CONTACT TRACING

OVVERO

LE APP
DI TRACCIAMENTO
DEI CONTATTI

LE APP DI TRACCIAMENTO DEI CONTATTI

Oltre ai droni (per ora usati più che altro a fini propagandistici e per seminare terrore, che non per altro) e alle misure di contenimento domiciliare subito seguite dal rafforzamento dei controlli in città, in strada, in spiagge e in parchi ed aree verdi, che dal 10 marzo al 4 maggio hanno portato all'identificazione di più di 13 milioni di persone e a migliaia di multe, tra le strategie messe in campo a livello globale dai vari governi per contenere il contagio da coronavirus c'è il cosiddetto "contact tracing", il tracciamento dei contatti, cioè l'uso dei dispositivi mobili (smartphone) per la mappatura degli spostamenti dei soggetti che potrebbero essere entrati in contatto con persone infette. Si tratta di un protocollo previsto dall'Organizzazione Mondiale della Sanità (OMS) in caso di epidemie, e che i governi han fatto proprio basandosi sull'esempio di paesi come Cina, Sud Corea, Taiwan, Honk Hong, Singapore ed altri, tra i primi a sviluppare questo tipo di tecnologie di controllo.

IL RUOLO DELL'UNIONE EUROPEA

Partiamo dal fatto che la materia è disciplinata dalle norme di ciascuna nazione che recepiscono la Direttiva 2002/58/CE sulla tutela dei dati personali nel contesto di reti e servizi di comunicazione elettronica (che riguarda anche l'accesso ai dispositivi mobili come gli smartphone).
Il principio è che i relativi trattamenti possono svolgersi sulla base del consenso dell'interessato o se i dati sono resi anonimi o aggregati, però dove questo non sia possibile, cioè quando non si possa (o non si voglia) trattare i dati in modo anonimo, l'articolo 15 della Direttiva consente agli Stati Membri l'introduzione di norme emergenziali per ragioni di sicurezza pubblica.
Anche lo European data protection board (EDPB), ovvero il **Comitato Europeo sulla Protezione Dati** che riunisce le Autorità garanti europee per la privacy, ha ribadito di recente che il regolamento generale europeo per la protezione dei dati e per la privacy (**GDPR** UE 679/2016) ammette forme di controllo dei dati personali in caso, per esempio, di gravi emergenze sanitarie, com'è stata considerata la pandemia da coronavirus dichiarata dall'OMS. Il testo del regolamento, che non è un'indicazione ma è direttamente vincolante per gli stati membri anche se offre flessibilità per alcuni aspetti, dice che le deroghe sono ammesse "*se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana*" (art.46 GDPR). Il GDPR è stato adottato il 14 aprile 2016 ed è diventato esecutivo a partire dal 25 maggio 2018 e si applica a qualsiasi ente ed impresa, indipendentemente dalla sua ubicazione, che stia elaborando le informazioni e i dati personali all'interno della UE e dello spazio economico europeo, regolando anche il trasferimento di dati personali al di fuori di questo spazio.
Le deroghe ai regolamenti comprendono per esempio l'omissione della classica informativa sull'uso. Anche se, per tracciare gli spostamenti di una persona, i dati dovrebbero essere usati in forma anonima e aggregata, per produrre, per esempio, mappe sulla concentrazione degli smartphone in un determinato luogo, per misurare l'affollamento di focolai del contagio o individuare assembramenti. E qualora i dati non possano essere usati in forma anonima, l'EDPB avverte che, prima di adoperarli, un governo dovrebbe dotarsi di leggi ad hoc. Il Garante europeo

della privacy ha comunque ribadito che simili applicazioni dovrebbero essere installate sì su base volontaria, ma precisando che la base giuridica del trattamento non deve essere quella del consenso della persona, ma piuttosto l'interesse pubblico. Un bell'ossimoro!
Più nello specifico, lo sviluppo delle app di tracciamento si inquadra in un processo già in atto in Europa, che prevede la collaborazione degli Stati membri al fine di definire e perfezionare l'uso di queste tecnologie. La stessa OMS aveva propugnato il "contact tracing" come metodo per aiutare a prevenire l'espansione del coronavirus che causa il Covid-19.
La **Commissione Europea** e il **Parlamento Europeo** hanno presentato ad aprile una tabella di marcia che accompagni la revoca delle misure di contenimento per il coronavirus in Europa, la *"Risoluzione del Parlamento europeo sull'azione coordinata dell'UE per lottare contro la pandemia di COVID-19 e le sue conseguenze"* del 15 aprile (n.2020/2616 (RSP)).
Nel documento si parla del tracciamento dei contatti come una delle misure idonee per il controllo della pandemia. Un'indicazione simile era già stata diffusa il 9 aprile dall'**ECDPC** (European Centre for Disease Prevention and Control) in un report tecnico dettagliato, contenente anche una proposta di algoritmo per gestire le segnalazioni di soggetti positivi o potenziali positivi.
Il **Comitato Europeo sulla Protezione Dati** (EDPB)**,** ha pubblicato, sempre a metà aprile, le linee guida sulle app di tracciamento, contenute in una lettera firmata dalla presidente Andrea Jelinek e indirizzata alla Commissione Ue, con l'obiettivo di creare un modello paneuropeo nella gestione delle app. La direzione intrapresa, infatti, non è quella di una app unica per tutta l'Europa, ma di un approccio europeo condiviso che renda disponibili principi comuni e standard tecnici da applicare poi sulle diverse app a livello nazionale.
Il 15 aprile, a Bruxelles è stato così adottato il "*Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States"*, un voluminoso documento tecnico recante considerazioni sulle applicazioni adottabili dagli stati membri per l'esigenza COVID 19.
Da parte sua, recependo le note dell'EDPB, la Commissione Europea ha divulgato una serie di raccomandazioni riguardo allo sviluppo delle tecnologie di tracciamento, per favorire l'approccio comune da parte degli Stati. Secondo la Commissione, queste linee guida dovrebbero essere guardate come a *"una cassetta degli attrezzi congiunta verso un approccio coordinato per l'uso di app per smartphone che rispettino gli standard di protezione dei dati dell'UE"*. Una *"cassetta degli attrezzi"* dai quali i vari Paesi possono attingere per costruire le rispettive app nazionali, in associazione alle direttive dell' EDPB.
Gli Stati membri non sono comunque tenuti a chiedere l'autorizzazione all'Unione Europea per approvare i loro progetti di contact tracing, però non possono trascurare alcuni requisiti essenziali stabiliti dalla Commissione Ue, le cui principali sono:

