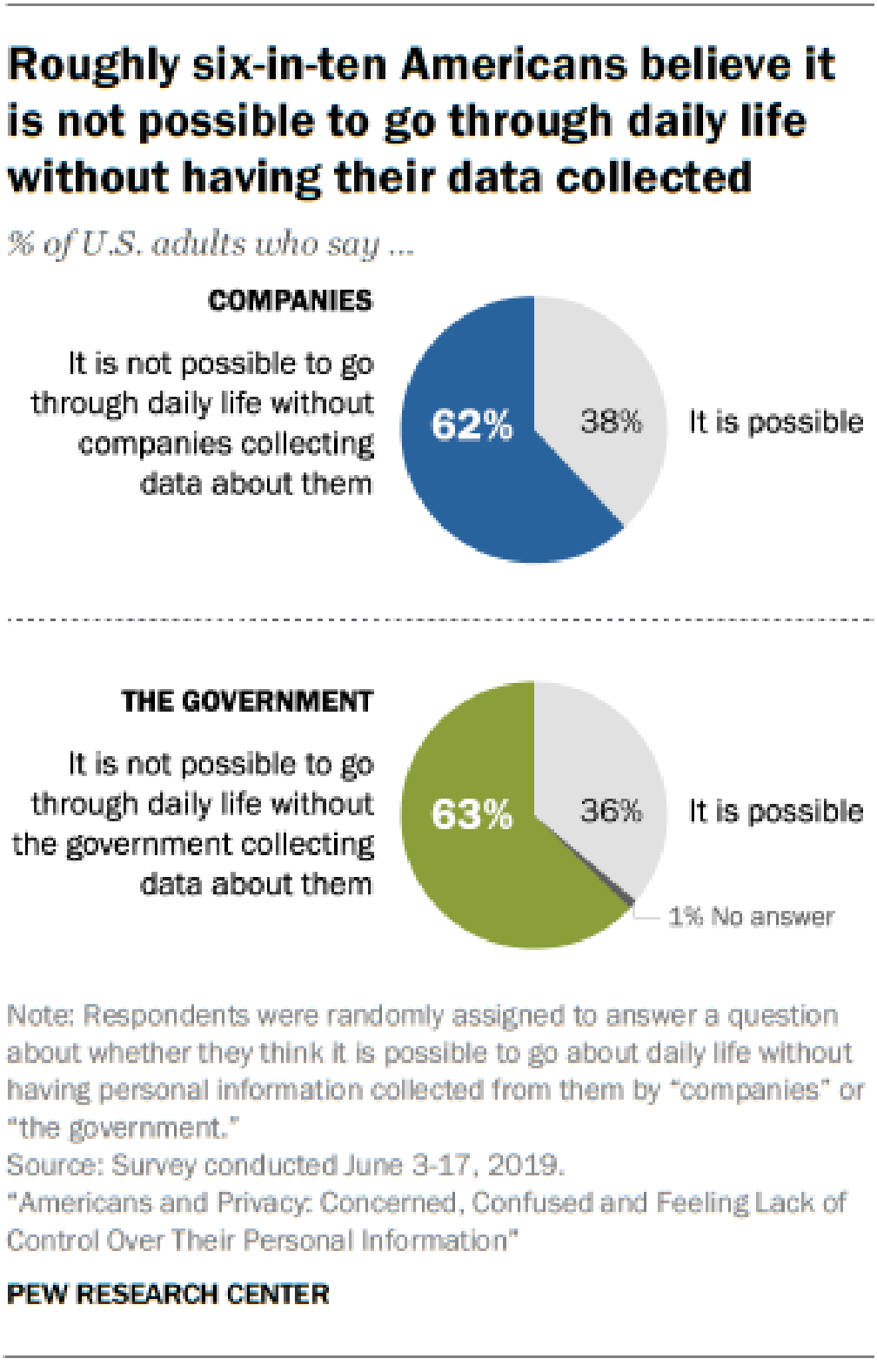
la personalizzazione e customizzazione;

gli esperimenti continui (ovviamente a insaputa delle cavie, cioè noi).

