

Attenti alla App

scritto da perUnaltracittà

Perché stare attenti alla App di tracciamento Covid-19 | Undicesimo Aggiornamento

Aggiornamento del 25/06/2020 ore 15.00

Questo articolo doveva parlare specificatamente della App di tracciamento contatti che doveva fare parte delle strategie di contrasto alla diffusione dell'epidemia da Covid19 che ancora non era disponibile. Abbiamo fatto vari aggiornamenti (siamo a undici) perché quello che uno aveva scritto poteva essere smentito dai fatti o perché si presentavano fatti nuovi o nuove considerazioni. Adesso l'App c'è, ma l'attenzione mediatica si è spostata. In più la gente ha voglia di normalità e meno paura, per cui la App è un flop con il risultato che come avevamo sospettato (vedi più sotto) tutti ci troviamo nel sistema operativo dei nostri telefoni la predisposizione ad un tracciamento non soltanto dei nostri spostamenti (c'è già), ma anche dei nostri incontri e delle nostre frequentazioni. È teoricamente inattiva, ma chi controlla che Google o Apple l'attivino? In particolare la Apple il cui sistema operativo è chiuso e non verificabile?

L'App Immuni è dunque disponibile già da oltre una settimana. L'hanno scaricata e installata soltanto circa il 10% dei possessori di telefoni. Per avere una certa efficacia si era parlato di tutt'altre cifre, tra il sessanta e il settanta per cento. Questo non ha impedito che ci fossero le prime "vittime". Ovviamente nessuna App può essere totalmente "immune" da falsi negativi e falsi positivi, quello che però lascia allibiti (anche se una serie di dubbi li avevamo segnalati) è il fatto che la procedura che segue la segnalazione di contatto non preveda nessun tipo di verifica (con tampone o anche sierologica), con il risultato di recludere obbligatoriamente nella propria abitazione per 15 giorni i segnalati dalla App anche se possibili falsi positivi senza nessuna verifica da parte dell'autorità sanitaria. Scarichi la App e questa ti segnala per un contatto che potrebbe essere stato contagioso, il risultato è una quarantena obbligatoria senza alcuna verifica. Una delle strategie più importanti per contrastare la diffusione del virus è quella di individuare i contagiati attraverso una campagna di tamponi la più grande possibile. Ma la procedura non prevede che a ogni positività segnalata dall'App segua il tampone.

Aggiornamento del 09/06/2020 ore 13.00

La trasmissione Report sul terzo canale della rete nazionale, conferma tutti i dubbi che qui avevamo sollevato, [questo il link](#).

In particolare l'imprecisione delle misurazioni con l'alta probabilità di falsi sia positivi che negativi. [Un altro sito](#) ha testato l'App facendo emergere anche in questo caso tutti i problemi che avevamo segnalato ed in particolare il fatto che dietro l'App non ci sia una strategia specifica tanto che l'App stessa sia poco comprensibile nelle sue funzioni. Il sospetto rimane il solito: l'emergenza pandemica ha stimolato la messa in atto di una tecnologia di tracciamento che oltre alla posizione restituisce anche tutti gli incontri che riguardano ogni utente. Cosa questo comporti lo potete intravedere continuando a leggere questo articolo.

Aggiornamento del 03/06/2020 ore 13.00

È disponibile negli store l'App Covid 19, in Italia "Immuni". Se desiderate qualche informazione e possedete uno smartphone Android potete andare su "impostazioni", quindi su Google poi su "Notifiche di esposizione al Covid-19, dove al secondo paragrafo scoprirete che la funzione di geo-localizzazione deve essere attivata. Questo significa che quello che paventavamo più sotto è una possibilità reale. Google e Apple possiedono una tecnologia che non soltanto può tracciare dove si recano le persone, quindi dove, ma anche chi incontrano e per quanto tempo. Già il garante della privacy aveva sollevato dei dubbi nel documento che dettava le linee guida:

20 In effetti, un ampio corpus di ricerche ha dimostrato che dati relativi all'ubicazione ritenuti

anonimi possono di fatto non esserlo. Le tracce di mobilità dei singoli individui sono

caratterizzate intrinsecamente da forte correlazione e univocità. Pertanto, in determinate

circostanze possono essere vulnerabili ai tentativi di re-identificazione.