1. conformità alle normative UE in materia di protezione dei dati e di tutela della privacy;
2. stretto coordinamento con le autorità sanitarie e approvazione di queste ultime;
3. installazione su base volontaria e dati rimossi quando non più necessari;
4. tecnologia basata su Bluetooth;
5. dati anonimizzati o pseudonimizzati;
6. interoperabilità della tecnologia in tutta l'UE

Gli Stati membri hanno inoltre il compito di riferire in merito alle misure intraprese a livello nazionale entro il 31 maggio 2020 e renderle accessibili alla Commissione per una valutazione.

La Commissione valuterà poi i progressi compiuti e pubblicherà relazioni periodiche a partire da giugno 2020. Dell'interoperabilità si sta occupando la *eHealth network* della Commissione europea. Ai tavoli partecipa anche il ministro della Salute italiano e la task force di esperti del ministero dell'Innovazione guidati dal responsabile tecnologico del dipartimento **Paolo de Rosa**,
come consulenti per la parte tecnica.
La stessa Commissione ha annunciato in un comunicato (*https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043*) che, il 16 giugno, i membri dell'Unione europea hanno concordato gli standard tecnici per assicurare l'interoperabilità tra le app nazionali di tracciamento dei contatti ma quelle che funzionano sulla base di un'architettura decentralizzata. L'accordo riguarda la vasta maggioranza delle app di tracciamento decentralizzate già lanciate o in procinto di esserlo nell'Ue. La app del proprio paese di residenza ora dovrebbe funzionare senza interruzioni quando si viaggia in altri Stati membri dell'Ue.
Per il momento il sistema tuttavia funzionerà, come detto, solo per le app decentralizzate (tra cui "Immuni" in Italia e Corona-Warn-App in Germania) e non per quelle centralizzate (come "Stop Covid" in Francia).

LA CORSA AL CONTACT TRACING IN ITALIA

Per quanto riguarda l'Italia, che ha avuto notizia del primo malato di Covid-19 il 21 febbraio a Codogno, nel Lodigiano, il Governo attraverso il primo DECRETO-LEGGE 9 marzo 2020, n. 14 del 9 marzo (https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2020-03-09&atto.codiceRedazionale=20G00030&elenco30giorni=false) ha affidato alla Protezione civile, al ministero della Salute e all'Istituto superiore di sanità, poteri speciali sull'uso dei dati. La Protezione civile, con questo decreto, può acquisire in deroga e trattare i dati biometrici o quelli sulla salute personale. Il fantomatico diritto alla privacy disciplinato dal GDPR [Regolamento europeo 679/2016] ha cambiato dunque repentinamente i suoi connotati con il pretesto dell'emergenza COVID-19. Comunque il Governo italiano aveva già sospeso di fatto il diritto alla protezione dei dati personali, almeno in materia fiscale. Col disegno di legge di bilancio 2020, depositato al Senato il 12 novembre scorso, aveva legiferato "*che l'Agenzia delle Entrate, previa pseudonimizzazione dei dati personali, si avvale delle tecnologie, delle elaborazioni e delle interconnessioni con le altre banche dati di cui dispone, per elaborare criteri di rischio utili a far emergere posizioni da sottoporre a controllo e incentivare l'adempimento spontaneo*".
Per le stesse finalità "*la Guardia di finanza è autorizzata ad utilizzare le informazioni contenute nell'Archivio dei rapporti finanziari*". La profilazione algoritmica dei contribuenti per fini fiscali è partita dal 1 aprile. In Italia esistono oltretutto delle norme specifiche (introdotte con il decreto legge 14 del 2014) con le quali vengono previste modalità più "snelle" di gestione dei dati personali da parte dei soggetti istituzionali in situazioni di "crisi", ed anche il garante per la privacy ha ammesso che la Protezione civile può scambiare dati sensibili con altri soggetti (forze dell'ordine, comuni, enti, ma anche privati). Successivamente, il Governo ha nuovamente derogato alle norme