Questo primo testo – la nostra impronta digitale – è talmente gigantesco che nessun cittadino è in grado di vedere le informazioni che contiene (e men che meno di controllarle ed eventualmente farle correggere). Oltretutto molte di queste informazioni sono state raccolte a nostra insaputa, in violazione di qualunque principio di privacy e senza alcuna possibilità di controllo: “il diritto alla privacy, alla conoscenza e al suo uso è stato usurpato da un mercato aggressivo che ritiene di poter gestire unilateralmente le esperienze delle persone e le conoscenze da esse ricavate” (p. 17).

In una prima fase questi dati venivano utilizzati a favore dell'utente, per garantirgli un servizio più efficace. Ma a partire dal 2002, in seguito allo scoppio della bolla di internet e all'imperativo di massimizzare i profitti, questo *surplus comportamentale* è stato dirottato a favore degli inserzionisti: le informazioni (espropriate agli utenti) hanno prodotto un advertising mirato, attraverso forme di *user profile information* sempre più accurate (grazie alle economie di scala e agli effetti di rete), in grado di “inferire e dedurre i pensieri, le emozioni, le intenzioni e gli interessi di individui e gruppi” (p. 91) con crescente precisione.

Oggi Google estrae surplus comportamentale da “qualunque elemento del mondo digitale: ricerche, email, messaggi, foto, canzoni, chat, video, luoghi, schemi comunicativi, atteggiamenti, preferenze, interessi, volti, emozioni, malattie, social network, acquisti e così via” (p. 139). Ma non è solo Google. L'estrazione è sistematica, ossessiva, invasiva. Già nel 2015 “chiunque avesse visitato i 100 siti più popolari aveva raccolto più di 6000 cookie nel proprio computer, l'83 per cento dei quali appartenenti a parti terze non correlate al sito visitato” (p. 146).



Secondo Zuboff, ci siamo comportati come gli indigeni ai quali i colonizzatori facevano firmare contratti che non potevano capire, cedendo la proprietà delle terre in cambio di collanine e perle di vetro. In questo modo la nostra vita privata, la nostra esperienza e la nostra intimità ci sono state sottratte, in un "ciclo

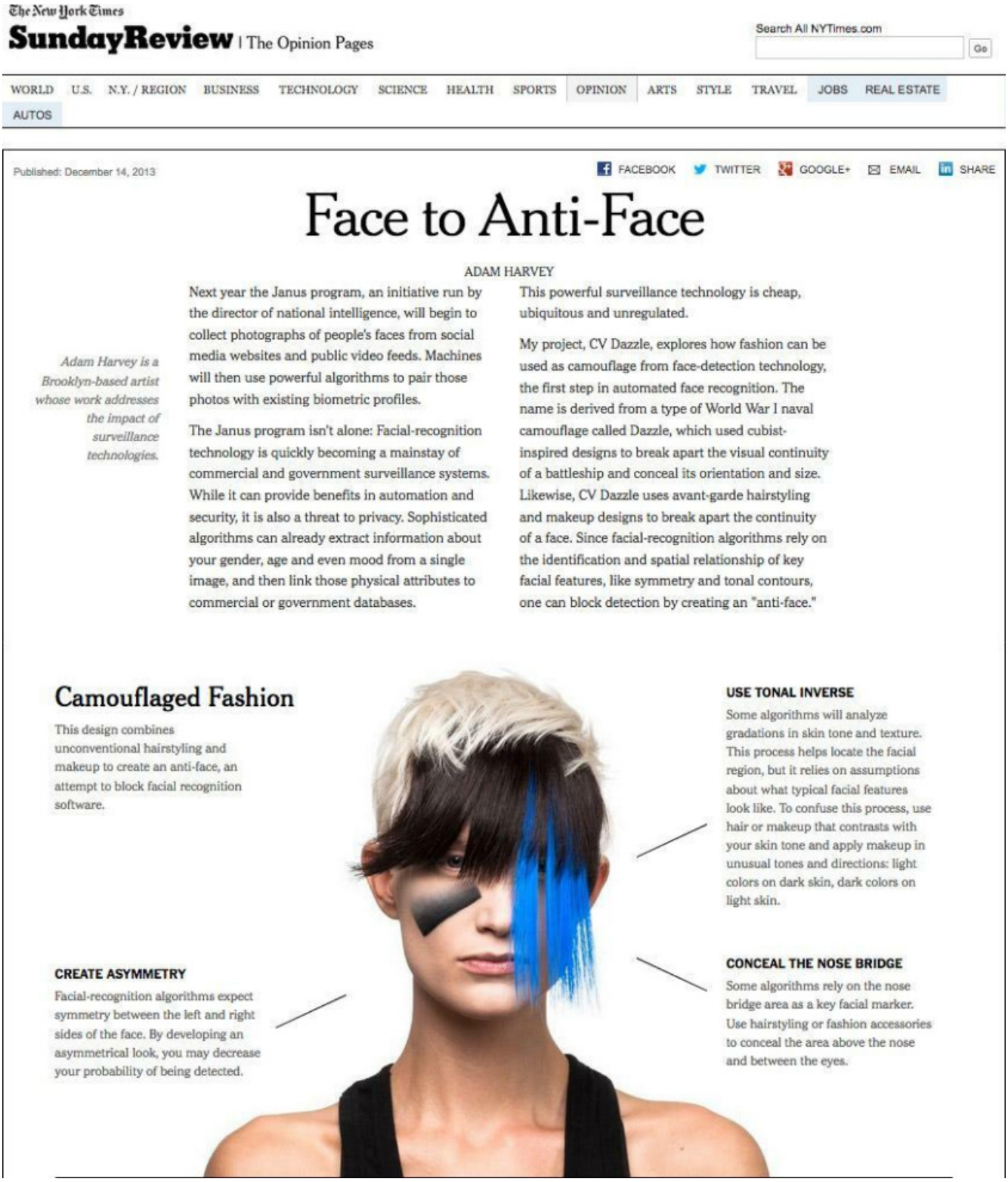
dell'esproprio” incessantemente ripetuto, basato sull'*incursione* dei vari dispositivi nelle nostre vite, sulla *assuefazione* al nuovo scenario, su un *adattamento* minimo in caso di eventuali resistenze e contestazioni, e sul *reindirizzamento* verso nuovi obiettivi. Senza nemmeno darci le perline...