21 Un'unica serie di dati che consenta di rintracciare l'ubicazione di un individuo lungo un arco di

tempo significativo non può essere pienamente anonimizzata. Questa affermazione resta valida

se non si riduce in misura sufficiente la precisione delle coordinate geografiche registrate, o se non si eliminano dettagli del percorso di tracciamento, e anche se si mantiene solo l'ubicazione dei luoghi in cui l'interessato permane per un tempo considerevole. E vale anche in caso di insufficiente aggregazione dei dati relativi all'ubicazione.

Il problema attualmente non è l'applicazione in sé che potete scegliere liberamente di scaricare oppure no, è di nuovo il fatto che dei soggetti privati gestiscano in maniera quasi monopolista delle tecnologie che potrebbero limitare le nostre libertà.

Aggiornamento n. 8

La relazione che il Copasir (Comitato parlamentare per la sicurezza della Repubblica) ha rilasciato è stata resa pubblica in vista della presentazione in parlamento. La relazione segnala vari punti critici che riprendono diversi dei dubbi e delle attenzioni che avevamo segnalato in questo stesso articolo (vedi più avanti). La prima osservazione è che ancora mancano alcuni elementi definatori dei modi di funzionamento della APP stessa rivelandosi in alcuni casi una semplice cornice «i cui dettagli, molti dei quali rilevanti, devono essere ancora individuati e determinati, attraverso atti di natura amministrativa. Ad esempio, il sistema di Contact tracing viene definito complementare rispetto alla ordinaria modalità in uso nell'ambito del Ssn, mentre il Comitato ritiene che esso dovrebbe essere considerato integrativo di tali modalità, per evitare che il C.T. digitale sostituisca il tracciamento ordinario»



ATTENTI ALLA APP

Il Copasir segnala che a partire dalla composizione dell'azionariato si possono «evidenziare rischi non trascurabili sul piano geopolitico, che secondo quanto emerso dalle audizioni sarebbero non mitigabili» Dietro la Bending Spoons ci sono infatti: la H14 dei tre figli di Silvio Berlusconi, la holding Nuo Capital della famiglia Pao Cheng di Hong Kong e StarTip (veicolo di Tamburi Investments Partners spa che rimanda a: Amplifon, Eataly, Ferrari, Moncler, Furla, Fca, Prysmian, Azimut Benetti, Beta, iGuzzini, Advanced Accelerator Applications, Roche Bobois, Servizitalia.) «Infatti, la definizione dettata da privati dell'architettura dell'intero sistema informatico, inclusa la App, nonché la necessità di ricorrere a soggetti privati non nazionali, per quanto da considerare affidabili, per il Cdn destinato a contenere i dati raccolti, potrebbero prestarsi a manipolazioni dei dati stessi, per finalità di diversa natura: politica, militare, sanitaria o commerciale».

Mettere le mani sui dati può significare «potrebbe far sovrastimare o sottostimare l'entità stessa dell'epidemia - dice sempre il Copasir - Va inoltre evidenziato come, qualora ciò dovesse essere confermato, la soluzione di trasmettere i dati dei cittadini italiani alla Content Delivery Network pare contrastare con il contenuto dell'articolo 6, comma 5, del decreto-legge n. 28 del 30 aprile 2020, in cui si esplicita in maniera chiara che la piattaforma, di titolarità pubblica, è realizzata esclusivamente con infrastrutture localizzate sul territorio nazionale» Occorrerà anche un adeguato controllo per far sì che i dati raccolti attraverso l'applicazione non possano «essere trattati per finalità diverse da quella di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute, salva la possibilità di utilizzo in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica» Dice allora il Copasir: «Per quanto appena evidenziato un simile 'transito di dati', anche se fosse temporaneo e avvenisse esclusivamente per mezzo di sistemi informatici presenti sul territorio nazionale, dovrebbe obbligatoriamente essere non solo chiarito ed esplicitato, ma anche e soprattutto regolamentato con estrema attenzione sotto il punto di vista giuridico, al fine di adempiere a quanto previsto dalla normativa europea e nazionale in materia di trattamento di dati personali»

