

DOPPIOZERO

Cosa avrei chiesto a Mark Zuckerberg

Oliviero Ponte Di Pino

13 Aprile 2018

“Per risolvere i problemi di Facebook ci vorranno anni”, [ha dichiarato Mark Zuckerberg](#) quando ha iniziato a rendersi conto della gravità del bubbone Cambridge Analytica, lo scandalo che gli ha fatto mettere la giacca e la cravatta prima di sedersi sul banco degli imputati davanti al Congresso USA. Per capire i problemi di Facebook bisogna fare un passo indietro, non basta risalire al 2013, quando è stata fondata Cambridge Analytics.

Se servono anni per risolvere questi problemi, quando sono iniziati?

Forse bisogna tornare ai primi anni Duemila, nell'Era dell'Innocenza della Rete, quando ancora non esistevano i social network e la rete era una Zona Temporaneamente Liberata: avevamo tutti diritto di parola e “uno valeva uno” (almeno in teoria). Vivevamo in un'anarchica Era dell'Ingenuità, con i forum senza moderatore, l'anonimato, gli pseudonimi fantasiosi e provocatori. La sgangherata utopia della rete aveva qualche difetto: il fenomeno “zero comments”, dove tutti parlano e nessuno ascolta; la “fine dell'esperto”, ovvero l'incompetenza al potere; infine l'imperversare di troll, haters e molestatori vari.

Chi gestiva un forum “aperto”, o lo ospitava, correva due rischi. Il primo era la sicurezza: gli hacker bombardavano di post con pubblicità di portali dedicato ad azzardo, porno, dating (o peggio), s'impadronivano dei siti oppure ci inoculavano un simpatico virus. Il secondo rischio era la responsabilità civile e penale: ogni sito ha un responsabile (una persona fisica) registrato all'autorità, che risponde civilmente e penalmente di qualunque amenità venga scritta sul sito e nei forum, da lui o da chiunque altro, così come capita alle testate giornalistiche (questo anche se il sito non è registrato come testata giornalistica in Tribunale, in Italia). Così – scusate l'accenno autobiografico – grazie al vivace, troppo vivace forum ospitato su ateatro, ho ricevuto qualche minaccia di querela e il sito è finito sulla lista nera di Google perché “non sicuro” (senza alcun preavviso): chi aveva la sventura di atterrare sul sito, veniva accolto da una pagina che avvertiva di terribili pericoli.

Ma il povero webmaster, a partire dal 2008, aveva una via di salvezza facile e gratuita: chiudere il forum all'istante e aprire una pagina su un social network, per esempio Facebook. La piattaforma si accollava i problemi della sicurezza; per quanto riguarda il rischio di querela, la risposta era semplice: “Non siamo una testata giornalistica o un editore, non siamo una media company, siamo solo una piattaforma tecnologica che offre un servizio gratuito”. Incredibilmente i governi e i tribunali non hanno avuto niente da obiettare. Nemmeno i webmaster: Facebook consentiva di ampliare molto in fretta la propria audience e di monitorarla. Tutto questo è successo nell'arco di pochi mesi, tra il 2010 e il 2012: i forum sono morti e i social network hanno iniziato a prosperare.

Ma davvero i social network sono solo un servizio? Non hanno alcuna responsabilità per i contenuti che pubblicano e diffondono, rilanciando quelli degli utenti? Nemmeno quando questi canali hanno un ruolo centrale nella sfera pubblica e nel dibattito politico?