I terreni da colonizzare e sfruttare si stanno moltiplicando.

Lo spazio pubblico è controllato dalle telecamere di sorveglianza (e presto dai droni) che, con i meccanismi di riconoscimento facciale, sono ormai in grado di ricostruire i movimenti di veicoli e persone (vedi Madhumita Murgia, *Who’s using your face? The ugly truth about facial recognition*, “Financial Times”, 18 settembre 2019, e Silvia Bottani, *L'occhio della macchina*). Anche le nuove automobili intelligenti sono una miniera di dati.

Nelle nostre case l'IoT, l'*internet of things*, sta connettendo alla rete elettrodomestici, abiti, giocattoli... Assistenti personali come Alexa, Cortana e Siri convivono già con il 25 per cento degli americani adulti e trasmettono un costante flusso di informazioni, elaborate senza alcun controllo da parte dell'utente.

Ma non basta. Il “primo testo” fornisce le materie prime per un secondo testo, un “testo ombra” ancora più invisibile e gigantesco, tanto complesso e dinamico che può essere gestito solo dagli algoritmi. Qui i contenuti hanno poca importanza: contano le relazioni che le macchine riescono a estrarre dalla “materia prima”, cioè gli utenti di internet. Come hanno scoperto nel 2011 tre ricercatori dell'Università del Maryland, “i semplici metadata (...) sono più utili e predittivi dei dati grezzi originali” (p. 287). I *dati di scarto* che intasavano i server di Google e degli altri giganti del web sono diventati la più preziosa delle merci.



The New York Times
SundayReview | The Opinion Pages

Search All NYTimes.com Go

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION ARTS STYLE TRAVEL JOBS REAL ESTATE AUTOS

Published: December 14, 2013

FACEBOOK TWITTER GOOGLE+ EMAIL SHARE

Face to Anti-Face

ADAM HARVEY

Adam Harvey is a Brooklyn-based artist whose work addresses the impact of surveillance technologies.

Next year the Janus program, an initiative run by the director of national intelligence, will begin to collect photographs of people's faces from social media websites and public video feeds. Machines will then use powerful algorithms to pair those photos with existing biometric profiles.

The Janus program isn't alone: Facial-recognition technology is quickly becoming a mainstay of commercial and government surveillance systems. While it can provide benefits in automation and security, it is also a threat to privacy. Sophisticated algorithms can already extract information about your gender, age and even mood from a single image, and then link those physical attributes to commercial or government databases.