Concludendo poi: «In tal senso, potrebbe essere opportuno verificare che nessun attore nazionale e soprattutto internazionale, ivi compresa la società aggiudicataria dello sviluppo della App, possa in qualsivoglia modo accedere

direttamente o incidentalmente ai dati raccolti, anche nel caso in cui questo soggetto abbia dato un qualsiasi apporto - anche tecnologico - per la realizzazione o per l'efficacia del sistema nazionale di allerta Covid-19. Ciò al fine di impedire che simili informazioni - rilevanti sia sul piano della qualità sia della quantità e soprattutto della capillarità - possano più o meno direttamente entrare nel possesso di attori europei e internazionali, sia pubblici sia privati, a vario titolo interessati».

Le criticità sono tante e le risposte ancora mancano. Occorre perciò mantenere sveglia la vigilanza, ribadendo il discorso fatto precedentemente. Ci sembra che la App, al di là della sua efficacia, arrivi in ritardo e che le energie che si sono scomodate per la sua realizzazione non possano essere in una prospettiva usa e getta. La App rimanda a una tecnologia di tracciamento certamente appetibile per il [Capitalismo Digitale](#).

Aggiornamento n. 7:

[A questo link](#) potete trovare la notizia che l'aggiornamento dei sistemi operativi dei telefoni da parte di Google e di Apple, è stata appena licenziata. Da oggi 1 (22/05/2020) le App specifiche di tracciamento in relazione alla pandemia da Corona virus potranno essere implementate e messe a disposizione negli specifici *store*. Al di là dell'App in senso stretto, da adesso in poi i telefoni con sistema operativo Android o iOS (praticamente tutti) potranno implementare una funzione che "traccia" i nostri incontri. Ovviamente c'è una differenza a partire dal fatto che questo dato sia conservato sul proprio dispositivo o sul *cloud*, (ne abbiamo già parlato - vedi più avanti), ma quello che ci interessa sottolineare è il fatto tecnico in sé: i nostri telefoni sono degli strumenti capaci di memorizzare ogni incontro che noi facciamo e con chi lo facciamo. È una pura potenzialità, non ancora messa in atto, ma a disposizione! Non c'è nessun complottismo, nessun grande fratello, soltanto l'attenzione da dover riservare al fatto che all'interno dei sistemi operativi dei nostri telefoni questa possibilità è presente e che potrebbe essere attivata, stante le cose, da delle aziende private fuori dal controllo che si può esercitare nelle democrazie mature e (in particolar modo per i sistemi operativi il cui codice non è pubblico) anche a nostra insaputa.

Altro piccolo aggiornamento. [Ecco il parere](#) di uno dei maggiori epidemiologi del mondo. Uno scienziato che lavora con i *big data* e che ne ha appunto quella familiarità per la quale la sua opinione acquista il dovuto valore:

E la polemica sulla App?

Io non l'ho capita. Ma davvero pensiamo di sconfiggere Covid con una app?

Proprio lei è scettico?

Sì, e non perché da informatico non abbia fiducia nelle tecnologie, si figuri. Ma perché le persone vanno se-gui-te. Lei se lo immagina uno che si alza la mattina e tutto tranquillo si autoisola perché lo schermo del telefonino gli diventa rosso?

In teoria dovrebbe essere così.

Ma no, perché quell'infecto è un uomo che non può essere lasciato da solo. Magari sono un padre e ho una famiglia da far campare. Magari sono un precario e devo uscire. Magari non ho lo spazio domestico per tutelare i miei.

Esattamente quello che è accaduto in Italia.