Sulla base del contratto che sottoscrive (in genere senza leggerlo, ma non hanno alternativa), l'utente accorda all'azienda di Zuckerberg una "licenza non esclusiva, trasferibile, che può essere concessa come sottolicensing, libera da royalty e valida in tutto il mondo, che consente l'utilizzo dei contenuti (...) pubblicati su Facebook o in connessione con Facebook". Insomma, Facebook è libera di utilizzare tutti gli altri contenuti conferiti dall'utente ovunque lo ritenga opportuno e senza versare un centesimo in termini di royalty. I contenuti, foto comprese, restano quindi di proprietà dell'utente ma Facebook non deve versare alcun corrispettivo economico se le vuole riutilizzare. E infatti le riutilizza, pubblicandole sui wall delle varie pagine. Ma senza alcuna responsabilità. Perciò potrebbe pubblicare senza rischi tutto quello che pubblicano gli utenti, senza alcuna forma di filtro o di censura, come i vecchi forum. Ma non lo fa, ovviamente.

Nel 2017 la app inventata da Mark Zuckerberg per rimorchiare le studentesse più carine della sua università ha superato i due miliardi di utenti. Una percentuale considerevole degli abitanti della Terra ha oggi l'opportunità di dialogare sempre e con tutti, in uno straordinario "qui e ora" planetario. Il profeta nerd con le connessioni giuste nella Silicon Valley e a Washington (e forse nella CIA) ha vinto la lotteria del capitalismo digitale e globalizzato. A trent'anni è uno degli uomini più ricchi e potenti del pianeta, pronto a candidarsi alla Casa Bianca per evitare un secondo mandato al Mostro Trump. Geniale e ingenuo, visionario e travolgente come Alessandro Magno e Napoleone, ha colonizzato il mondo 2.0. Fin dagli inizi, era facile prevedere qualche contraccolpo. E per vari ordini di motivi, che non riguardano solo Facebook ma tutti i social network e la logica stessa della rete.

Quale contributo può dare alla democrazia questo potentissimo strumento? Come pensate di favorire lo sviluppo di una democrazia più matura e partecipata? Ha mai seguito un corso di educazione civica, di scienze politiche, di giornalismo?

Per cominciare va ricordato che i grandi player della rete (a cominciare da Microsoft, Apple, Google, Twitter o Amazon) non sono organizzazioni filantropiche che hanno per obiettivo il bene dell'umanità e la nostra emancipazione culturale. Non vogliono – per nostra fortuna – fare di noi esseri umani "migliori", qualunque cosa questo voglia dire. Sono aziende (spesso società per azioni) che hanno per obiettivo il profitto.