in materia di protezione dei dati personali con l'articolo 14 del Decreto Legge 9 marzo 2020 [Art. 14, DL 9 marzo 2020, n. 14 "Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19"], attraverso il quale ha dotato la Protezione civile di nuovi poteri straordinari in materia di privacy che hanno preparato, di fatto, la svolta sul controllo dei dati degli individui per motivi di sicurezza e salute. Il Governo ha inoltre concesso alle Regioni, attraverso i DPCM del presidente del Consiglio, la facoltà di adottare poteri straordinari in materia di privacy, che possono derogare alle leggi europee in materia di dati sensibili.
Non va peraltro dimenticato il quadro in cui si inserisce l'adozione di tali dispozioni.
La dichiarazione dello "stato emergenziale" nel gennaio di quest'anno in seguito all'epidemia da coronavirus ha portato a partire dal 9 marzo all'adozione da parte del Governo di misure estremamente restrittive delle libertà personali su tutto il territorio nazionale, che inizialmente sarebbero dovute durare 2 settimane, prorogate poi di volta in volta anche se nell'ordinamento italiano non è previsto espressamente un vero "stato di emergenza". La dichiarazione di un qualcosa che si avvicina allo stato di emergenza è prevista unicamente da una fonte legislativa (Decr. Lgs n. 1/2018 - Codice della Protezione Civile) la quale attribuisce poteri straordinari al Presidente del Consiglio che può procedere in deroga alle disposizioni di legge ma con dei limiti e solo per un tempo massimo di 12 mesi (che comunque è un bel lasso di tempo, in cui se si vuole si ha tempo anche per cambiare le leggi a proprio favore...la storia insegna!). Negli stessi articoli costituzionali che regolano la libertà personale (art. 13) e la libertà di circolazione (art. 16) è prevista la possibilità di stabilire dei limiti al loro esercizio per motivi di emergenza sanitaria o di sicurezza pubblica, procedendo però con atti aventi forza di legge, non quindi con i famosi DPCM ma con Leggi o Decreti-Legge, sottoposti successivamente all'iter parlamentare. Abbiamo invece assistito in questi ultimi mesi alla centralizzazione del potere politico-sanitario nelle mani del presidente del Consiglio, dei suoi consiglieri sanitari e dei vari gruppi di "esperti", con l'emanazione continua di decreti presidenziali (DPCM). In questo quadro, L'**Enac** (l'Ente Nazionale per l'Aviazione Civile), in deroga alle disposizioni vigenti, ha autorizzato, con una nota inviata al Ministero dell'Interno, dei Trasporti e della Giustizia, e a diverse articolazioni di polizia locale, il controllo attraverso i droni per "*le operazioni di monitoraggio degli spostamenti dei cittadini sul territorio comunale*" da parte delle Polizie locali (https://www.lettera43.it/coronavirus-app-tracciamento/).
Era dunque solo questione di tempo per vedere esteso l'utilizzo del tracciamento dei dati tratti dal traffico telematico e telefonico, ottenuti dai provider internet (la cosiddetta *data retention*), fino a poco tempo fa consentito solo per la scoperta e la repressione dei reati – anche in funzione preventiva – per ragioni legate al controllo dell'epidemia. A mancare, ovviamente, sono norme specifiche, non soltanto decreti che deroghino alle leggi attuali. Ma sicuramente, prima o poi, arriveranno anche quelle. Così, dopo la nomina del "comitato tecnico-scientifico", un "team di esperti" per "*dare concreta attuazione alle misure adottate per il contrasto e il contenimento del diffondersi del virus con particolare riferimento alle soluzioni di innovazione tecnologica*", introdotto con il varo del decreto del 17 marzo (il cosiddetto Cura Italia), il 24 marzo, il governo ha lanciato *"Innova per l'Italia"*, un'iniziativa congiunta del Ministro per l'Innovazione tecnologica e la Digitalizzazione, Paola Pisano, il Ministro per lo Sviluppo Economico, Stefano Patuanelli, e il Ministro per l'Università e la Ricerca Gaetano Manfredi, insieme ad **Invitalia** (Agenzia nazionale per l'attrazione degli investimenti e lo sviluppo d'impresa S.p.A.) e con il supporto tecnico di **AgID** (Agenzia per l'Italia Digitale) e della struttura del Commissario Straordinario per l'emergenza Coronavirus, Domenico Arcuri oltre al coordinamento fornito dall'Istituto Superiore di Sanità e dall'Organizzazione Mondiale della Sanità (https://www.key4biz.it/contact-tracing-con-una-call-il-governo-prova-a-trovare-la-tecnologia-anti-covid-19/296467/).

L’iniziativa, in gergo una “call”, è stata lancita per aziende, università, enti e centri di ricerca pubblici e privati, associazioni, cooperative, consorzi, fondazioni e istituti, chiamati a “*fornire un contributo*” per il contrasto al diffondersi del virus.

Questo contributo riguardava:

1. il reperimento, l’innovazione o la riconversione industriale delle proprie tecnologie e processi, per accrescere la disponibilità di dispositivi di protezione individuale (mascherine) e di respiratori per il trattamento delle sindromi respiratorie;
2. il reperimento di kit o tecnologie innovative che facilitino la diagnosi del Covid-19, quali tamponi ed altri strumenti per la diagnosi facilitata e veloce;
3. la disponibilità di tecnologie e strumenti per il monitoraggio, la prevenzione e il controllo del Covid-19, quali ad esempio tecniche e algoritmi di analisi e intelligenza artificiale, robot e droni.

Qui, ovviamente, è la terza voce a interessarci, perché si rivolge direttamente agli sviluppatori di tecnologie di tracciamento. Il tracciamento dei contatti era stato proposto fin da fine febbraio anche dall’economista Carlo Alberto Carnevale Maffè, dal tecnologo Alfonso Fuggetta e altri. Era stato sostenuto, in tempi non sospetti, dal manager, non ancora presidente della task force per la “fase due”, Vittorio Colao, ex Vodafone. Nel frattempo, l’Europa sviluppava le sue linee guida.
Fra i primi sostenitori dell’uso dei big data e del contact tracing in Italia, come detto, ci sono insigni docenti universitari, come **Alfonso Fuggetta**, presidente del centro **Cefriel** al Politecnico di Milano, che ha sedi a Londra e New York e una a Milano, in Viale Sarca 226, fondato da università e aziende per l’innovazione tecnologica, e **Carlo Alberto Carnevale Maffè**, professore di organizzazione aziendale alla School of management dell’**università Bocconi di Milano**, che sostengono il tracciamento dei cellulari e l’applicazione delle misure “*dei paesi asiatici*”.
Alfonso Fuggetta, pure membro del “team di esperti” del governo italiano, uno dei primi apologi del contact tracing in Italia, ha espresso il proprio malumore il 12 aprile su Twitter contro *“quelli che dicono che non bisogna usare il GPS”*.
C’è anche chi, come **Walter Ricciardi**, consulente del ministero della Salute, per la “Fase2” vorrebbe un sistema di data tracing in cui sono unificate banche dati con informazioni sui dati anagrafici, sulle condizioni di salute e sulle attività lavorative che riguardano i singoli cittadini. Per poi utilizzare le celle telefoniche, i geolocalizzatori degli smartphone e i movimenti delle carte di credito per tracciare le persone. Quello che è stato descritto come un vero e proprio panopticon digitale (https://www.corrierecomunicazioni.it/privacy/coronavirus-ecco-la-strategia-in-tre-step-per-il-data-tracing/).
Il 24 marzo e per tre giorni consecutivi, sul sito del ministero dell’Innovazione tecnologica e la digitalizzazione, soggetti pubblici e privati hanno così potuto inviare proposte per lo sviluppo di *“tecnologie e soluzioni per il tracciamento continuo, l’alerting e il controllo tempestivo del livello di esposizione al rischio delle persone e dell’evoluzione dell’epidemia sul territorio, strumenti di analisi di Big Data, tecnologie hardware e software utili per la gestione dell’emergenza sanitaria”*.
Alla “call” hanno risposto 823 fra aziende, centri di ricerca e università: 504 con proposte su telemedicina e 319 su analisi dei dati sulla diffusione del coronavirus e app di tracciamento.

