SCOPERTE

di TELMO PIEVANI

Basta una connessione in rete: tutti saremo ricercatori scientifici

Questa non è una scoperta sperimentale, ma sociale. I cittadini possono diventare protagonisti della ricerca scientifica: questa volta, però, non come donatori o come soggetti di studio, bensì come attori della ricerca stessa. Il movimento si sta diffondendo in tutta Europa e adesso ha una sua associazione, con sede al Museo di Storia naturale di Berlino, la European Citizen Science Association. La filosofia è quella di andare oltre la comunicazione della scienza e i laboratori didattici. Grazie alle nuove tecnologie, si coinvolgono direttamente gli studenti, le famiglie e gli appassionati nell'indagine sperimentale e nell'osservazione. Ciascuno, munito di tablet e smartphone, diventa responsabile di una piccola porzione della ricerca. Il lavoro coordinato di centinaia di persone sparse sul territorio può infatti dare risultati formidabili. Si può quantificare la biodiversità di un ecosistema, identificare insediamenti e spostamenti delle specie, monitorare l'andamento di crisi ambientali o sanitarie, istituire efficienti reti di segnalazione, creare gruppi di pazienti, costruire banche dati online, coinvolgere comunità marginalizzate. Si condividono i risultati della ricerca e le implicazioni sociali. Si impara il metodo, praticandolo. Qualcuno ha storto il naso davanti a questa scienza fatta «dal basso», temendo le approssimazioni dei dilettanti, che si possono evitare con un'attenta supervisione scientifica. In Italia un'esperienza di punta è al Museo di Storia naturale della Maremma (Grosseto). Le prime scoperte dovute a *citizen science* cominciano a essere pubblicate. Forse stiamo entrando davvero nell'era della cittadinanza scientifica attiva.

EUROPEAN CITIZEN SCIENCE ASSOCIATION

Il logo
La prima conferenza internazionale si svolgerà dal 19 al 21 maggio 2016 a Berlino. Titolo: *Citizen Science - Innovation in Open Science, Society and Policy*

Orizzonti

Nuovi linguaggi, scienze, filosofie, religioni

laLettura

Francesco Barilli è il #twitterguest

Francesco Barilli (Selvazzano Dentro, Padova, 1965) ha scritto *Piazza Fontana* e *Piazza della Loggia* (disegni di Matteo Fenoglio), *Carlo Giuliani. Il ribelle di Genova* (disegni di Manuel De Carli) ed è tra gli autori de *La traiettoria delle lucciole, antologia del nuovo giornalismo a fumetti italiano* (tutti per BeccoGiallo). Ha collaborato con «Liberazione», «Wired» e «la Lettura». Da oggi su Twitter consiglia un libro al giorno ai follower de @La_Lettura.

Grande fratello Programmi di riconoscimento, app, assistenti come Siri: il telefonino si trasforma in un microfono aperto

Zitto, lo smartphone ti ascolta

I sistemi vocali presenti su pc e cellulari registrano le nostre conversazioni, che possono essere «rubate» per venderci prodotti o, peggio, sorvegliarci

di SERENA DANNA

Per catturare le informazioni riservate di privati cittadini non servono tecnologie sofisticate o misteriosi programmi di sorveglianza. Può essere sufficiente il microfono installato sul telefono, collegato a un browser di navigazione del web o ad applicazioni. Se vi è mai capitato di ricevere pubblicità online su argomenti di cui avete discusso a cena con amici o sul divano con il partner a fine giornata, controllate la funzione microfono sul vostro cellulare. Probabilmente sarà attiva. In secondo luogo, provate a verificare a quante applicazioni avete permesso — senza pensarci troppo — l'utilizzo del microfono. Ci sono ottime probabilità che siano diverse.

I microfoni installati su iPhone, computer e iPad — gli stessi che servono per parlare al telefono, eseguire ricerche o dare istruzioni agli assistenti vocali — catturano le nostre parole, le conservano sui server delle aziende e le trasformano in testi. Quei documenti preziosi vengono archiviati e usati dai fornitori dei servizi per conoscere meglio i propri clienti e, giurano, migliorare il servizio; ma può succedere che vengano intercettati da siti terzi. Questi — nel migliore dei casi — li analizzeranno per trovare parole-chiave che identificano gusti, preferenze e desideri immediati delle persone, profilando così, con estrema precisione, la loro offerta commerciale.