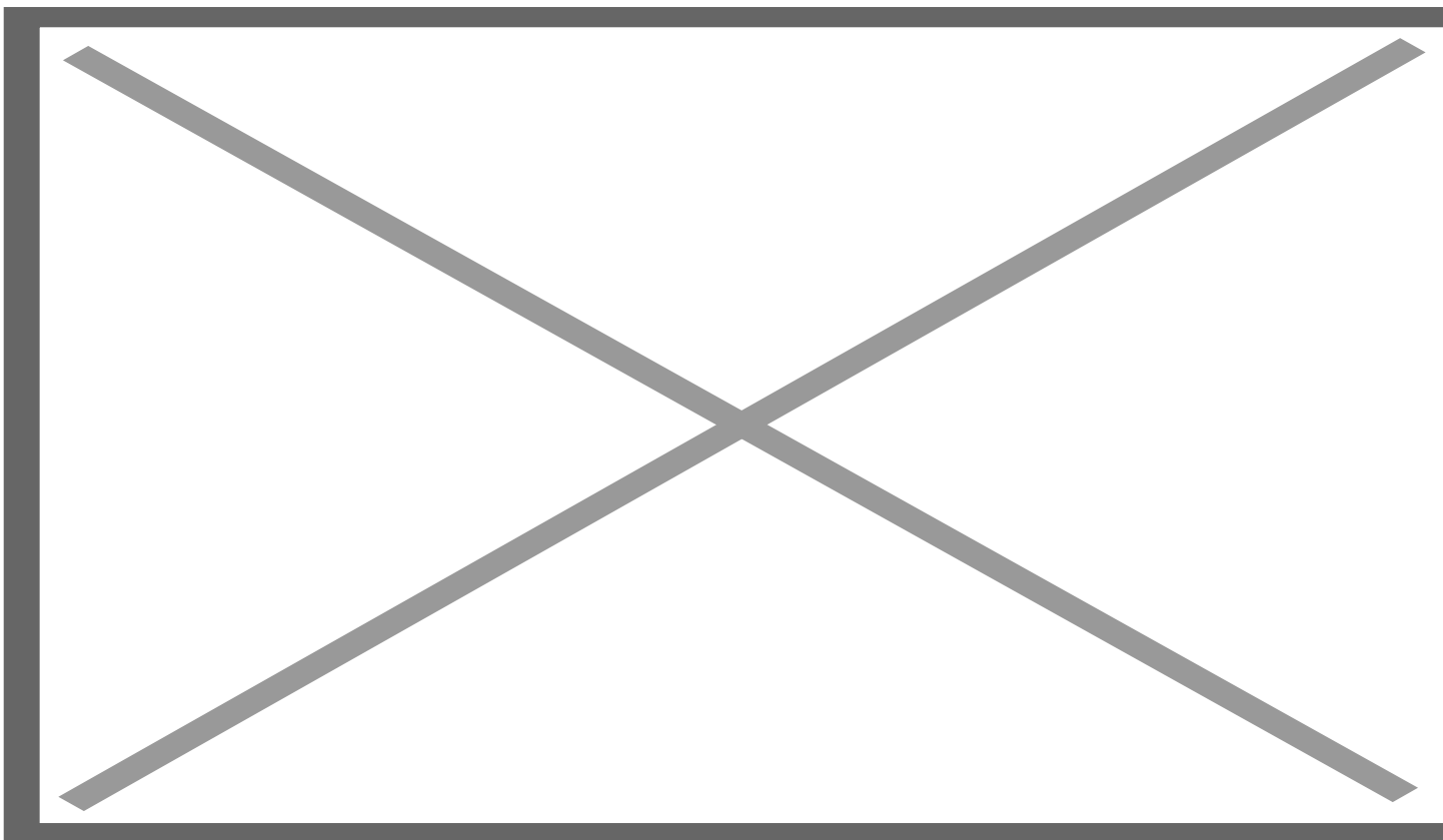
Quanto ha incassato Facebook da Cambridge Analytica? Avete offerto consulenze? Con quali obiettivi e risultati?

Puntare al profitto è legittimo ma comporta una serie di conseguenze a vari livelli, soprattutto perché queste imprese private hanno un fortissimo impatto sia sulla sfera pubblica sia sulla privacy dei cittadini. Questo impatto diventa imponente nell'era dei big data, quando l'enorme mole di informazioni raccolte viene filtrata da sofisticate tecniche statistiche.

Che uso viene fatto dei dati personali degli utenti? Con quali obiettivi? A chi vengono ceduti? Con quali vincoli? Quando condividete questi dati con terze parti, informate gli interessati?

Internet tende ad abolire la privacy, con il consenso più o meno consapevole degli utenti. La rete è un *panopticon* che tutto vede, registra e ricorda. Una parte delle informazioni le forniamo direttamente e volontariamente come utenti alle diverse piattaforme. Altre informazioni vengono raccolte a prescindere della nostra volontà e dal nostro consenso, attraverso smartphone, telecamere di sorveglianza (e riconoscimento facciale), acquisti, ricerche online, mail...