This powerful surveillance technology is cheap, ubiquitous and unregulated.

My project, CV Dazzle, explores how fashion can be used as camouflage from face-detection technology, the first step in automated face recognition. The name is derived from a type of World War I naval camouflage called Dazzle, which used cubist-inspired designs to break apart the visual continuity of a battleship and conceal its orientation and size. Likewise, CV Dazzle uses avant-garde hairstyling and makeup designs to break apart the continuity of a face. Since facial-recognition algorithms rely on the identification and spatial relationship of key facial features, like symmetry and tonal contours, one can block detection by creating an "anti-face."

Camouflaged Fashion

This design combines unconventional hairstyling and makeup to create an anti-face, an attempt to block facial recognition software.

USE TONAL INVERSE

Some algorithms will analyze gradations in skin tone and texture. This process helps locate the facial region, but it relies on assumptions about what typical facial features look like. To confuse this process, use hair or makeup that contrasts with your skin tone and apply makeup in unusual tones and directions: light colors on dark skin, dark colors on light skin.

CREATE ASYMMETRY

Facial-recognition algorithms expect symmetry between the left and right sides of the face. By developing an asymmetrical look, you may decrease your probability of being detected.

CONCEAL THE NOSE BRIDGE

Some algorithms rely on the nose bridge area as a key facial marker. Use hairstyling or fashion accessories to conceal the area above the nose and between the eyes.

Per capire che cosa pensiamo, che cosa desideriamo, qual è il nostro stato emotivo, è più utile – nel caso di Instagram, per esempio – guardare quali filtri usiamo, quanti post facciamo (e quando), quanti cuoricini mettiamo (e a chi), e chi mette i like sui nostri post (e quanti e quando). Quel che si vede nelle immagini è relativamente irrilevante, con buona pace di chi proclamava che “in

rete il contenuto è re”. Per questo i social network e i motori di ricerca non sono interessati a eliminare le *fake news*: al centro dell'attenzione ci sono le azioni e le relazioni, e le *fake news* sono efficacissime nel generare “traffico”.

Il “secondo testo”, il nostro DNA digitale, viene estratto da quello ci è stato massicciamente sottratto senza che ce ne accorgessimo e senza chiederci permesso (o meglio, estorcendolo con quei contratti online che firmiamo senza leggere... e che è inutile leggere). Oggi tutti questi big data sono nelle mani dei “capitalisti della sorveglianza”, senza alcun controllo. Nella prima fase gli algoritmi hanno imparato a prevedere le nostre scelte, con margini di incertezza sempre minori. Ora si stanno attrezzando per orientare le nostre decisioni.

Le società di assicurazione vorrebbero da sempre ottenere un profilo preciso del cliente e del suo comportamento, per ridurre i margini di rischio ed eventualmente spingerlo entro determinati parametri comportamentali. Per farlo è necessario monitorare le azioni dell'automobilista, che però diffida di questa intrusione nella privacy e non si fida dell’azienda che vuole controllarlo. Se “il denaro non è abbastanza convincente, si consiglia agli assicuratori di presentare il monitoraggio del comportamento come 'divertente', 'interattivo', 'competitivo' e 'gratificante' (…) Questo approccio, noto come *gamification*, incoraggia i conducenti a partecipare a 'gare basate sulla performance' e a 'sfide fondate sugli incentivi'” (pp. 230-231). Meccanismi di condizionamento analoghi, che mirano a cambiare il comportamento degli utenti, si possono applicare alla sanità o all'istruzione.

Se il presupposto è l'ubiquità della sorveglianza, l'obiettivo, il vero potere, “è quello di *modificare* le azioni in tempo reale nel mondo reale. (…) Le analisi in tempo reale si traducono in azioni in tempo reale” (p. 309).



Anche in questo caso le strategie sono già affinate:

il *tuning*, che utilizza “indizi subliminali per dare forma impercettibilmente a un flusso di comportamenti” (ne sono esperti gli architetti delle case da gioco, per creare assuefazione negli scommettitori: ma anche internet e i social sono *addictive*);

lo *herding*, che lavora sul contesto che circonda la persona (perché l'invidia e i meccanismi imitativi, ovvero “l'influenza sociale”, fanno parte del nostro bagaglio comportamentale) e punta a un “contagio emotivo”;

il *condizionamento*, ben noto agli psicologi comportamentisti, che spinge gli animali (e dunque anche gli esseri umani) a selezionare i comportamenti di maggiore successo.