Sono isolato a casa, in quarantena, non faccio il tampone, nessuno sa come sto, e poi magari chiamo la ASL che non mi risponde perché ha tante telefonate. Folle.

Quindi per questo la app non va bene.

Le app vanno benissimo, possono essere un grande supporto, ma serve un servizio umano. Serve una tutela a distanza che non si può realizzare solo con un algoritmo o con le faccine sul telefonino.

Altro parere questa volta di Alessandro Vespignani, fisico di formazione, da quasi vent'anni vive e lavora in America; alla fine degli anni '90 è passato dallo studio dei virus informatici a quelli biologici. Ha lottato contro Ebola in Congo, Zika in Sudamerica, la pandemia influenzale del 2009, la Sars. Ora fa parte del team della Casa Bianca che si occupa del coronavirus. Da una intervista [sul Manifesto](#)

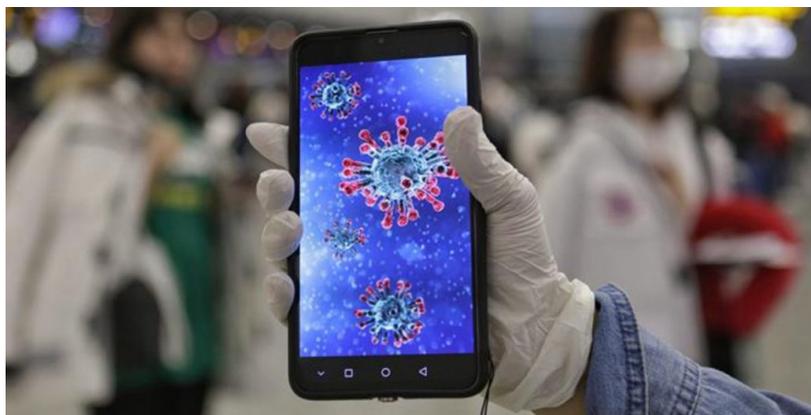
Riguardo il tracciamento, lei che ha una formazione da ingegnere informatico. Quanto bisognerebbe concedere a livello di privacy alle app di tracciamento?

Bisogna che i dati vengano aggregati per rintracciare i focolai, quindi un po' bisognerà concedere ma si può fare tracciamento del virus con le app in modo non troppo invasivo. Bisogna però accompagnare la app a un esercito di esseri umani, perché se la app ti dice che sei stato in contatto con il virus hai bisogno di qualcuno che si occupi di te, che ti porti la spesa, che mandi un certificato al tuo datore di lavoro, che venga a farti i test se sviluppi dei sintomi. Inoltre queste app servono ora, se le fanno tra 2 mesi sono inutili. C'è una

sottovalutazione generale della velocità di questo virus che non lascia pause di riflessione.

In Asia e soprattutto in Cina la lotta a quello che ormai è chiamato il Covid-19 passa per il controllo totale dei singoli attraverso il digitale, senza alcuna privacy. «Una biopolitica digitale che va di pari passo con una psicopolitica digitale. L'Europa non ne adotti il modello», esorta Byung-Chul Han filosofo coreano che insegna in Germania. Ma qual è questo controllo e perché in Europa non si è messo in piedi niente di simile? Il fatto è che le sensibilità di orientali e occidentali nei riguardi della privacy sono molto diverse. In Cina in particolare il controllo digitale dei cittadini è diffuso e pervasivo. La finzione distopica messa in scena nell'episodio "[caduta libera](#)" di Black Mirror, è sorpassata dalla realtà del sistema di crediti sociali "[sesamo](#)" dei cinesi ([ne abbiamo parlato qui](#)).

Ma adesso, di fronte alle performance cinesi nella lotta contro la diffusione del virus, in confronto con i disastri occidentali - anche a causa di una sanità pubblica erosa da decenni di tagli e sempre più ceduta al privato - anche in occidente si stanno vagliando le possibilità di **un uso anti virale delle tecnologie digitali**.