Stephen Brobst, Cto di Teradata, una società che si occupa di big data ed ex membro dell’Innovation and Technology Advisory Committee di Barack Obama, nel 2015 ha spiegato che gli europei si preoccupavano troppo della privacy: “Dopo le rivelazioni di Edward Snowden sulla sorveglianza di massa dell’Nsa le preoccupazioni degli europei sono aumentate e questo è sicuramente giustificato. Ma Nsa a parte i governi europei tendono a esercitare un controllo un po’ rigido sul mercato. Negli Stati Uniti pensiamo che il mercato si auto-regoli e lo Stato non debba intervenire: sono i consumatori a decidere se un prodotto è valido oppure no: è il mercato che decreta il fallimento o il successo. Lo Stato interviene solo se le aziende non si comportano correttamente, ma sono le aziende a fissare termini e condizioni per il loro business. Diranno per esempio: raccogliamo questi dati che ci lasciate con la vostra navigazione e li usiamo in questo modo e per questo motivo. Non rispettano tale impegno? Lo Stato interviene sanzionando le aziende scorrette. Ma non è lo Stato a dettare le condizioni e i modi di fare business. Gli Stati europei tendono a voler dettare queste condizioni, a decidere loro al posto dei loro consumatori. Lei sa come definiscono gli americani gli Stati europei? [Nanny States](#). Non dico che sia vero, ma è questa la reputazione diffusa: gli Stati europei vogliono fare da balia ai loro cittadini”.



Kevin Kelly, fondatore di “Wired”, già [nel 2014 scriveva](#) che “da qui a 50 anni il monitoraggio e il controllo saranno la norma” perché, per come è stata concepita, Internet è sostanzialmente una macchina per tenere traccia delle cose che fa chi la utilizza: “Saremo sempre più monitorati da una grande rete, dalle multinazionali e dai governi. Tutto ciò che può essere misurato è già tracciato, e tutto ciò che prima non era misurabile inizia a essere quantificato, digitalizzato” e di conseguenza diventa tracciabile. Poiché siamo già sotto controllo e lo saremo sempre di più, a causa di un processo inevitabile, la soluzione più praticabile e meno spaventosa è fare in modo che anche il controllato possa tenere d’occhio il controllore”.

Per i signori e per i teorici della rete, nel villaggio globale 2.0 la privacy non ha più senso. È un lusso. Infatti i vertici di Facebook erano ben consapevoli dei rischi del panopticon che essi stessi avevano creato e utilizzavano [uno strumento segreto](#) che consentiva di eliminare i messaggi inviati dai top manager, Mark Zuckerberg su tutti, senza notificarlo ai destinatari né lasciare una qualche traccia dei messaggi rimossi.

La fine della privacy – a lungo termine – implica anche la fine della politica che era tradizionalmente basata sulla separazione tra privato e pubblico, tra la casa e la piazza, tra l'economia, ovvero il governo della casa (*oikos*), e la politica, ovvero ciò che attiene alla *polis*, la città.

La privacy degli utenti, compreso Mark Zuckerberg, è stata difesa con la necessaria efficacia? Che cosa possiamo fare per migliorare la situazione? Che cosa possono fare gli utenti?

Una seconda conseguenza: il nostro capitale sociale, ovvero le nostre amicizie, relazioni, conversazioni, diventano merce. Hanno un valore, possono essere comprate e vendute. I signori della rete si sono appropriati (hanno “privatizzato”) di un bene che era pubblico e diffuso: gli “Amici” e gli interessi personali, che sono alla base delle interazioni dei social network. Ma anche i nostri movimenti, le curiosità, le abitudini di acquisto eccetera. Era un sapere che ciascuno di noi possedeva per quanto lo riguardava, di cui amici e parenti potevano sapere alcuni frammenti, e che per il resto era nella disponibilità di diversi soggetti (sistema sanitario o pensionistico, banca, fisco, sistema scolastico, assicuratore...) che non avevano la possibilità di scambiare e sommare le informazioni.

Ma il social network non raccoglie le informazioni del singolo: somma le informazioni di tutti gli utenti, e a partire da questa base statistica è in grado di estrapolare dati e previsioni di straordinaria efficacia: già nel 2012 due ricercatori, Michael Kosinski e David Stillwell, hanno dimostrato che bastano 68 like per stabilire il colore della pelle di un utente, il suo orientamento sessuale, l’affiliazione politica, il quoziente intellettivo, l’appartenenza religiosa, l’uso di alcol, sigarette e droghe, e molto altro. Nella loro ricerca Kosinski e Sitwell avevano utilizzato [una app, MyPersonality](#), simile al test di personalità di thisisyourdigitallife utilizzato da Cambridge Analytica.