Il risultato è devastante: “Affermando di poter modificare le azioni umane in modo segreto e a scopo di lucro, il capitalismo della sorveglianza di fatto ci esilia dal nostro stesso comportamento, cambiando l'espressione del futuro 'io vorrò' a 'tu vorrai” (p. 325). Per Zuboff, stiamo perdendo la nostra libertà a favore del

Grande Altro che rende gli individui oggetti. Non siamo stati vittime di un colpo di Stato, ma di un *coup de gens*: consumatori e cittadini sono schiacciati da una gigantesca asimmetria dell'informazione, nelle mani di poche aziende e di un potere politico più o meno occulto ma sicuramente antidemocratico.

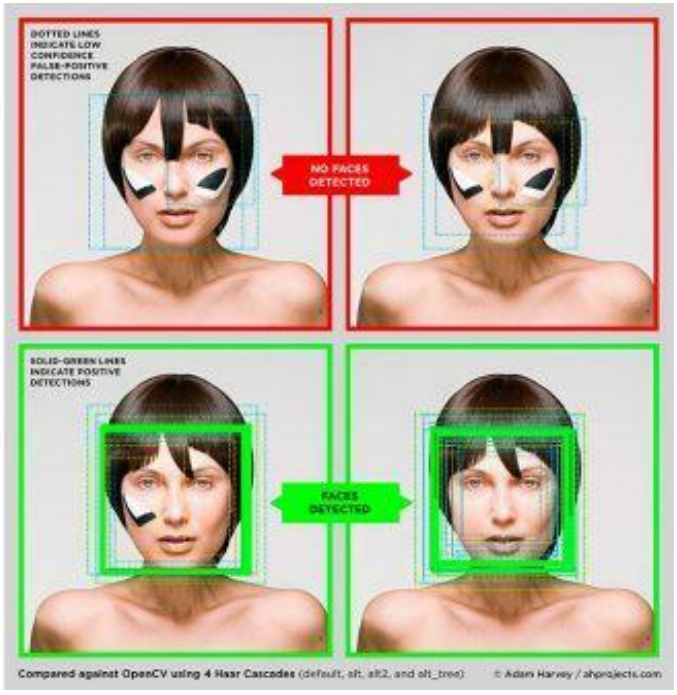
I due internet secondo Edward Snowden

Anche i servizi segreti americani hanno costruito un internet parallelo, in grado di raccogliere valanghe di informazioni sui cittadini americani (e non solo), a loro insaputa (e senza informare gli organi democratici). Quando si accorse dell'esistenza di questo *deep State* – il programma PRISM con la *upstream collection*, ovvero la “raccolta a monte” dei dati dei cittadini – Edward Snowden era un nerd che lavorava per la National Security Agency, ovvero i servizi segreti USA. Restò sbalordito, sconvolto, indignato, come racconta nel suo autobiografico *Errore di sistema* (Longanesi, Milano, 2019, 350 pagine, 18,60 €).

“Immaginate di sedervi al computer per visitare un sito web. Aprite un browser, digitate un indirizzo e premete INVIO. La vostra azione equivale a una richiesta, e tale richiesta parte alla ricerca del server di destinazione. A un certo punto del suo viaggio verso il server, però, la vostra richiesta dovrà passare attraverso TURBULENCE, una delle armi più potenti dell'NSA”. Ogni interazione in rete viene filtrata. La NSA, se ritiene che ci sia qualcosa di sospetto, installa sul vostro computer un malware da usare contro di voi: “In meno di 686 millisecondi ottenete tutti i contenuti che volevate, assieme a tutta la sorveglianza che non volevate” (pp. 225-226), senza passare dal giudice. La Intelligence Community degli Stati Uniti aveva “hackerato la Costituzione”, alla quale Snowden voleva restare fedele. Si trovò lacerato da un dilemma tragico: tacere, per garantirsi una carriera e una vita tranquilla ma portandosi dentro quest'ombra, oppure...