Il *whistleblower* Thomas Drake, cripto-linguista della National Security Agency fino al 2008 (quando ha denunciato, prima di Snowden, attività illecite di spionaggio dell'agenzia), contattato da «la Lettura» ha dichiarato che le app collegate ai microfoni dei cellulari «in alcune circostanze sono ad alto rischio di spionaggio. Spegnete i microfoni e cancellate periodicamente le vostre ricerche dalla cronologia», ha esortato via mail.

Israele chiama Mountain View

Nel settembre 2013, sei mesi dopo il debutto del microfono per la ricerca vocale su Google, un programmatore israeliano, Tal Ater, ha scoperto un difetto in grado di trasformare il proprio pc letteralmente in un «microfono aperto» 24 ore su 24 e intercettabile da chiunque. Va detto che la funzione di ricerca vocale deve essere attivata dall'utente, ma quello che spesso sfugge (anche perché non è esplicitato) è che — una volta terminato il servizio — l'utente deve disattivare la funzione per evitare che Google continui a registrare e a trasformare in testi tutte le conversazioni che ascolta. La presenza del bug individuato da Ater renderebbe facile per i siti «male intenzionati» catturare quelle trascrizioni. A distanza di due anni dalla scoperta, Ater conferma via mail a «la Lettura» che il problema, poiché non viola formalmente alcuna norma, non è stato risolto del tutto da Mountain View.

Se è noto che gli assistenti vocali come Siri di Apple o Cortana di Microsoft conservano tutti gli audio per un periodo di circa due anni, quando permettiamo ad applicazioni di accedere ai nostri profili social (succede spesso poiché sono sempre di più quelle che offrono l'opzione per velocizzare i passaggi), bisogna verificare — ancora una volta — se tali applicazioni abbiano accesso al microfono. Si nasconde anche lì il rischio concreto di aziende e persone che possono controllarlo. «I server conservano la tua voce — spiega Bhiksha Raj, docente del Language Technology Institute della Carnegie Mellon University —, che può essere utilizzata per cercarne tracce in altri luoghi del web, per esempio su YouTube; oppure venduta ad aziende che la utilizzano per tracciarti o per scopi criminali: possono "editare" le registrazioni ed effettuarne di false».

Laboratori
Le tecnologie biometriche, che identificano i profili in base a caratteristiche biologiche, sono le più ambite. Una grande attenzione viene dedicata oggi alla voce

Il valore (economico) della voce

Le tecnologie biometriche sono quelle che identificano una persona in base a caratteristiche biologiche: il Dna, la retina, l'iride, le impronte digitali, la voce. Mentre in Italia il governo discute del «riconoscimento facciale» come strumento efficace per la prevenzione del terrorismo, gli studiosi della biometria assicurano che il segmento su cui aziende e governi stanno

ILLUSTRAZIONE
DI **FRANCESCA CAPELLINI**

Finanziamenti online Le campagne del sito

Crac & successi I conti (da rifare) di Kickstarter

di **PIETRO MINTO**

Lo scorso settembre Kickstarter ha cambiato ragione sociale diventando una Public Benefit Corporation, un'azienda con l'obiettivo di avere un impatto benefico nella società. Un grande passo che, secondo la giurisdizione statunitense, spetta alle imprese che sappiano dimostrare «di avere l'aspirazione di contribuire al bene pubblico», senza l'ossessione per crescita e bilanci. La scelta ha segnato una nuova fase nella vita del sito che dal 2009 permette a chiunque di presentare un progetto e chiedere soldi agli utenti sotto forma di donazioni, contributi o pre-ordini del progetto stesso. Kickstarter ha finanziato di tutto — film, gadget, servizi digitali — e reinventato in pochi anni il concetto di crowdfunding.

Nelle settimane successive alla svolta «benefica», però, il sito ha subito pesanti colpi di immagine che rischiano di danneggiare la candida reputazione della novella Public Benefit Corporation. Tutto è iniziato con Zano, un piccolo drone da 236 euro ideato da un'azienda britannica e pensato «per portare i selfie a un nuovo livello», con una videocamera manovrabile dal proprio smartphone. Non senza sorpresa, nel novembre 2014, la campagna è diventata il più grande successo europeo nella storia del sito (con 3,4 milioni di dollari raccolti), prima di sgonfiarsi in poco meno di un anno, quando i pochi modelli distribuiti (solo 600 su un pre-ordine di 15 mila) si sono rivelati fallati, costringendo l'azienda a rinviare la consegna di Zano. Dopo le recenti dimissioni dell'ingegnere-capo del progetto — dovute a «motivi di salute e differenze inconciliabili» con i superiori —, il progetto è collassato definitivamente, lasciando i finanziatori con un palmo di naso. Un buco nell'acqua notevole per una campagna così popolare e uno shock per il team di Kickstarter, che ha spiegato di aver scoperto dell'affaire Zano «come tutti voi, leggendo uno stringato aggiornamento nella pagina del progetto».

