DOPPIOZERO

Sei disposto a rinunciare alla tua privacy per salvarti la vita?

Oliviero Ponte Di Pino
18 Aprile 2020

La sera del 16 aprile 2020, il Commissario straordinario per l'emergenza sanitaria, Domenico Arcuri, ha ufficializzato la scelta dell'app italiana per il tracciamento. “Immuni” è stata sviluppata dalla società milanese Bending Spoons, che ha al suo attivo app di successo per Yoga e Fitness, in collaborazione con il Centro Medico Sant'Agostino e Jakala. Ha vinto la selezione operata dal gruppo di 74 esperti della task force lanciata il 31 marzo 2020 dal Ministro per l’innovazione tecnologica e la digitalizzazione in accordo con il Ministero della Salute. Il ministro Paola Pisano aveva spiegato che la app avrebbe dovuto “individuare e valutare soluzioni tecnologiche *data driven* per supportare il Governo e gli altri pubblici decisori nella definizione di politiche di contenimento del contagio da Covid-19”.

Delle 319 proposte arrivate, il 10% (compresa “Immuni”) usava il bluetooth (che traccia i contatti), anche se il presidente della task force Colao avrebbe preferito utilizzare anche il GPS, che traccia la posizione.

Durante la fase 2, ovvero il progressivo ritorno alla normalità dopo il lockdown, “Immuni” ci permetterà di verificare l'utilità del Capitalismo della Sorveglianza per la salute pubblica. L'emergenza coronavirus segna uno spartiacque, come ha scritto Yuval Harari sul “Financial Times” il 30 marzo. Fino a poche settimane fa, il “tracciamento” era riservato ai sospetti criminali (nel corso delle indagini giudiziarie), ai detenuti agli arresti domiciliari o ai malati di Alzheimer (il braccialetto elettronico). I servizi segreti israeliani già usavano questi dati nell'ambito della lotta contro il terrorismo.

I sondaggisti avevano ridotto la questione a una domanda: “Sarebbe d'accordo che lo Stato controllasse gli spostamenti anche senza il loro consenso, limitatamente al periodo dell'epidemia?” Secondo SWG, il 64% degli italiani si era dichiarato favorevole.

Si tratta ora di estendere questo controllo capillare all'intera popolazione, su base volontaria (come accade con “Immuni”) oppure a insaputa dei cittadini (attingendo ai big data di aziende private come le telecom o i big di internet) oppure obbligandoli a fornire informazioni personali. Per il virologo Roberto Burioni, a giudicare dal tweet del 12 aprile, la sorveglianza va accettata senza troppe storie: “Anche io chiedo che la privacy sia tutelata; ma chi di fronte a una epidemia che sconvolge le nostre vite dice 'mi spengo GPS e bluetooth' lo classifico tra i babbei”.

Una app non è un vaccino. Perché “Immuni” possa risultare efficace nel contenere l'epidemia, devono verificarsi diverse condizioni. In primo luogo, deve essere scaricata da un gran numero di persone: in Italia dovrebbero essere alcune decine di milioni di utenti, tutti dotati di smartphone (anche se non tutti gli italiani ne hanno uno). Deve essere aggiornata periodicamente, anche due volte al giorno in caso di positività. Va integrata con altre misure, come tamponi e test sierologici di massa. Infine va inserita in un flusso di comunicazione che può essere gestito solo dal sistema sanitario.

“Se c'è una cosa che questa pandemia ci rivela è che dati e computazione corrispondono alla nostra sopravvivenza, capacità e possibilità di esistere. (…) Dall'accesso a enormi quantità e qualità di dati dipende, quindi, la nostra possibilità di conoscere, comprendere, posizionarci ed agire nei confronti delle sfide fondamentali del nostro ambiente” (Salvatore Iaconesi, *Dati usati per ricostruire le relazioni sociali*, in “Il Sole-24 Ore”, 5 aprile 2020).

Il cittadino come miniera di dati

Già oggi ognuno di noi già oggi produce un'enorme quantità di dati, in quanto consumatore, perché è iscritto a un social network, quando usa un servizio pubblico, o semplicemente quando si sposta... Secondo Michail Kosinski della Stanford University, nel 2012 ciascuno di noi produceva in media 500MB al giorno, oggi siamo a 62 GB.