Scegliere di non lavorare più “per il governo” ma “per le persone” non fu una una decisione facile, per il rampollo di una dinastia di fedeli servitori dello Stato. Come Snowden sia riuscito a trafugare e rendere pubblici ai primi di agosto del 2013 migliaia di documenti segreti senza farsi arrestare e senza impazzire, diventando uno dei più celebri *whistleblowers* della storia, è meglio scoprirlo leggendo la sua emozionante epopea solitaria (e lo struggente diario della sua compagna Lindsay nei giorni cruciali).





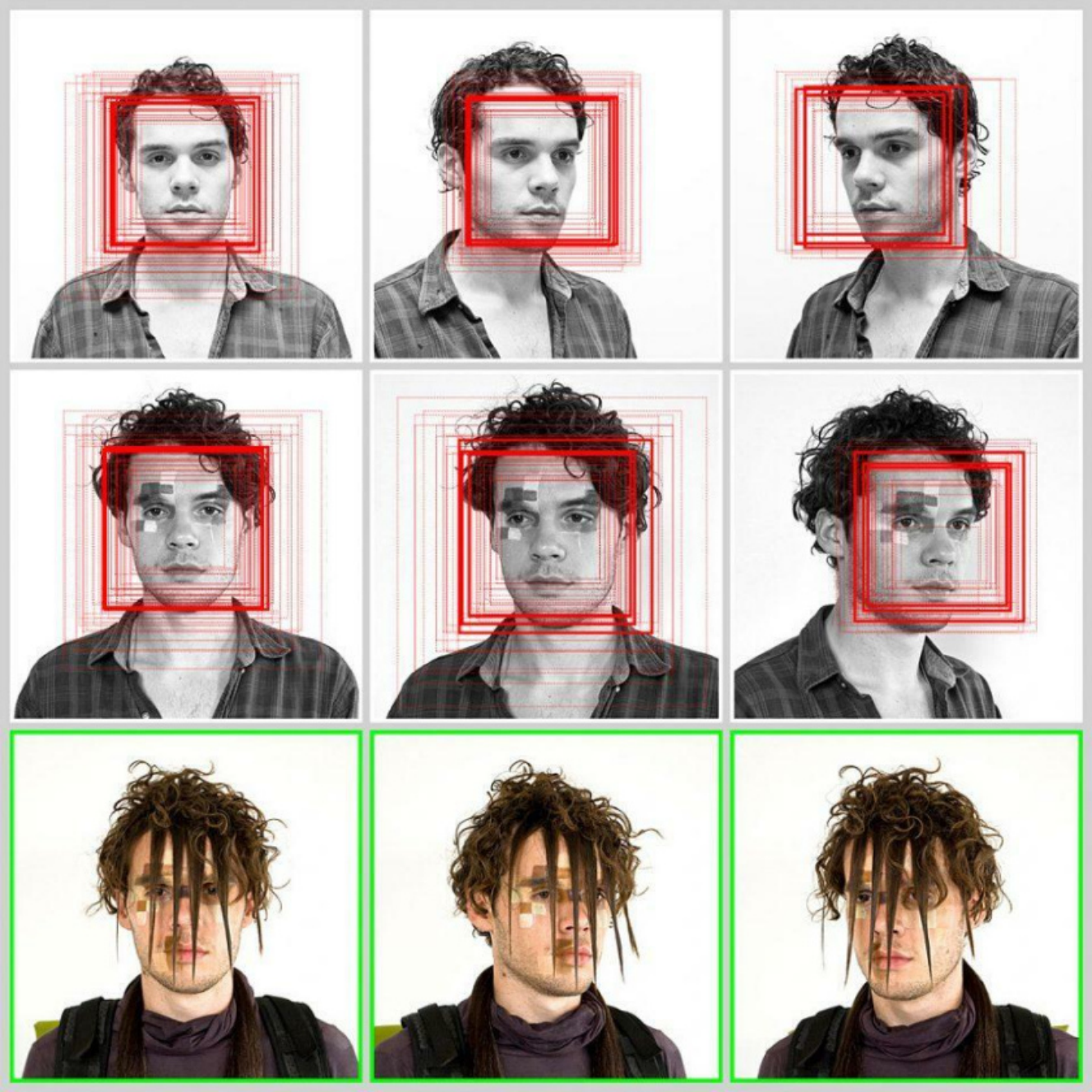
Onniscienza, controllo, certezza

Nell'indifferenza pressoché generale si è generato un sistema feroce, mostruoso, occulto. Come sia stato possibile, ce lo spiegano Snowden e Zuboff. Le cause sono molteplici. Il rapporto costante tra i servizi segreti e le aziende, fin dalla nascita di internet, che in origine era un'infrastruttura militare (ARPANET). Un'ideologia neo-liberista e individualista, che ha ridotto le tutele di leggi e regolamenti, dando spazio all'iniziativa privata senza alcun contrappeso della società civile e dei lavoratori. La necessità di alcune grandi aziende di massimizzare i profitti e ripagare gli azionisti dopo la bolla del 2000. L'ossessione per la sicurezza dopo l'11 settembre 2001.

Contribuisce anche, spiega Zuboff, la visione utopica di alcuni signori della rete. Larry Brin e Sergei Page di Google, come Mark Zuckerberg di Facebook, sono convinti che i loro algoritmi renderanno il mondo migliore: offrono “soluzioni ai singoli individui sotto forma di connessioni sociali, accesso all'informazione, risparmio di tempo, e spesso con l'illusione di un sostegno”, e offrono “soluzioni alle istituzioni sotto forma di onniscienza, controllo e certezza”. A differenza degli utopisti del passato, che erano filosofi squattrinati, questi profeti 2.0 dispongono di enormi risorse finanziarie per imporci le loro visioni.

Il loro intento, avverte Zuboff, “non è quello di porre rimedio all'instabilità – la corrosione della fiducia sociale, la rottura dei legami di reciprocità, le