L’APP DI TRACCIAMENTO ITALIANA

Quattro giorni dopo il lancio di ***Innova per l’Italia***, la “fast call” governativa, il 31 marzo il Ministro per l’innovazione tecnologica e la digitalizzazione ha nominato il “*Gruppo di lavoro data-driven per l’emergenza COVID-19 (…) con il compito di procedere in tempi rapidi alla valutazione delle proposte formulate dai partecipanti alla fast call for contribution, al fine di selezionare la proposta più efficace e idonea ad essere implementata in tempi rapidi a livello nazionale*”.
L’ufficializzazione è avvenuta il 16 aprile scorso: la app proposta dalla società milanese **Bending Spoons S.p.a.**, **“Immuni”** - che già dal nome è fuorviante, perché servirebbe al contrario a tracciare i contagiati e non gli immuni -, è stata “*ritenuta la più idonea per la sua capacità di contribuire tempestivamente all’azione di contrasto del virus, per la conformità al modello europeo delineato dal Consorzio PEPP-PT e per le garanzie che offre per il rispetto della privacy*”.
Quella di Bending Spoons, che guida una cordata di società con cui ha sviluppato l’app di tracciamento, è stata dunque la proposta scelta tra le oltre 300 pervenute che sono state vagliate dal gruppo dei 74 esperti del “comitato tecnico-scientifico” nominato dal ministero dell'innovazione, Paola Pisano. Tra le altre cose, proprio perché facente parte del ***Consorzio europeo PEPP-PT***.
Il 16 di aprile, con un’ordinanza firmata dal Commissario Straordinario per il coronavirus, **Domenico Arcuri** (a.d. di **Invitalia**), il governo ha dunque ufficializzato la sua scelta per lo sviluppo dell’app nazionale che diverrà “*un elemento importante all’interno di una strategia sostenibile post-emergenza e di ritorno alla normalità*” in grado “*di dare un contributo rilevante per un tracciamento di prossimità molto più efficiente e rapido di quello tradizionale*” [qui il testo: http://www.governo.it/sites/new.governo.it/files/CSCovid19_Ord_10-2020_txt.pdf].
Secondo il governo, l’app sarà essenziale durante la cosiddetta “Fase 2” dello stato di emergenza. Il commissario Arcuri, in tempi non sospetti aveva più volte ripetuto come l'app sarà "un pilastro importante nella gestione della fase successiva dell'emergenza".
Anche per il ministro della Salute, Roberto Speranza, la app Immuni “rafforzerà la sanità digitale”.
La società privata che ha sviluppato “Immuni”, la milanese Bending Spoons, ha stipulato il contratto con lo Stato italiano, cedendo a quest’ultimo in maniera gratuita la licenza d'uso dell’applicazione, mantenendo solo i diritti d’autore. Nel contratto citato dall’ordinanza del Commissario Arcuri è infatti scritto che“*Bending Spoons ha concesso la licenza d’uso aperta, gratuita, perpetua e irrevocabile del codice sorgente e di tutte le componenti dell’app “Immuni”, nonché si è impegnata, sempre gratuitamente e pro bono, a completare gli sviluppi software necessari per la messa in esercizio del sistema nazionale di contact tracing digitale, **per la durata di sei mesi** e comunque nel limite di 10.000 ore/uomo”*. Dunque Blending Spoons continuerà ad occupersi del “miglioramento” e della funzionalità dell’app Immuni almeno fino a fine anno 2020 (e poi chissà chi lo farà al suo posto). *https://www.key4biz.it/immuni-bending-spoons-mettera-mano-fino-alla-fine-dellanno-poi/303359/*
Da fonti governative è stato più volte detto che il download dell’app “Immuni” sul proprio cellulare sarà almeno per ora volontario ma che, per essere efficace, la dovranno scaricare in tanti.
Uno studio (https://science.sciencemag.org/content/368/6491/eabb6936.full) dei ricercatori di Oxford fatto proprio dal governo italiano, nel marzo 2020 parlava almeno del 60% degli abitanti, 6 persone ogni 10 (il modello del team del Big Data Institute dell'Università di Oxford, parla di una percentuale del 56% della popolazione inglese, cioè all'80% dei possessori di smartphone nel Regno Unito; nel modello, tra l’altro, gli anziani dovrebbero ancora autoisolarsi in massa). Dunque in Italia stiamo parlando di più di 35milioni di individui, praticamente lo stesso numero di utenti che ha oggi Facebook nel belpaese (pari appunto a 35 milioni di iscritti, secondo i dati Agcom del 20 gennaio 2020). Al di sotto di questa percentuale l’efficacia del tracciamento viene ritenuta insufficiente.
Trattandosi di uno strumento volontario (ripetiamo, per ora) e visto il fatto che in Italia non tutte le fasce di popolazione hanno dimestichezza con gli smartphone, è evidente che il problema principale per il governo sarà proprio quello di raggiungere questa soglia di adesione “volontaria”.