L'idea è che attraverso una qualche forma di tracciamento si possano individuare gli interscambi, le promiscuità, gli incontri tra le persone per poter individuare tutti quelli che hanno avuto a che fare con un soggetto positivo ed operare di conseguenza

(tamponi, quarantena etc.) Ovviamente insensata l'idea del sindaco Nardella di chiedere alle compagnie telefoniche i dati sugli spostamenti captati tramite i dati di cella, per inquisire i furbetti della passeggiata. Sappiamo che il posizionamento tramite la triangolazione tra le antenne è meno preciso del GPS basato sui satelliti e quindi si rischierebbe di prendere delle grosse cantonate. La tracciatura, i nostri spostamenti, sono invece dati disponibili da parte di Google che li ricava dal nostro uso di "Maps". [Qui le indicazioni per poterli vedere anche noi](#). Ma sono dati che se non incrociati con quelli degli altri non possono servire a questo scopo. Ecco che, su indicazioni delle autorità europee, che hanno dato le linee guida per una eventuale App di tracciamento, si è scelto di usare un'altra

tecnologia, quella bluetooth.

In realtà non serve una mappa completa dei nostri reciproci spostamenti, basta registrare gli incontri. Serve un sensore che sondi la presenza nel suo raggio di azione di un sensore compatibile. Tutti gli smartphone moderni ne sono dotati, anche quelli da due lire (pochi centesimi, spiegazione per i millennials). Basterà che tutti carichino un'apposita app che monitorerà le presenze nelle proprie vicinanze di altri dispositivi, a quanti metri si trovano e per quanto tempo. Si aprono sicuramente problemi di privacy; di conservazione ed uso dei dati così ricavati, ed è su questo che il garante della privacy ha posto una serie di paletti che intricano tutta la problematica. Ecco comunque che la task force messa in piedi dal governo ha scelto un App - chiamata "Immuni" - prodotta dalla Bending Spoons, start up milanese che vede presenti all'interno del proprio capitale di H14 (family office italiano di Barbara, Eleonora e Luigi Berlusconi, azionista di Fininvest), Nuo Capital (holding di investimenti della famiglia Pao/Cheng di Hong Kong) e StarTip (veicolo controllato al 100% da Tamburi Investments Partners S.p.A che concentra tutte le partecipazioni in start-up e in società attive nel segmento del digitale e dell'innovazione). Tra i cui consulenti di Bending Spoons c'è John Elkann, presidente di FCA. La partecipazione di Elkaan sulla supervisione tecnica dell'app è fondamentale in quanto si dice su alcuni quotidiani che l'app potrebbe essere testata nelle prime settimane presso la fabbrica Ferrari di Maranello, prima dei test tra il pubblico.

«La app Immuni si potrà scaricare liberamente, nessuno sarà obbligato ad installarla, ma il download sarà solo su base volontaria. E' composta da due parti. La prima è un sistema di tracciamento dei contatti che sfrutta la tecnologia Bluetooth, attraverso cui rilevare la vicinanza tra due smartphone nell'ordine di un metro. In questo modo, la app conserva sul dispositivo di ciascun cittadino una lista di codici identificativi anonimi di tutti gli altri dispositivi ai quali è stata vicino entro un certo periodo. Nel caso in cui si venga sottoposti a test per Coronavirus, con un codice il cittadino può caricare su un server su cloud i dati raccolti dalla sua app, compresa la lista anonima delle persone a cui è stato vicino. Il server a sua volta calcola per ogni identificativo il rischio di esposizione all'infezione sulla base di parametri come la vicinanza fisica e il tempo, e genera una lista degli utenti più a rischio, ai quali è possibile inviare una notifica sullo smartphone. Ma la app presenta anche, ed è questa la seconda funzione, una sorta di diario, nel quale a ciascun utente verranno chieste alcune informazioni

rilevanti riguardanti anche la propria salute e che dovrebbe essere aggiornato tutti i giorni con eventuali sintomi.» ([Qui il sito di provenienza dell'informazione](#))