conseguenze pericolose dell'ineguaglianza, i regimi basati sull'esclusione – ma lo sfruttamento delle vulnerabilità prodotte da tali condizioni" (p. 400). Il "*cloud* che lavora in armonia con i sensori intelligenti" dell'IoT sarà in grado di anticipare e prevenire le deviazioni dalla norma "prima che possano accadere", ha annunciato nel 2017 Satya Nadella, amministratore delegato di Microsoft. Come ha avvertito Evgeny Morozov, diventa possibile prevenire (o reprimere) il dissenso ancora prima che si manifesti, e addirittura prima che gli interessati siano consapevoli di essere fuori dalla norma (*Internet non salverà il mondo*, traduzione di Gianni Pannofino, Mondadori, Milano, 2014, 454 pagine, 19 €).



Negli Stati Uniti, a guidare la danza sono le grandi aziende, alleate con l'apparato statale. La Comunità Europea tenta di frenare questa ingerenza con i suoi regolamenti sui monopoli, sul copyright e sulla privacy (GDPR). In Cina, è lo Stato (ovvero il Partito Comunista) a governare il meccanismo.

Sesame Credit, il sistema di “calcolo dei crediti personali” di Ant Financial (Ali Baba), valuta il regolare pagamento di crediti e bollette, ma anche “gli acquisti (videogame anziché libri per bambini), livello d'istruzione, quantità e 'qualità' degli amici”. Usando questi dati, l'algoritmo decide chi può acquistare un biglietto d'aereo o per un treno ad alta velocità e chi deve invece viaggiare su un Regionale, chi può iscriversi al Partito e chi non può comprare una casa (Zuboff, pp. 407-408). Gli utenti di Sesame Credit hanno subito iniziato a ripagare i loro debiti alla banca.

Di recente i big data sono stati integrati con la geolocalizzazione (la strada l'ha tracciata un esperimento di massa come *Pokemon Go!*) e il riconoscimento facciale: il risultato è il *social credit* personale, un incubo che sembra una puntata di *Black Mirror*, come racconta il documentario *Social Credit: China's Digital Dystopia In The Making*. Il social credit si rivela utilissimo per zittire ogni dissenso. Anche per questo la lotta degli studenti di Hong Kong è doppiamente eroica.