Ma era solo l'inizio. Nelle stesse settimane, un'altra stella di Kickstarter ha cominciato a spegnersi nonostante l'iniziale successo. «Coolest Cooler», un frigorifero portatile di ultima generazione, dotato di casse bluetooth, caricatore per smartphone e altri optional tra cui luci al led, è stato la campagna più fruttuosa nella storia del sito (prima di essere superato dall'orologio Pebble Time nel corso del 2015): 62.642 finanziatori per un totale di 13,2 milioni di dollari raccolti. Ryan Grepper, il suo creatore, sembrava avere il compito più facile del mondo: prendere la somma e usarla per mettere in produzione il prodotto. Poi, come per il drone Zano, le cose sono andate storte. Anche a causa degli scioperi che hanno colpito una delle ditte fornitrici del frigo, Grepper è stato costretto a mettere in vendita il suo frigo su Amazon (a 499 dollari) per terminare la produzione «e consegnare il prodotto ai finanziatori del progetto» — cosa che dovrebbe succedere entro aprile 2016. Così «Coolest Cooler» è entrato nel mercato in modo antitetico rispetto alla filosofia di Kickstarter: non disponibile a chi ne ha reso possibile, pagando, l'esistenza e nel contempo comodamente ordinabile su Amazon da chiunque.

Nonostante questi intoppi, Kickstarter rimane il principale attore nel settore del crowdfunding e una fucina continua di successi «facili», alcuni dei quali hanno sfruttato il meccanismo del sito in modi incredibili. Ne sa qualcosa Zack Danger Brown, che lo scorso anno ha deciso di raccogliere 10 dollari per prepararsi un'insalata di patate e, grazie alla viralità ottenuta dall'iniziativa, si è trovato con 55 mila dollari provenienti da quasi settemila utenti (che ha speso organizzando un party in Ohio).

Successo e fallimento sembrano assumere tratti inediti sul sito, coniugando l'approccio casalingo alla *start up culture*. Lo ha notato per primo Silvio Lorusso, ricercatore e designer italiano, ideatore di Kickended.com, un sito che archivia tutte le campagne Kickstarter concluse senza aver raccolto nemmeno un dollaro: una parata di fallimenti. Secondo Lorusso, dottorando allo Iuav di Venezia, gli ultimi crac testimoniano quanto l'approccio di molti utenti del sito sia viziato: «Il caso "Coolest Cooler" dimostra che il capitale raccolto non è un criterio efficace per misurare la riuscita di un prodotto, né tantomeno un sinonimo di "successo"». Per quanto riguarda le conseguenze delle campagne, Lorusso prevede che «il controllo di Kickstarter sulla riuscita sarà nettamente intensificato», così come richiedono molti degli utenti truffati.

Il rischio di queste nuove regole, spiega il ricercatore a «la Lettura», è quello di snaturare la natura stessa del sito con il rischio di penalizzare «proprio ciò su cui Kickstarter ha costruito la sua fortuna: grandi progetti nati nello scantinato di casa».

@pietrominto

investendo di più sia quello vocale. «La Lettura» ha avuto accesso a un documento riservato che rivela di un programma di sicurezza al vaglio del governo americano sulla «profilazione e individuazione dei cittadini» attraverso la loro voce. Come mai tutto questo interesse?

«La voce umana è un pattern unico», spiega Slobodan Ribaric, a capo del programma europeo Cost (Coopération européenne dans le domaine de la recherche Scientifique et Technique) sulla de-identificazione per la protezione di dati. «Non ci sono due persone con la stessa voce — continua —, ognuno ha una propria identità vocale che porta con sé informazioni come il sesso, l'età, il livello di educazione, lo stato di salute, quello emotivo e l'origine». Rita Singh del James K. Baker Center for Voice Forensic si spinge oltre. Spiega che la voce umana è un biomarcatore: può rivelare se una persona sta mentendo, se parla sotto costrizione, e livello di stress, rendendola uno strumento cruciale per la medicina e per la lotta al terrorismo e alla criminalità.