Il sistema, come molti nei vari forum hanno fatto notare, ha comunque qualche problema. Il sistema, la app può registrare incontri che non ci sono mai stati. Pensate a due persone separate da una parete, da un vetro, da un pannello di plexiglas. o che ci sono stati ma non dovrebbero essere presi in considerazione come quello che un infermiere fa emergere in uno di questi forum:

Sono infermiere domiciliare, AL LAVORO protetto da FFP2, tuta, occhiali, guanti, visiera, ecc posso avere contatti con persone COVID+, (anche a domicilio) ma, dotato degli opportuni DPI, il problema non si pone (il cellulare è in sacchetto chiuso nella divisa interna, acceso con la suoneria tolta). Finito il turno ho lo stesso rischio "sociale" di tutta la popolazione (es. supermercato, ecc). Quindi per infermieri, medici, ecc l'app dovrebbe (in base al codice fiscale e alla verifica dello stesso all'ordine professionale) chiedermi se sono "al lavoro, protetto da DPI" (e questi contatti dovranno essere gestiti con le procedure sanitarie in uso, che abbiamo usato fino ad adesso senza app) oppure "non sono al lavoro e non indosso DPI" e quindi ho il rischio sociale di tutta la popolazione. Lo stesso problema si pone, ad esempio, con i medici di guardia medica. Se mi reco al domicilio per una visita e sono protetto da DPI il problema "contagio" non si pone.

Si tratta dei falsi negativi e di quelli positivi. Ora se è normale mettere in quarantena i positivi accertati, lo sarebbe molto meno quella di usare gli stessi criteri per quelli presunti. **Si sta per caso sdoganando quel concetto di palese incostituzionalità di perseguire un reato presunto, cosa già esperita nel caso del daspo sportivo e tentata con quello urbano?**

Altre domande aperte includono se il Bluetooth sia abbastanza preciso da distinguere i contatti stretti dato che la sua portata, sebbene tipicamente intorno ai 10 metri, può teoricamente raggiungere fino a 400 metri e che la potenza del segnale varia ampiamente in base al chipset, alla batteria e al design dell'antenna. La distanza che prenderà in considerazione per constatare la positività del contatto, quanto sarà precisa?

Sicuramente si potranno progettare implementazioni che affrontino alcuni o tutti questi problemi ma la sicurezza che questo avvenga ci può essere data soltanto da

chi controlla il controllore, esercitando cioè quelle forme di controllo tipiche delle democrazie e non delegando tutto il potere ai decisori che dichiarando lo stato di eccezione se lo sono preso.

C'è poi un altro problema. Anche in questo caso come ci si dovrebbe comportare?

Si parla di lavorare e conservare dati aggregati; si parla di usare a questo scopo un server italiano collocato in Italia; di cancellazione dopo un certo periodo; si dice che la app non sarà geo referenziata. Ma gli interrogativi che nascono, non hanno risposte facili. **Chi conserverà questi dati visto che non c'è una struttura pubblica di cloud? Un privato, ma a quale prezzo?** Come, in denaro o in natura? Accettare di mettere a disposizione le proprie strutture non equivarrà ad una azione di lobbying? Così come potrebbe anche essere la fornitura a titolo gratuito della App? Apple e Google stanno facendo campagna affinché i dati raccolti non vengano centralizzati, proponendo che i dati vengano conservati all'interno dei propri *device*. Sembra anche che stiano lavorando congiuntamente a una loro App o a implementare il tutto nei sistemi operativi con la possibilità di una incompatibilità tra "Immuni" e quest'ultimi. Che siano le API o una vera e propria implementazione, ha poca importanza. Gli interrogativi rimangono gli stessi. Codice aperto o codice proprietario? Chi ci garantirà che non ci venga implementato anche un "cavallo di troia" per carpire dati così importanti come quelli sanitari?