Avete mai informato gli utenti che estrapolando i dati da loro inseriti è possibile ottenere un profilo completo della loro personalità e della loro situazione? Li avete mai informati dell'uso che fate di queste informazioni?

Sulla base di queste informazioni, l'attenta drammaturgia (ovvero gli algoritmi) del social non ci fa vedere tutto quello che accade in rete, anche perché sarebbe un flusso di dati insostenibile. L'algoritmo seleziona sia gli autori dei post che vediamo sia i loro contenuti. L'obiettivo è quello di creare un'atmosfera favorevole all'acquisto, evitando spiacevoli tensioni e contrasti. Il meccanismo favorisce l'omofilia, ovvero la tendenza a interagire con persone che hanno i nostri stessi gusti, tendenze, interessi, portando alla creazione di bolle

autoreferenziali, che rappresentano il target perfetto per il marketing. Il meccanismo è accentuato dal “pregiudizio di conferma”: tendiamo a dare maggior credito alle informazioni che confermano i nostri pregiudizi e a trascurare quelle che potrebbero confutarli o metterli in crisi (è anche per questo che a un politico conviene dire due verità inconciliabili ai gruppi di potenziali elettori).

Naturalmente l'algoritmo non è infallibile e molti utenti sono oltremodo curiosi e ficcano il naso su bacheche che non dovrebbero frequentare. Così possono essere identificati e additati al pubblico ludibrio alcuni contenuti “controversi”, o peggio ancora decisamente oltraggiosi e inaccettabili (compresi stalking, minacce, bullismi...).

Di fronte alle inevitabili polemiche, i responsabili dei social network rispondevano che non operavano censure o verifiche: “Non siamo testate giornalistiche, e la mole di dati pubblicata ogni minuto rende impossibile ogni controllo sistematico e puntuale”. Naturalmente non era vero: Facebook e gli altri social sono sempre stati attentissimi a rimuovere all'istante – per esempio – contenuti ritenuti pornografici, con effetti spesso esilaranti. Accade anche oggi. Solo nelle ultime settimane sono state censurate la [Libertà di Delacroix](#), [la danza a seni nudi in un museo di Trieste](#), la [Venere di Willendorf](#), la [copertina del Bafometto](#) pubblicato da Adelphi. Di recente [un post su Auschwitz](#) è stato eliminato “perché contiene scene di nudo”. In Francia [L'origine del mondo di Courbet](#), censurata da Facebook, è stata al centro di un'interessante disputa giudiziaria.

Non le sembra ridicolo accanirsi contro questi capolavori? Perché lo fate? Ha mai seguito un corso di storia dell'arte?

Per capire la ragione di questo accanimento, bisogna ricordare che il vero motivo delle censure non è tanto la difesa del “comune senso del pudore”, ma l'irritazione dei potenziali inserzionisti, che non vogliono che i loro spot compaiano accanto a immagini “scandalose”. Di recente [il colosso Unilever](#) ha minacciato di togliere la pubblicità a Youtube e Facebook a causa dei contenuti razzisti, mentre loro i detersivi devono venderli al tutti, a prescindere da religione e colore della pelle.

Su quali basi, con quali metodi e procedure eliminate alcuni dei contenuti pubblicati?

I social censurano i contenuti seguendo diverse procedure.