I dati a disposizione fin d'ora ci dicono, infatti, che l'utilizzo delle app di tracciamento hanno avuto una percentuale di diffusione compresa tra l'8% della regione Lombardia, dove l'app di tracciamento AllertaLom, è stata scaricata da 800 mila persone su una popolazione di 10 milioni di abitanti, e il 38% dell'Islanda, certamente uno dei dati più alti al mondo ma comunque una percentuale ben lontana da quel 60% che vuole ottenere il governo italiano.
In mezzo c'è il 18% circa di Singapore, paese più volte preso a modello dagli stati occidentali, ed anche dall'Italia, dove l'app è stata scaricata da un milione di abitanti ma poi attivata realmente dal 50% di coloro che l'hanno scaricata.
Sarà interessante capire quindi come il governo vorrà procedere per ottenere un simile traguardo. Una delle ipotesi è quella di elargire sgravi fiscali, premi economici o punti da spendere in negozi convenzionati (**Jakala**, una delle società con cui Bending Spoons ha sviluppato l'app Immuni, nel giugno 2019 ha comprato **Volponi**, un'azienda per la raccolta punti e premi nella grande distribuzione), ovvero misure che incentivino il download dell'applicazione con la conseguenza di rendere solo formale la sbandierata volontarietà.
Al tempo stesso, si è fatto intendere che se non saranno tante le persone che scaricheranno questa app, potrebbero continuare ad esserci in futuro ordinanze di chiusura e limitazioni degli spostamenti nelle zone a più alto rischio di contagio. Un bel ricatto, insomma! Non obbligatoria ma fortemente "consigliata". Alcuni esponenti del team di esperti tecnici del governo hanno, del resto, diffuso l'allarme che la volontarietà da sola non basti, quindi c'è il consistente rischio che per il futuro, se si dovesse assistere ad una risalita della curva dei contagiati dal virus, il governo possa anche decidere di rendere questa applicazione obbligatoria per legge (o...per DPCM).
Ma in cosa consiste, nella pratica, "Immuni"? Intanto la app si comporrà di due parti. La prima è il sistema di tracciamento vero e proprio per mappare i contatti tra smartphone e che funzionerà attraverso il Bluetooth (più specificatamente attraverso la tecnologia **Bluetooth Low Energy**, BLE).
La seconda funzione è un diario clinico contenente le informazioni più rilevanti della persona (sesso, età, malattie pregresse e passate, assunzione di farmaci) da aggiornare tutti i giorni con eventuali sintomi e cambiamenti sullo stato di salute. Stiamo parlando di una mole enorme di dati cosiddetti sensibili, insomma.
Oltre ai propri dati clinici, ritornando al sistema di tracciamento, la app - che come detto si avvale della tecnologia Bluetooth (vedremo in seguito per quale ragione si è optato per il Bluetooth e non per altre tecnologie come il WIFI o il GPS) - fornirà tre informazioni importanti: quali e quanti sono i cellulari con i quali il proprio dispositivo è entrato in contatto ravvicinato, a che distanza questo è avvenuto, per quanto tempo. La app permette quindi di ricostruire l'intera rete dei contatti tra smartphone. Una tecnologia simile a quelle sperimentate nei paesi asiatici.

Come funziona il tracciamento di Immuni

Il meccanismo di Immuni, in sostanza, funziona così:

- Lo smartphone scambierà via Bluetooth con altri cellulari con installata Immuni dei codici casuali (ID) che cambiano ogni quindici minuti circa. Ogni giorno l'app archivierà sul proprio cellulare la lista di questi codici, con informazioni sulla distanza e sul tempo del contatto (sembra da un minimo di cinque ad un massimo di 30 minuti).
- Quando uno dei soggetti che ha scaricato l'app risulta positivo al virus dopo aver effettuato un test o un tampone, gli operatori sanitari (in possesso di una app differente che genera codici) gli forniscono un altro codice di 16 cifre con il quale questi invierà su un server

statale i dati raccolti dalla sua app, ovvero la lista degli ID casuali dei cellulari con cui è stato vicino nei giorni precedenti (a un metro, per un numero sufficiente di secondi o minuti), così da consentire il loro "abbinamento" agli utenti che hanno scaricato l'app. Per evitare che le persone si dichiarino malate sull'app anche quando non lo sono effettivamente, prima che inizi il processo di invio, serve non solo la conferma dell'utente, ma anche quella di un medico curante o di un operatore sanitario.

- A questo punto c'è un "vaglio qualitativo" algoritmico dei contatti, per ridurre il rischio di falsi positivi. Cioè il server valuta per ogni identificativo la vicinanza fra i dispositivi mobili e il tempo di esposizione fra gli stessi e restituisce un valore di "rischio contagio" generando un elenco di persone da avvertire tramite una notifica (alert) su smartphone.
- Il server quindi invia una notifica (automatica) a tutti gli utenti di Immuni, cioè ai dispositivi di persone potenzialmente a rischio contagio, con un allerta di colore giallo che arriva tramite l'app. Si diventerà "gialli" sembra dopo 15 minuti di esposizione con "un rosso", cioè con un contagiato (la app, infatti, funziona come un semaforo: "verde" ok, "giallo" a rischio e "rosso" positivo, che non è una canzone di Tiziano Ferro).
- La notifica dovrebbe avere un messaggio preimpostato deciso dalle autorità sanitarie e chiede di seguire un protocollo (autoisolamento, quarantena, contattare numeri di emergenza per presa in carico ed eventuale tampone).