Negli ultimi anni si è aperta una gigantesca caccia ai dati personali. Alcuni vengono forniti volontariamente e consapevolmente. Altri vengono “regalati”, in apparenza di nostra volontà attraverso i “contratti” che firmiamo online, ma in realtà “estratti” senza alcuna reale possibilità di controllo da parte nostra. Altri dati siamo obbligati a fornirli: per esempio, attraverso l'autocertificazione sulle ragioni degli spostamenti “necessari” che ci viene richiesta dalle autorità di polizia.

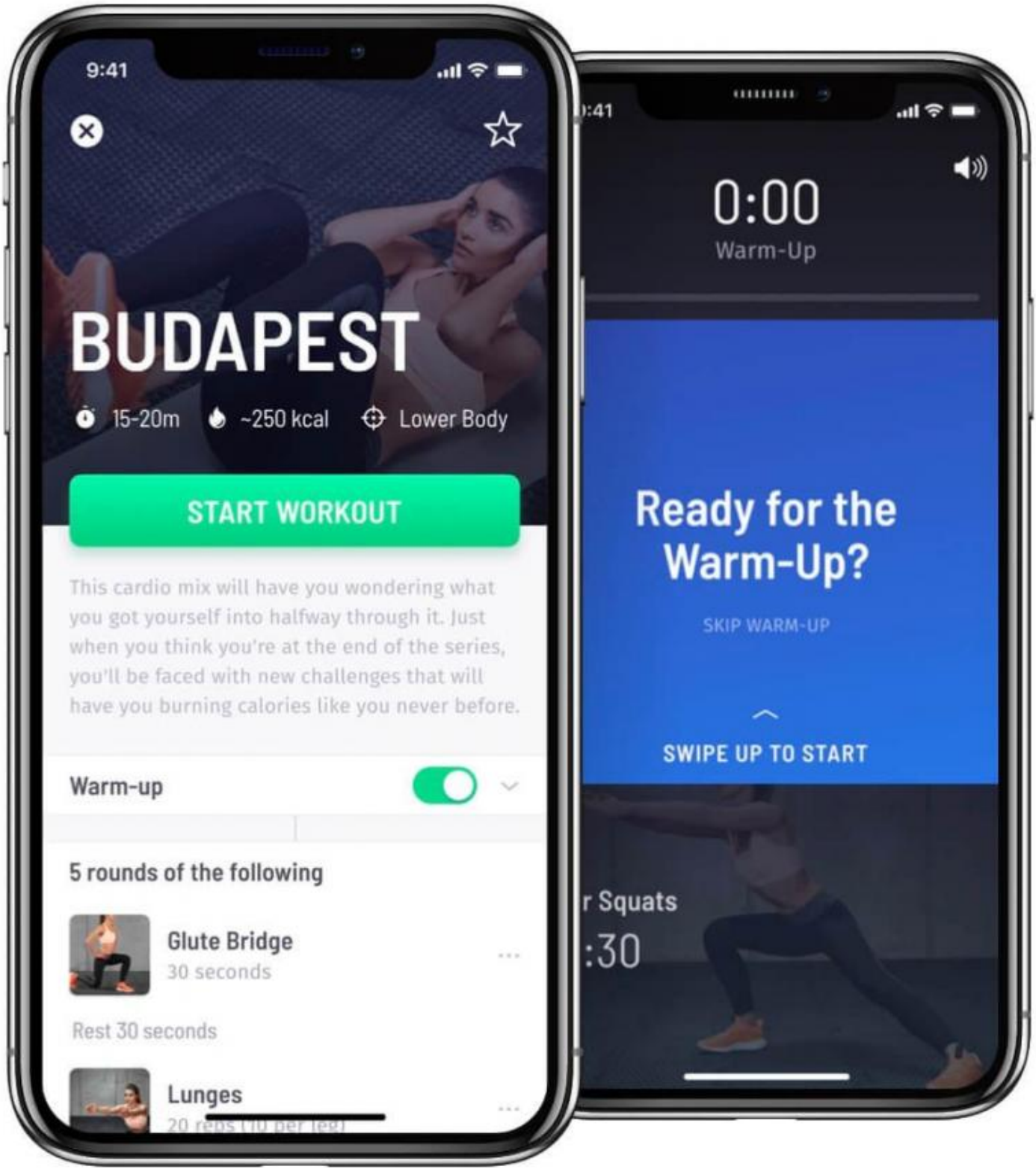
Un primo problema riguarda dunque la consapevolezza dei dati che forniamo e il controllo che ne abbiamo. Quali dati? Quanti? Sono veri o falsi? Possiamo consultare i nostri profili e magari correggerli?