La prima sono algoritmi che dovrebbero individuare quelli ritenuti “inappropriati”. Il problema è che gli algoritmi sono opera degli esseri umani e gli esseri umani sbagliano. Quando l'algoritmo sbagliato viene applicato sistematicamente, l'errore diventa sistematico. In Italia su Facebook la parola “negri” è considerata politicamente scorretta, e dunque scompaiono anche i signori che hanno il [cognome “Negri”](#). Siccome gli idioti razzisti taggano le fotografie delle persone di colore con [“gorilla”](#) o [“scimpanzé”](#), il motore di ricerca di Google Foto ha deciso di rendere nulli i risultati della ricerca con queste parole chiave. Il lodatissimo algoritmo di ricerca di Google porta a [risultati spesso imbarazzanti](#): le femministe sono “pazze”, il Ku Klux Klan è una “organizzazione cristiana”, i nazisti sono “le nuove persone”.

Ma questi sono errori ridicoli. C'è una problematicità più profonda. Gli algoritmi si presentano come procedure oggettive impersonali e tuttavia rispondono sempre a un punto di vista, ovvero a una precisa ideologia, di cui spesso gli autori sono portatori inconsapevoli. I programmatori sono in grande maggioranza giovani maschi caucasici, la distorsione dovuta al loro vissuto è pressoché inevitabile e sistematica.

Una seconda procedura censoria parte dalle segnalazioni degli altri utenti: ma è fin troppo facile che una campagna ben orchestrata, che mobiliti qualche decina di fanatici o mercenari in località diverse, porti alla cancellazione di un profilo sgradito.

Allora si tratta di verificare: l'algoritmo cancella e l'utente si lamenta, arriva la segnalazione e non è detto che sia fondata. Così, per rispondere a censori e censurati, e per cercare di tenere la comunicazione sotto controllo, nel corso degli anni [Facebook ha assoldato un esercito di moderatori](#): si parla di centinaia di migliaia di persone sparse nel mondo, che hanno il compito di verificare le segnalazioni degli utenti, in particolare per evitare hate speech, terrorismo, minacce specifiche di violenza e bullismo.

Quali sono i protocolli usati dai vostri moderatori? Chi ha deciso i protocolli? Come vengono scelti e formati i moderatori? Quali margini di discrezionalità ha il singolo moderatore? E quanti secondi ha per prendere una decisione che riguarda spesso complessi dilemmi morali? Queste procedure possono essere verificate pubblicamente? È giusto che sia un'azienda privata a decidere i criteri che delimitano la discussione pubblica, secondo criteri non trasparenti?

Il discorso diventa ancora più delicato quando si affrontano tematiche politiche, e quando si evoca il fantasma delle fake news. Il termine è diventato di moda quando il sito Buzz Feed ha scoperto che durante [la campagna che ha portato Donald Trump alla Casa Bianca](#) le fake news erano state più viste delle notizie “vere” dei media “ufficiali”.

Si è scoperto e si sta scoprendo che buona parte dell'informazione che circola sui social (e dunque in rete) è opera di fake o di bot. In teoria, l'uso dei fake è vietato: gli utenti di Facebook devono essere persone fisiche ben identificabili. In realtà, come sa bene chiunque gironzoli in rete, i fake sono una moltitudine e vengono [smascherati assai di rado](#). O meglio, si annuncia con squilli di tromba la scoperta e la strage di centinaia di troll solo quando sono russi. I bot sono un tipo particolare di fake: non hanno nemmeno bisogno di essere umani e sono molto più veloci, efficaci e affidabili: una recente indagine ha dimostrato che [due terzi dei link su Twitter sono opera di algoritmi](#) che li sparano in automatico, milioni al minuto.

Cosa fate per smascherare i fake? Cosa fare per limitare l'inquinamento mediatico dei bot?

La scoperta del potere della fake news ha scatenato un'ondata di panico morale e innescato la ricerca di antidoti a questa terrificante epidemia di disinformazione. Sono state ipotizzate (e vengono sperimentate) [diverse strade](#): chiedere agli utenti di segnalare le notizie e le fonti attendibili (o quelle considerate “false”); chiedere ai media tradizionali (agenzie di stampa, giornali) di segnalare le notizie e i siti attendibili (o quelli che non lo sono), magari con un bollino rosso o verde; affiancare alle notizie false il link all'informazione attendibile, quando si è scoperto il pulsante rosso era inefficace o controproducente; inventarsi un algoritmo in grado di decidere se una notizia è falsa per cancellarla (oppure inventare un algoritmo che calcoli la “percentuale di affidabilità” di una notizia). Sono stati lanciati numerosi programmi in queste direzioni, sia dai colossi del web sotto accusa sia dalle autorità pubbliche. Anche la [Commissione Europea](#) ha cercato di correre ai ripari creando un High Level Group di super-esperti.