Se dunque una persona dovesse risultare positiva al test del virus questa stessa persona, tramite l'app e dopo la conferma dell'operatore sanitario, può caricare la lista dei contatti avuti sul server centrale e le persone che hanno avuto dei contatti riceveranno un allerta sul proprio cellulare.
Se è abbastanza evidente che chi ha effettuato un tampone ed è risultato positivo al virus sia già conosciuto dalle autorità sanitarie, cosa che agevola il compito di controllo dei tempi della quarantena domiciliare, non è invece ancora chiaro cosa si dovrà fare in caso di avvenuta notifica di rischio tramite l'app, se la quarantena sarà volontaria od imposta, a prescindere che si sia stati veramente contagiati o che ci sia la possibilità immediata di fare il tampone. Anche se, a dire il vero, è poco credibile che il sistema funzioni non sulla base dell'obbligo, che è da sempre il terreno dello Stato, ma attraverso il solo sistema dell'auto-quarantena volontaria. È molto probabile, infatti, che se la si violerà si rischierà una denuncia per attentato alla salute pubblica. Ma come eseguire i controlli se i dati sono davvero anonimi? Se si dovrà controllare l'effettivo svolgersi della quarantena, significa che lo Stato deve trovare un modo per risalire dai dati che ha in mano, che sono pseudonimi e non anonimi, fino alle persone reali in carne ed ossa. Riguardo all'archiviazione dei dati, per fare accettare questa tecnologia di sorveglianza si è fatta volontariamente una grande confusione, continuando col ripetere che l'app rispetterà un approccio decentralizzato, rispettoso della privacy e con un'archiviazione dei dati solamente sui cellulari degli interessati, mentre è invece vero che il governo ha sempre ribadito che si sarebbe affidato anche a server centralizzati "pubblici e italiani", come alla fine ha fatto. Eppure si continua a ripetere che gli unici dati che verranno trasmessi al Servizio Sanitario Nazionale sono solo quelli raccolti dalla app in forma aggregata, col conto del numero complessivo di notifiche che sono state inviate, senza alcun riferimento né alle persone che sono proprietarie dei telefonini, né al luogo dove vivono (altra piccola bugia, dato che per funzionare l'app richiede il cap della propria provincia di residenza).
Paolo de Rosa, responsabile tecnologico del dipartimento della ministra dell'Innovazione Paola Pisano, in una intervista ha ribadito che sul server *"vanno solo i codici identificativi dei soggetti infetti e i dati quantitativi sui contagiati, il resto è sui dispositivi"* nonché *"le prime due cifre del*

Cap, con il consenso dell'utente, per calcolare il livello di rischio su base regionale".
E l'integrazione con il sistema sanitario? *"Partiremo solo con il tracciamento, intanto il ministero della Salute e le Regioni stanno valutando di usare l'app per il monitoraggio dei sintomi dei contatti a rischio da parte delle singole Asl"*.
L'eventuale notifica all'ufficio di prevenzione della Asl viene descritta come una scelta discrezionale di chi riceverà una notifica da parte della App [https://www.corriere.it/tecnologia/20_maggio_09/app-immuni-de-rosa-pronti-fine-mese-sogei-garante-sicurezza-327c2c4a-91c6-11ea-9f60-1b8d14bed082.shtml?refresh_ce-cp].
Ma è scontato che da qualche parte si dovrà immancabilmente associare lo stato di salute della persona, l'eventuale positività al virus e un identificativo certo con cui risalire al possessore del cellulare, altrimenti l'app non servirebbe proprio a niente – e sappiamo bene quanto lo Stato abbia in orrore la possibilità che le persone prendano da sé le loro scelte!
Quindi, certo, è vero che la app conserverà sul dispositivo di ciascuna persona la lista dei contatti avuti solo attraverso codici identificativi casuali che cambiano nel tempo ogni 15 minuti, per cui sarà più arduo (ma non impossibile) per i possessori del cellulare entrare a conoscenza delle identità reali delle altre persone. Ma per chi gestirà il server statale è tutto un altro discorso: questi codici identificativi casuali o aggregati sono cosa ben diversa dai dati anonimi, perché avendo accesso alla banca-dati probabilmente si potrà avere la possibilità di risalire a quale cellulare sono stati inviati, andando a vedere a ritroso nel tempo in che giorno, in che minuto e a quale cellulare un determinato codice casuale sia stato inviato, ed ecco che il gioco è fatto. Si potrà chiedere direttamente alle varie compagnie telefoniche, non sembra poi così difficile. Magari per iniziare lasceranno pure che le persone si mettano in auto-quarantena da sole, ma chi ci assicura che poi, una volta accettata questa tecnologia di sorveglianza, la quarantena non diventi mano a mano obbligatoria per tutte le persone che hanno ricevuto una segnalazione di rischio (che non equivale certo ad una diagnosi medica di avvenuto contagio!)?
L'anonimato totale è una pura invenzione giornalistica, dato che questi codici non sono anonimi né per chi gestisce il server statale né per chi gestisce i sistemi operativi dei dispositivi mobili, ma eventualmente solo per i possessori degli smartphone. Dal momento in cui la si scaricherà sul cellulare, le società pubbliche e private che gestiranno il funzionamento dell'app avranno accesso ai nostri dati, checché ne si dica, tenendo inoltre presente che la scansione potrebbe funzionare anche con l'app in background (cioè senza essere stata aperta sullo smartphone).
Per quanto tempo verranno conservati sui server i dati? Si è affermato che al termine dell'emergenza (indicata approssimatamente nella fine dell'anno in corso, anche se il primo DPCM la estendeva solo fino a luglio) tutti i dati dovrebbero venire cancellati ma naturalmente nessuno ce lo assicura. Nessuno ci ha detto qual'è la durata di vita di questa applicazione prima del suo "spegnimento", semmai davvero ci sarà.
Anche il fatto che saranno impiegati server centrali statali e non in mano ai privati non ci deve rassicurare. Lo Stato entrerà in possesso dei dati di milioni di persone (almeno nelle intenzioni) che incrocerà con gli altri già in suo possesso. E non è detto poi che la società privata Blending Spoons, che l'anno scorso ha fatto segnare oltre 90 milioni di fatturato, e che continuerà ad effettuare la manutenzione ordinaria della app per almeno 6 mesi dal lancio, accedendo in qualche modo al server non possa riuscire ad avere accesso ai dati personali e poi venderli per fini commerciali. Tanto più che nell'assetto societario della società milanese figurano molti nomi noti del capitalismo nazionale (e non solo).
Ma l'incognita più grande è quella dei sistemi operativi dei cellulari, iOS e Android, che notoriamente sono di proprietà di Apple e Google. Le due società americane hanno in pratica il