Un secondo ordine di problemi riguarda l'uso che viene fatto di queste informazioni. Per il bene della collettività? Per una campagna di marketing personalizzata? Perché un assicuratore valuti le mie probabilità di ammalarmi prima di propormi una polizza? Per la salute pubblica?

Chi usa “Immuni” lo farà su base volontaria, è ovviamente consapevole delle informazioni che inserisce, e che restano sul suo dispositivo. Il suo smartphone conserva anche la lista dei contatti recenti via bluetooth (ma anonimizzati).

Le criticità sono notevoli. La vicinanza tra due smartphone a volte non è una informazione sufficiente. È dunque necessario valutare con attenzione (e con ulteriori indagini) la prossimità e il livello di esposizione al rischio, che dipendono da molteplici fattori, come per esempio il tempo di esposizione al contagio, se avvenga in spazi chiusi o aperti, affollati o meno. Ma questi elementi sono ancora oggetto di indagine scientifica (e la app deve poter prevedere di “aggiustare” i parametri sulla base delle nuove evidenze). In realtà il sistema non richiede la perfezione, ma solo un accettabile margine di errore.

Il valore delle informazioni di un singolo individuo dipende in maniera determinante dalle operazioni che si possono compiere su una grande mole di dati, attraverso strumenti statistici in grado di “estrarre” correlazioni significative. Questo sapere aggregato è del tutto impermeabile al controllo individuale: è proprietà di chi gestisce i dati e gli algoritmi di estrazione e correlazione, incomprensibili ai profani.



La raccolta della gestione dei dati: problemi qualitativi e quantitativi

La raccolta e la gestione di questi dati comportano diverse problematiche.

Un primo versante riguarda la loro qualità, la precisione e l'affidabilità.

Gli attuali sistemi di geolocalizzazione, sia attraverso le celle telefoniche sia attraverso il GPS attivo in Italia, riescono a determinare la nostra posizione con un margine di errore di 7-13 metri (a volte anche di più). Se la distanza interpersonale sotto la quale si attiva il contagio è di un metro o due, la risoluzione è insufficiente: servono sistemi militari, il 5G (già attivo in Corea del Sud) o il bluetooth, utilizzato anche dalla app frutto dell'inedita alleanza tra Google e Apple.

Una seconda criticità riguarda la gestione delle enormi quantità di data point prodotti da un'intera popolazione. La raccolta di questa mole di dati e l'"estrazione" delle informazioni necessarie sono attività costose, che richiedono potenti investimenti sia in ricerca e sviluppo sia di gestione. In Italia è un problema serio, visti i disastri della app utilizzata dall'Anpal (Agenzia Nazionale Politiche Attive Lavoro) per gestire il reddito di cittadinanza, e il flop dei computer dell'INPS quando si è trattato di accogliere le domande per i 600 euro destinati ai lavoratori autonomi. È in ogni caso prevista una fase di sperimentazione, in alcune Regioni e situazioni pilota, a cominciare dai lavoratori della Ferrari di Maranello e di Modena.

Chi raccoglie e gestisce i dati: pubblico e privato

Siamo tutti clienti di telecom, social network, piattaforme per transazioni finanziarie (banche, carte di credito e debito), piattaforme di streaming come Netflix, supermercati con carta fedeltà, app per viaggi e turismo... Usiamo tutti i negozi online, a cominciare dal gigante Amazon. Ognuna di queste aziende ha centinaia di migliaia di utenti registrati, a volte centinaia di milioni.

Tutte queste piattaforme operano da anni una raccolta dati sistematica, intensissima e di fatto incontrollata (o forse incontrollabile). In teoria, tutti i dati necessari a un tracciamento di massa della popolazione, sono già stati raccolti (e vengono utilizzati).