Un'altra domanda è cosa fanno i funzionari con le intuizioni che anche i dati anonimi e aggregati possono generare. Incoraggiare il distanziamento sociale volontario è una cosa, aumentare gli interventi della polizia in zone non conformi è un altro. I dati creeranno immagini fuorvianti del comportamento all'interno di comunità a basso reddito o di immigrati in un modo che potrebbe portare a risultati pregiudizievoli come una eccessiva attività di polizia.

Anche quando ti dicono che i dati saranno raccolti in forma anonima, forse non basta, più tecnici e scienziati hanno fatto presente che è sorprendentemente difficile rendere anonimi i dati. Ciò è doppiamente vero per quanto riguarda i dati sulla posizione, perché le persone si rivelano da dove vanno; anche le informazioni anche apparentemente approssimative sulla posizione di una persona spesso la identificano in modo univoco. Ad esempio, secondo uno studio, solo conoscere il codice postale di dove lavori e dove vivi identificherà in modo univoco il 5 per cento della popolazione. Con qualche riferimento in più, l'uso di

un mezzo pubblico o altro, si può arrivare a ipotizzare un indirizzo di residenza. E, naturalmente, una volta identificato l'indirizzo di casa di una persona, rimangono pochi dubbi sulla sua identità. Nel caso di una pandemia, anche senza una solida identificazione univoca, potrebbero seguire stigma e molestie. Immagina quattro persone diverse che vivono tutte nel codice postale X e lavorano nel codice postale Y: anche se non sono identificate in modo univoco, se uno risulta positivo e i loro dati sulla posizione sono pubblicati, anche gli altri tre potrebbero essere sospettati e discriminati.

Il problema è che, [come abbiamo più volte detto](#), il sistema, l'algoritmo, la struttura macchinica dell'universo digitale sono viziate da **un pregiudizio di fondo, quello della ricerca del profitto che permea e condiziona tutta la struttura** che prolifera sull'onda dell'entusiasmo tecnologico che fa da apripista a ogni implementazione robotica.

Il punto sul quale tenere sveglia l'attenzione è che **tutto sembrerebbe lecito ai tempi della pandemia. Ma finiti questi tempi, cosa succederà?** A noi pare che, anche a pensar bene, si sia in terribile ritardo. Una App ben funzionante sarebbe stata più utile agli inizi. Il sospetto è che al di là della sua applicazione all'evento pandemia, uno strumento di monitoraggio di questo genere avrebbe la sua appetibilità. **Se colossi come Apple e Google si mettono a lavorare alla cosa in questo momento, significa che la cosa potrà avere anche altri risvolti. Quali?**

Sappiamo che l'industria estrattiva della modernità digitale si basa su poche "[terre rare](#)" e sui dati. [All'industria della sorveglianza](#) interessano non solo gli spostamenti, ma anche chi incontri, quando, dove e per quanto tempo. [I dati sanitari](#) hanno addirittura un valore maggiore. Dati che potrebbero interessare anche a qualche altro soggetto più o meno istituzionale. Per farci cosa? Pensare che qualcuno affili le lame o lucidi i fucili, non ci rende più tranquilli semplicemente perché non li vediamo in uso; quando poi lame e fucili non si presentano in quanto tali, un filo di preoccupazione in più è lecito mettercela.

Un'altra domanda. Il garante della privacy [dice](#) : "Se non si fanno i tamponi immediatamente dopo aver individuato gli infetti, la app è inutile". C'è dunque questo piano di screening, o c'è solo la APP?

La APP crea una nuova categoria sociale, quelle dei contagiosi probabili. Se nelle

fasi successive ci saranno accessi e comportamenti consentiti a tutti o si discriminerà qualcuno lo si farà su una presunzione? Gli algoritmi di sorveglianza possono scovare principalmente le cose probabili. Lavorando sui dati, lavorano infatti sulle probabilità, le certezze sono manifeste. Ma si potrà agire in qualche modo in base alla probabilità?

Non tutto il mondo è paese: [il Mit giudica le APP](#)

***Laboratorio Politico per Un'altra città**