Questa deriva non dichiarata verso la censura si affianca alla tendenza dei regimi autoritari a controllare l'informazione, compresa quella sul web: accade in Iran, Cina o Turchia... Per capire come la legislazione contro le fake news sia un pretesto per zittire l'opposizione, basta guardare quel che sta accadendo in [Malesia](#) o in [Cambogia](#).

Ritiene che la qualità dell'informazione politica debba essere controllata e garantita da un'azienda privata come la sua? Dai media tradizionali? Dal governo? Dai tribunali? Ha in mente qualche meccanismo efficace?

La fake news più devastante degli ultimi decenni non è stata diffusa sui social networks, non è il frutto di un gruppo di hacker. L'hanno avallata e diffusa il presidente degli Stati Uniti d'America e il suo comandante in capo, il generale Colin Powell. Oggi sappiamo che Saddam Hussein non aveva né un arsenale nucleare né armi chimiche.

Se la Casa Bianca diffondesse una fake news, lei riuscirebbe a smascherarla? Con quali metodi? Come avvertirebbe i suoi utenti?

Facebook vale in borsa circa 400 miliardi di dollari perché il capitale sociale di ciascuno di noi ha un valore. Ma come può portare a un guadagno?

La prima strada, la più innocente, consiste nel vendere inserzioni indirizzando i messaggi degli inserzionisti verso il pubblico potenzialmente più ricettivo, con minori costi e maggiore efficacia. Per molti utenti, queste inserzioni – corredate di offerte speciali – appaiono come un servizio utile e apprezzato. Se digito “Maldives” nella mia mail o in un motore di ricerca, verrò bombardato da offerte di vacanze premio superscontate nell'arcipelago (anche se stavo cercando informazioni geopolitiche).

A volte gli effetti possono essere sorprendenti. Il genitore di una tredicenne protestava vivacemente contro il social che manda alla sua “bambina” pubblicità di pannolini e latte per neonati, solo per scoprire che la ragazza è incinta e non glielo aveva detto. Forse l'aneddoto è una fake news, ma è credibile.

In questo caso, i dati relativi agli utenti restano unicamente nella disponibilità di chi gestisce il social. In altri casi i dati finiscono nelle mani di terzi: basta pubblicare una app che chiede l'accesso ai dati personali, ai post sulla tua pagina e ai nomi degli amici (o addirittura ai loro dati). Per esempio, le app che ti fanno scoprire “Che è il tuo miglior amico?” o “Chi ti vuole più bene?": accedendo a questi servizi, si permette l'accesso, oltre che ai propri dati, anche a molte informazioni sugli amici (basta visitare la loro bacheca), a prescindere dal loro consenso. La famigerata app di Cambridge Analytica raccoglieva i dati con questo sistema, ma con una aggravante: si presentava agli utenti come esperimento scientifico. Negli ultimi giorni, dopo l'esplosione dello scandalo, facebook ha rimosso altre app, come [CubeYou](#) e [AggregateIQ](#).

Quante e quali sono le app che raccolgono dati con questi metodi? Lo ritenete legittimo? È corretto che queste terze parti abbiano accesso anche ai dati degli “Amici”, che non hanno espresso il loro consenso all'utilizzo dei dati personali? Cosa pensate di fare in futuro per difendere la privacy di terze parti che non hanno espresso alcun consenso?