I profili, prima di essere condivisi o diffusi, vengono di solito "anonimizzati", anche se è molto facile dare un'identità al singolo utente "anonimizzato", attraverso opportuni algoritmi e incrociandoli con altre banche dati. A Facebook bastano 10 like per conoscerci meglio dei nostri colleghi, 100–150 like per conoscerci meglio dei nostri amici, 250–300 like per conoscerci meglio del nostro partner e prevedere il nostro comportamento.

Questi dati vengono raccolti per finalità commerciali e spesso ceduti a terze parti anche per altri scopi: il caso più clamoroso è quello di Cambridge Analytica. Ci trasformano nei bersagli di una comunicazione per microtarget, dopo aver profilato le preferenze e la situazione (anche economica, sanitaria, psicologica, emotiva...) del singolo utente.

Anche i nostri corpi, i nostri stati d'animo, le nostre emozioni vengono trasformati in big data e possono essere manipolati da una comunicazione pervasiva.

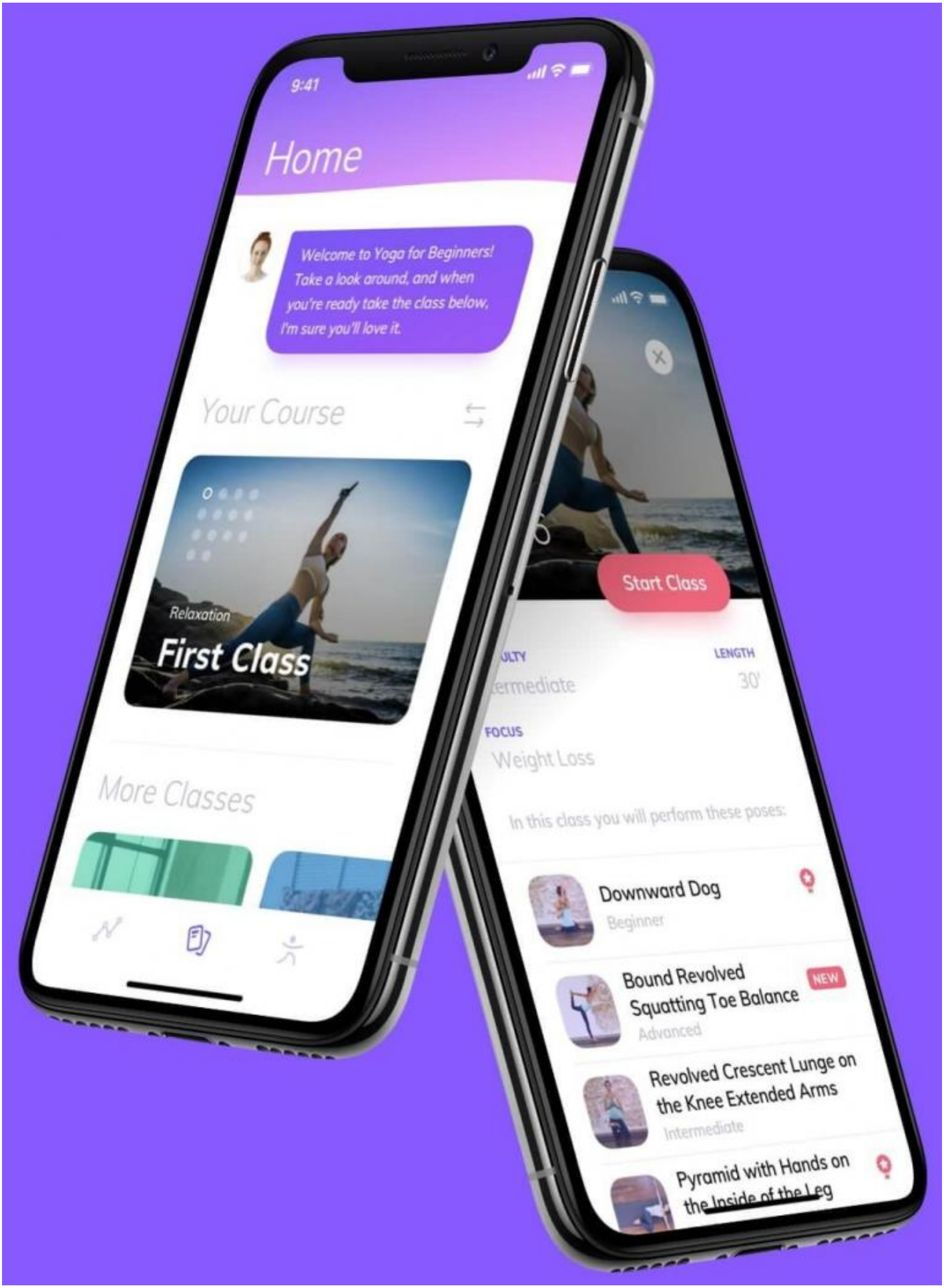
Autorità governativa

La scelta più semplice – quella che viene spacciata come "l'unica possibilità" – è un monitoraggio centralizzato e il rispetto delle misure adottate imposto da sanzioni feroci. È uno strumento potentissimo: "Se ascolti un discorso del Grande Capo e il braccialetto rileva i segni rivelatori della rabbia, hai finito", semplifica Harari.

I regimi totalitari non hanno problemi. I big data delle aziende sono già a disposizione delle autorità e dunque il tracciamento sociale è già attivo, senza alcun controllo da parte della popolazione.

I regimi democratici dovrebbero invece dotarsi di regole, procedure, organi di controllo e di garanzia. Lo devono fare in gran fretta e in emergenza, informando i cittadini delle varie opzioni e dei loro rischi.

A complicare il quadro, è necessario regolare i rapporti tra Stato ed enti locali, e tra i singoli Stati e la Comunità Europea, altrimenti si rischiano estenuanti conflitti di interesse, ma soprattutto la raccolta di dati disomogenei e disallineati.


9:41
Home
Welcome to Yoga for Beginners! Take a look around, and when you're ready take the class below, I'm sure you'll love it.
Your Course
Relaxation
First Class
More Classes
Start Class
LENGTH
30'
FOCUS
Weight Loss
In this class you will perform these poses:
Downward Dog
Beginner
Bound Revolved Squatting Toe Balance
NEW
Advanced
Revolved Crescent Lunge on the Knee Extended Arms
Intermediate
Pyramid with Hands on the Inside of the Leg

Per molte big companies, associarsi a un progetto di salvaguardia delle vite di milioni di persone non è solo un'efficace operazione di marketing: è prima di tutto la riprova della loro "bontà", la conferma della loro visione del mondo. Lo "stato di emergenza" dimostra che le tecnologie del controllo, che molti considerano una minaccia, rappresentano l'unica possibilità di salvezza per l'umanità.

Tuttavia queste infrastrutture non sono state concepite per proteggere la privacy, ma anzi per abolire il confine tra vita pubblica e ambito privato. Inoltre "sono, è triste dirlo, infrastrutture di consumo individualizzato, non di solidarietà e assistenza reciproca. Come ogni piattaforma digitale, possono essere usate per vari scopi, tra i quali attivismo, difesa dei diritti e collaborazione, ma simili usi solitamente implicano un costo elevato e spesso invisibile. Costituiscono delle fondamenta molto fragili per un ordine sociale non liberista e post-soluzionista, che dovrà essere popolato da attori che non siano consumatori, startup e imprenditori" (Evgeny Morozov, *L'emergenza sanitaria e il rischio del totalitarismo*, in "Internazionale", 13 marzo 2020).

Le azioni concrete

Una volta raccolti ed elaborati i dati, si tratta di passare all'azione.

Alcune misure saranno di carattere generale e suggeriti dai dati già a disposizione delle autorità: per esempio, di fronte a un incremento dei contagi o dei ricoveri in una certa regione, si possono reintrodurre "zone rosse". Si possono prevedere misure di contenimento destinate a segmenti di popolazione sulla base di età, sesso o professione, o per fasce orarie...

Queste app possono inviare messaggi personalizzati ai singoli utenti, con diverse modalità, più o meno coercitive: dal consiglio paterno ("Meglio se resti a casa", "Meglio passare di là") all'intimazione, con sanzioni più o meno pesanti ("La tua amante, che hai incontrato martedì scorso, è positiva. Vieni domattina alle 9 per il tampone, altrimenti ti vengono a prendere i Carabinieri e paghi una gran multa. Ah, dimenticavo, sappiamo in ogni istante dove ti trovi").