monopolio dei sistemi operativi per smartphone. Per quanto riguarda i tempi del rilascio dell'app "Immuni", i ritardi sulla tabella di marcia inizialmente prevista dal governo, che contava di renderla operativa già da inizio maggio, sono dipesi infatti soprattutto da aspetti tecnici collegabili all'entrata in campo delle due società americane. Immuni, infatti, come altre applicazioni simili introdotte in varie nazioni, si interfaccerà con i sistemi operativi di Apple e Google per funzionare al meglio, con le due multinazionali che hanno appositamente rilasciato degli aggiornamenti software (si chiamano API) per rendere i loro sistemi operativi interoperabili e per gestire i dati raccolti da Immuni e dalle altre app di tracciamento che hanno scelto di collaborare con loro. In questo modo i sistemi operativi dei due colossi hi-tech avranno totale accesso ai dati forniti col tracciamento.
Nel mentre si attendeva che Google e Apple rendessero disponibili per i loro sistemi operativi Android e IOS le tecnologie su cui "Immuni" e le altre app devono interfacciarsi, il progetto iniziale della cordata guidata da Bending Spoons ha subito, soprattutto per questa ragione, aggiustamenti in corso d'opera. La prima a lasciare la cordata è stata **Geouniq**, specializzata nella **geolocalizzazione** e quindi non più necessaria, dal momento che si è sempre detto che sarebbe stato escluso il ricorso al GPS. La presenza del **Centro medico Santagostino**, poi, è stata ridimensionata dall'entrata ufficiale del ministero della Salute, investito dal governo del ruolo di titolare del trattamento dei dati. Infine, ridimensionato appare anche il ruolo dell'azienda tedesca **Arago**, fondata da Chris Boos, imprenditore e padre padrone del consorzio europeo **Pepp-Pt**, di cui pure Bending Spoons faceva parte. Sulla fine della collaborazione con Arago, l'amministratore delegato di Bending Spoons, Luca Ferrari, ha chiarito in questo modo: "*Contattammo Hans-Christian Boos di Arago e Pepp-Pt durante la seconda metà di marzo. Stavamo studiando le idee per il tracciamento di prossimità che stavano emergendo a livello internazionale e Pepp-Pt ci sembrò molto valida. Decidemmo quindi di unirci al consorzio, che peraltro aveva già coinvolto diverse società e istituti di ricerca prestigiosi*", cosa che "*si è rivelata utile e che ha permesso a noi come agli altri partecipanti di sviluppare una comprensione più sofisticata del problema e delle possibili soluzioni*", dato che "n*on abbiamo mai lavorato in questo campo specifico in precedenza*".
Arago avrebbe dovuto fornire "*una componente che gestiva la comunicazione bluetooth sui dispositivi Android*". Ma la collaborazione è terminata, chiarisce Ferrari, "*non appena il governo ha deciso di integrare in Immuni le nuove tecnologie per il tracciamento di prossimità annunciate da Apple e Google (…) Come è risaputo, le suddette nuove tecnologie sono incompatibili con gli standard Pepp-Pt, che erano stati pensati quando queste non esistevano ancora e non ne avevano quindi potuto tenere conto e trarre vantaggio. Ne consegue che adottarle ci ha richiesto di riscrivere le parti di codice che seguivano gli standard del consorzio, del quale a quel punto non aveva ovviamente più senso far parte" [*https://www.wired.it/internet/web/2020/05/09/contact-tracing-app-immuni-copasir/?refresh_ce].
Immuni è dunque passata dal modello di Pepp-PT al modello di Google e Apple.
Un'altra causa del ritardo del lancio di Immuni può essere il fatto che alcune forze politiche avevano chiesto che l'app fosse introdotta solo previo il varo di una legge apposita votata in parlamento. A tal proposito, il Governo il 21 aprile ha confermato di non voler seguire la strada del decreto da parte del presidente del consiglio (DPCM) mentre mercoledì 29 aprile 2020 il Consiglio dei Ministri, su proposta del Presidente Giuseppe Conte e del Ministro della giustizia Alfonso Bonafede, ha approvato un decreto legge che tra le altre cose prevede espressamente che sia il Ministero della salute a gestire i dati della piattaforma per il tracciamento dei contatti (***Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile, e disposizioni***