Una terza modalità, probabilmente illegale visto che manca il consenso degli interessati, consiste nella cessione di questi dati a terze parti. Una app come [Grindr](#) chiede agli utenti “Hai l'HIV?” o “Quando ti sei testato l'ultima volta” e vende queste informazioni ad aziende. La cessione dei dati personali è faccenda

sempre delicata. Basta pensare ai minori, un tema toccato anche dall'audizione di di Mark Zuckerberg dell'11 aprile 2018: il giorno prima Facebook era stato accusato da 23 associazioni di aver tracciato, per facilitare la raccolta pubblicitaria anche i minori di 13 anni (l'età minima fissata dal Nuovo regolamento europeo – Gdpr –, con la possibilità di salire fino a 16). La faccenda diventa esplosiva quando ad acquistare i dati personali (o a disporne) sono organizzazioni politiche, che le utilizzano nel corso delle campagne elettorali. Nei sistemi politici maturi, i risultati elettorali sono determinati dalle scelte degli elettori indecisi nei collegi incerti: spostare un numero relativamente piccolo di voti può ribaltare il risultato. Diventa cruciale identificare questi segmenti decisivi e raggiungerli con una comunicazione mirata.

In quali tornate elettorali e da quali forze politiche sono state utilizzate le informazioni sugli utenti? Che effetto ha avuto questa comunicazione mirata sull'esito delle elezioni?

Non si tratta di un problema, ma di diversi problemi assai complessi e intrecciati tra loro. Ed è troppo facile dire che la colpa è di Zuckerberg o dei social network. Quella a cui stiamo assistendo è una trasformazione epocale, nella quale gli antichi strumenti non servono più. La nostra identità, il rapporto tra sfera pubblica e privata, la politica con i processi partecipativi e deliberativi, sono cambiati.

Zuckerberg, Brin, Page & Co., con i loro ingegneri e programmatori, possono illudersi che basta trovare un algoritmo più efficace, che magari sappia discriminare tra il “Negro sei una scimmia torna nella giungla” e “Il signor Negro è desiderato al telefono”, tra la tetta della pornstar strizzata dalla gangbang e il seno luminoso della Maja Desnuda. È una scelta che qualunque cittadino dotato di buon senso fa in pochi centesimi di secondo e che la nuova Artificial Intelligence potrà forse imparare a fare: magari ci metteranno solo qualche mese, e non anni.

Ma non è questo il problema. L'algoritmo giusto, “politicalmente corretto”, non farà altro che confermare i nostri pregiudizi, o la volontà della maggioranza, che spesso nel corso della storia si sono rivelati sbagliati o addirittura criminali.

Pensa che basti disporre alcuni algoritmi più efficaci per risolvere il Problema? Non è il caso di fare una riflessione politica e filosofica un po' più seria, per capire come la rete 2.0 ha cambiato e sta cambiando il nostro contratto sociale? O lo avete già deciso voi, il nuovo contratto sociale, con i nostri diritti e i nostri doveri?

Per fortuna oggi lavorano artisti che si divertono ad aggirare i meccanismi censori della rete e ad accrescere la nostra consapevolezza sui dispositivi che gestiscono la nostra comunicazione e la nostra socialità. Per esempio [Giulia Marsico](#) o [Emir Shiro](#). Ma loro usano l'ironia, e finora gli algoritmi non sono riusciti a coglierla e forse non ci riusciranno mai. Jeremy Deller, presente in questi giorni a Milano con una grande installazione, una Stonehenge gonfiabile, più prosaicamente, offre “[le istruzioni per abbandonare Facebook](#)”. Ma il problema non è il singolo utente, e nemmeno Facebook (che ha sempre meno appeal sui più giovani, anche per i motivi di cui sopra). Il problema è il nuovo scenario nel quale, ci piaccia o no, siamo tutti immersi. Anzi, il nuovo scenario che stiamo costruendo con i nostri piccoli dati personali, destinati a diventare big data nelle mani di pochi soggetti privati ma politicamente decisivi.

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