Perfino i disciplinatissimi sudcoreani hanno trasgredito, uscendo senza cellulare: infatti è stato imposto l'uso dei braccialetti elettronici.

Nel caso un utente di "Immuni" diventi positivo, il medico curante (che dispone di una app personalizzata) gli chiederà di sbloccare, sempre volontariamente, la lista dei contatti anonimizzati, che in questo caso riceveranno una notifica del tipo: "Sei a rischio contagio", con le istruzioni del caso.

Le conseguenze politiche

Il coronavirus sta offrendo un irripetibile trampolino di lancio ad alcuni dittatori (o aspiranti dittatori), che approfittano dell'emergenza per accumulare poteri. Al regime cinese, il caso Wuhan (ammesso che i numeri ufficiali siano reali) ha confermato la necessità e l'efficienza di un capillare modello di controllo, e implicitamente anche di *social rating*, il "punteggio sociale" che consente per esempio l'accesso a determinati servizi, come mutui e viaggi.

Per un regime democratico, la sfida è limitare drasticamente la libertà individuale, restando fedele ai propri valori.

Il ministro dell'Innovazione Paola Pisano, in audizione alla Commissione trasporti, poste e telecomunicazioni della Camera, ha parlato di una app che venga adottata su base volontaria, *open source* (ovvero con un codice pubblicamente consultabile) e raccolta di dati "sufficientemente anonimi" (una formulazione che ha messo in sospetto alcuni giuristi).

Per quanto riguarda la privacy, il bluetooth di "Immuni" consente di rilevare la prossimità, ma non la posizione e gli spostamenti degli individui.

Il garante per la privacy, Antonello Soro, in audizione alla Commissione trasporti della Camera l'8 aprile 2020, ha espresso i suoi timori: "Non potrebbe ritenersi effettivamente valido, perché indebitamente e inevitabilmente condizionato, il consenso prestato al trattamento dei dati acquisiti con tali sistemi, se prefigurato come presupposto necessario, ad esempio, per usufruire di determinati servizi o beni (si pensi al sistema cinese)".

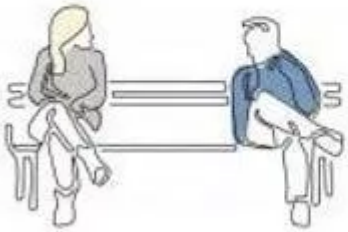
Non basta chiedere agli italiani se sono disposti a rinunciare alla privacy per salvarsi la vita. La differenza tra un regime totalitario e una democrazia non consiste nel fatto che un dittatore impone la sorveglianza centralizzata di massa con la violenza, mentre i regimi democratici fanno la stessa cosa, ma dopo aver "informato" e "convinto" i cittadini che questa è l'unica soluzione possibile.

Abbiamo diverse alternative e dobbiamo scegliere la migliore. Dobbiamo farlo democraticamente. Se la nuova tecnopolitica democratica ancora non esiste, ce la dobbiamo inventare, con una diversa consapevolezza e nuove forme di partecipazione. I protocolli imposti durante lo "stato di eccezione" non devono diventare la normalità. La guerra dichiarata dalle autorità e dai media non deve avere per nemico i cittadini, ritenuti "responsabili" del contagio.

Come ha sottolineato il Consiglio d'Europa il 30 marzo 2020: "È possibile usare tecnologie di tracciamento contro il coronavirus, ma la tenuta democratica richiede alcune accortezze, per evitare di ritrovarci domani in una società della sorveglianza di massa".

Non sarà facile immaginare e costruire un mondo in cui le app non siano strumento di controllo e manipolazione, ma creino consapevolezza, emancipazione e partecipazione attiva.

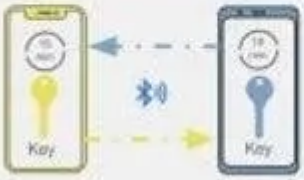
Alice and Bob meet each other for the first time and have a 10-minute conversation.



Bob is positively diagnosed for COVID-19 and enters the test result in an app from a public health authority.

A few days later...

Their phones exchange anonymous identifier beacons (which change frequently).



With Bob's consent, his phone uploads the last 14 days of keys for his broadcast beacons to the cloud.

Google