Il ruolo della Nsa

Singh è stata la impiegata numero uno del Center of Excellence creato dalla National Security Agency alla Johns Hopkins University per studiare le tecnologie di riconoscimento vocale, primo esempio «ufficiale» dell'interesse dell'agenzia verso il settore. Tra le rivelazioni di Edward Snowden, l'ex dipendente della Nsa che ha fatto luce sulle tecniche di sorveglianza di massa, una riguarda l'entusiasmo con cui l'agenzia ha festeggiato l'iniziativa «Google for Voice», il programma con cui Mountain View traduce in tempo reale in testo quello che ascolta. Se le trascrizioni delle telefonate, benché molto usate dalle intelligence, sono complicate e facilmente soggette a disturbi, il nuovo sistema lanciato da Google avrebbe permesso all'agenzia, quanto meno nelle sue intenzioni, di avere accesso a milioni di testi «puliti» con parole chiave già in evidenza. D'altronde, le tecnologie di conversione testi sono usate dalla Nsa da almeno dieci anni. L'agenzia utilizza metodi di «Natural Language Processing» per selezionare persone potenzialmente «interessanti» in giro per il mondo. E — secondo un documento del 2011 citato da «The Intercept» — avrebbero fondato in Afghanistan un laboratorio di «Tecnologia di linguaggio umano» per contrastare forze militari e terroristi sul campo.

«Da studioso di legge — afferma Oleksandr Pastukhov, uno dei massimi esperti europei di privacy — devo constatare che l'avvento delle tecnologie biometriche non ha ricevuto il livello di attenzione che merita». Il ricercatore spiega che la direttiva europea sulla protezione dei dati «non riconosce quei dati come *sensibili* — ovvero la categoria che ha diritto al più alto grado di protezione — ma impone semplicemente "una valutazione di impatto sulla protezione dei dati" prima di processarli».

Elsa Kindt, autore di *Privacy and Data Protection Issues of Biometric Applications*, spiega che per identificare i cittadini attraverso la voce non c'è bisogno di un'autorizzazione scritta: «Il riconoscimento vocale non richiede al momento che venga definito chi è intitolato a farlo, in quale circostanze e seguendo quali procedure».

I personaggi
Thomas Drake (in alto) è un ex manager della National Security Agency considerato il primo *whistleblower* (informatore) dell'agenzia di sicurezza dove ha lavorato fino al 2008. Drake ha rivelato le attività illegali di spionaggio dei cittadini americani a seguito degli attentati terroristici dell'11 settembre 2001. È stato accusato di spionaggio e processato in base all'Espionage Act, ma nel 2011 tutte le accuse contro di lui sono cadute. Rita Singh (sopra) è ricercatrice del James K. Baker Center della Carnegie Mellon University di Pittsburgh, Pennsylvania. È stata la prima impiegata del Center of Excellence creato dalla National Security Agency alla Johns Hopkins University per studiare le tecniche di riconoscimento vocale

In cerca di soluzioni

Al momento i tentativi portati avanti da accademici e gruppi di ricerca per arginare il rischio sorveglianza insito nei dispositivi audio si muovono nella direzione della de-identificazione: una tecnica per nascondere o rimuovere identificatori personali e sostituirli con «surrogati» per evitare che quelle informazioni vengano attribuite a una persona in particolare e quindi utilizzati per uno scopo diverso da quello iniziale. «Ci sono due approcci principali per la protezione della privacy — illustra Slobodan Ribaric —. Il primo è basato sul principio della trasformazione della voce: andiamo a modificare le caratteristiche non linguistiche di un discorso, senza cambiare il contesto. Il secondo è basato sul criptaggio delle caratteristiche biometriche della voce».

Le ricerche del team di Bhiksha Raj al Carnegie Mellon provano invece a far sì che i sistemi che utilizzano la voce degli utenti possano catturare l'informazione (e portare a termine il servizio) senza però identificare la persona. Ma il problema è anche culturale. «I cittadini non si rendono conto che le informazioni che rilasciano ai device attraverso la loro voce — continua Raj — sono preziose quanto i numeri delle carte di credito, gli indirizzi, le mail riservate e tutte le informazioni che hanno imparato a proteggere da occhi online indiscreti». Il ricercatore fa un paragone con internet degli anni Novanta, quando tutti scrivevano e cercavano qualsiasi argomento online senza preoccuparsi delle conseguenze sulla privacy. Succede oggi con le comunicazioni vocali: le direzioni al navigatore, le istruzioni per le ricerche, i messaggi vocali così popolari su WhatsApp. Stiamo costruendo un enorme database di informazioni preziosissime sul nostro conto. «Vi siete mai chiesti — conclude — dove finiscono quelle informazioni?».

@serena_danna