Una sovversione che viene dall'alto

Zuboff si chiede come possiamo resistere alla “macchina alveare nella quale rinunciamo alla libertà in cambio di una conoscenza perfetta che qualcun altro amministra per il proprio profitto” (p. 459). È un problema politico: “*Chi sa? Chi decide? Chi decide chi decide?*” È anche una questione di benessere psichico. “La scomparsa della società tradizionale e l'evoluzione della complessità sociale hanno accelerato il processo di individualizzazione”. Dunque “la connessione digitale è divenuta un mezzo di partecipazione sociale necessario”, ma dominato e strumentalizzato dal capitalismo della sorveglianza. Costruiamo la nostra identità sulla base del confronto sociale: ma più il bisogno degli altri viene soddisfatto (con il mix di esibizionismo e narcisismo tipico degli *influencer*), meno diventiamo capaci di costruire il nostro sé. Viviamo la *fear of missing out* (la “paura di perdersi qualcosa”) e cadiamo preda dell'invidia.

Secondo una ricerca di Holly B. Shakya e Nicholas A. Christakis pubblicata nel 2017 sull'“American Journal of Epidemiology”, mettere un like ai contenuti degli altri e cliccare sui loro link “sono azioni sempre collegate a problemi di benessere, mentre il numero degli status è collegato a una minor salute mentale [...] Una deviazione standard di 1 nel numero di like, [...] link cliccati [...] o aggiornamenti degli status viene associata a una diminuzione che va dal 5 all'8 per cento nelle condizioni di salute mentale riportate dal soggetto” (p. 480). Inutile precisare che questi dati forniscono al “testo ombra” valanghe di informazioni sullo stato personale dell'utente. La nostra interiorità, le nostre emozioni, sono diventate trasparenti, conoscibili e dunque manipolabili.

Tutto questo sta moltiplicando i profitti dei protagonisti del capitalismo della sorveglianza: i cinque big della rete (Amazon, Apple, Facebook, Google e Microsoft), ma anche i provider come Verizon, AT&T e Comcast, e poi le catene della distribuzione come Walmart, le grandi banche e assicurazioni, le piattaforme come AirBnB o eBay...



“La pressione del gruppo e la certezza computazionale sostituiscono politica e democrazia, annullando la percezione della realtà e la funzione sociale delle vite

degli individui” (p. 31).

Come uscire da questo ossessivo e vorace *panopticon*? Come evitare di sprofondare in un nuovo totalitarismo? Come salvare una zona di intimità di fronte all'invadenza dei dispositivi? Come difendersi dalla violenza “oggettivante” degli algoritmi? Come ridurre gli errori di sistema, visto che – per esempio – quasi tutti i programmatori sono maschi bianchi con un alto livello di reddito e di istruzione? C'è un paradosso. Gli algoritmi usano il passato per predire il futuro e dunque perpetuano e amplificano i pregiudizi razzisti e maschilisti: questa gigantesca macchina per prevedere e realizzare il più radioso avvenire è per sua natura reazionaria, come ha dimostrato Cathy O’Neil (*Armi di distruzione matematica. Come i big data aumentano la disuguaglianza e minacciano la democrazia*, traduzione di Daria Cavallini, Bompiani, Milano, 2017, 368 pagine, 18 €).

Di fronte all'opacità e alla segretezza che accompagna questa rivoluzione, che ci vuole ignari come le cavie degli esperimenti degli etologi, il primo passo è la consapevolezza e l'acquisizione di uno spirito critico. Il secondo gesto è autodifensivo e ironico: possiamo “trasformare l'atto di nascondersi in una scienza e un'arte” (Zuboff, p. 504). Ma naturalmente per difenderci dalla “sovversione che viene dall'alto” servono azioni politiche e strumenti legislativi, e soprattutto una ampia mobilitazione democratica. È questa la sfida che ci lancia il capitalismo della sorveglianza. Non sarà una battaglia facile.

Ecco, sei arrivato fino in fondo a questo lungo post e dunque sei un'anomalia.

Per capire chi sei, mi basta guardarti in faccia e guardare le tue scarpe.

Lo stesso vale per te.

Adesso possiamo cominciare a parlare.

PICCOLA SITOGRAFIA ARTIVISTICA

Adam Harvey, AH Projects

SA Rogers, *How to Be Invisible: 15 Anti-Surveillance Gadgets & Wearables*, su weburbanist.com, a questa pagina

Benjamin Grosser, *Twitter Demetricator* , a questa pagina.

Se continuiamo a tenere vivo questo spazio è grazie a te. Anche un solo euro per noi significa molto.
Torna presto a leggerci e SOSTIENI DOPPIOZERO