urgenti in materia di tutela dei dati personali nel tracciamento dei contatti con soggetti affetti da COVID-19) (qui il *testo del decreto-legge*).
Il presidente del consiglio, Giuseppe Conte, nell'occasione ha dichiarato: *"Il Governo, all'esito del Consiglio dei Ministri, ha adottato un decreto-legge che, tra le altre cose, contiene anche una norma quindi una copertura normativa di rango primario alle procedure di tracciamento dei contatti con funzioni di monitoraggio del virus. Il corpus di disposizioni, su cui poi il Parlamento potrà intervenire in sede di conversione in legge del decreto ha lo scopo di chiarire e rafforzare la disciplina di questo particolare trattamento dei dati personali, in coerenza con quanto ha precisato il Comitato europeo per la protezione dei dati personali e recependo le raccomandazioni emanate dalla Commissione europea il 16 aprile 2020"*
Nel testo del decreto del 29 aprile troviamo in più punti scritto chiaramente, come volevasi dimostrare, che i dati non saranno affatto anonimi ma solamente pseudonomizzati e dunque soggetti a reidentificazione: *"gli utenti ricevano, prima dell'attivazione dell'applicazione, informazioni chiare e trasparenti al fine di raggiungere una piena consapevolezza, in particolare, sulle finalità e sulle operazioni di trattamento, sulle tecniche di pseudonimizzazione utilizzate e sui tempi di conservazione dei dati"*. Si legge anche che i dati, come sapevamo, saranno conservati *"anche nei dispositivi mobili degli utenti, per il periodo strettamente necessario al trattamento, la cui durata è stabilita dal Ministero della salute. I dati sono cancellati in modo automatico alla scadenza del termine"* fissata al termine dello stato di emergenza disposto con delibera del Consiglio dei Ministri del 31 gennaio 2020 "e comunque non oltre il 31 dicembre 2020, ed entro la medesima data tutti i dati personali trattati siano cancellati o resi definitivamente anonimi".
Si prevede, infine, che *"il mancato utilizzo dell'applicazione non comporti alcuna limitazione o conseguenza in ordine all'esercizio dei diritti fondamentali dei soggetti interessati"* [http://www.governo.it/node/14548]·
Dunque il trattamento dei dati raccolti dall'app Immuni sarà responsabilità del ministero della Salute mentre gli stessi dati saranno "ufficialmente" cancellati entro fine anno, con la possibilità di disinstallare l'app Immuni anche prima di questo limite temporale, almeno se si vuol credere alle affermazione del ministro dell'Innovazione, Paola Pisano, durante l'audizione in videoconferenza alla commissione Affari costituzionali della Camera [http://www.rainews.it/dl/rainews/articoli/pisano-app-immuni-tutti-dati-cancellati-entro-dicembre-ministro-salute-responsabile-trattamento-1b1cc4fb-c042-46a6-8737-6d142d0be807.html].
Abbiamo scritto "ufficialmente", tra virgolette, perché oltretutto esiste da tempo una norma sul riuso a scopo statistico o di ricerca scientifica che prevede che i dati possano essere riutilizzati "in aggregato o in modo anonimo" anche per finalità diverse da quelle per cui erano stati raccolti: la prima opzione ("in aggregato") prevede un trattamento (su dati sanitari, poi) che non è affatto anonimo, essendo il trattamento in aggregato una modalità che può comportare la reidentificazione. I dati aggregati, tra l'altro, sono da sempre quelli più ambiti dalle società di marketing aziendale. Questo riutilizzo dei dati per fini statistici e di ricerca (ma sarebbe più onesto dire di mercato) fanno decadere il fittizio termine di cancellazione automatica dei dati a dicembre 2020.
A questo punto, rimane da sapere quale sarà il server statale su cui verranno archiviati tutti i dati raccolti dall'app Immuni e su cui il Ministero della Salute dovrà vigilare. Nella relazione del gruppo di lavoro del ministro dell'Innovazione, qualche tempo fa si leggeva che *Bending Spoons* aveva proposto inizialmente *"l'utilizzo della piattaforma Google Cloud Platform per la parte del server del progetto"* ma il ministro, durante l'audizione alla Camera, ha chiarito che *"i dati raccolti da Immuni saranno conservati in parte sul telefonino degli utenti e in parte all'interno di un server italiano della pubblica amministrazione gestito da* ***Sogei****, mentre* ***PagoPa*** *avrà il ruolo di sviluppo*

dell'app e del coordinamento tecnologico insieme al nostro dipartimento per la trasformazione digitale". Sogei e PagoPa, due società a partecipazione statale; in dettaglio le vedremo più tardi. Intanto va detto che si occuperanno della verifica del codice dell'app, della definizione dei requisiti tecnici e dei test di sicurezza.
Sempre il ministero dell'Innovazione ha pubblicato da ultimo, verso la fine di maggio, i documenti sul funzionamento del software dell'app e i codici sorgenti su Github, la piattaforma dove i nerd e gli sviluppatori da ogni parte del mondo si confrontano su progetti specifici.
Su Github è quindi diventato accessibile un link chiamato "immuni-documentation" [https://github.com/immuni-app/immuni-documentation], un link "Immuni ci-scheduler" [https://github.com/immuni-app/immuni-ci-scheduler] e poi un link chiamato immuni app-android e un link immuni app-ios.
A seguito della pubblicazione della documentazione e dei codici, Bending Spoons ha tenuto a precisare che è arrivato anche il gradimento del Massachusetts Institute of Technology (Mit) di Boston che "ha promosso Immuni a pieni voti, assegnandole 5 stelle su 5". Il riferimento è all'analisi del Mit, che ha lanciato il programma 'Covid Tracing Tracker' per fornire una mappa completa delle app per il contact tracing scelte dai vari Paesi. Non proprio una sorpresa questa assegnazione a 5 stelle, se si prende in considerazione che molte delle componentistiche di Immuni si basano proprio su strumenti tecnologici sviluppati sotto licenza del Mit. http://www.rainews.it/dl/rainews/articoli/coronavirus-app-immuni-su-github-la-documentazione-completa-1363fe30-0943-4dee-bc28-cdb8768a6a80.html?refresh_ce
Dopo le "traversie" che abbiamo descritto, Paolo de Rosa, responsabile tecnologico del dipartimento della ministra dell'Innovazione Paola Pisano ed anche uno dei tre coordinatori della task force che ha scelto Immuni, in un'intervista ha affermato che: *"Apple e Google dovrebbero essere pronte il 15 maggio. Da quella data inizieranno i test sul campo, che dureranno le due settimane necessarie, anche perché il 70-80% delle persone deve aggiornare i sistemi operativi. L'obiettivo è di arrivare entro fine maggio con la app disponibile per tutti"*. *https://www.corriere.it/tecnologia/20_maggio_09/app-immuni-de-rosa-pronti-fine-mese-sogei-garante-sicurezza-327c2c4a-91c6-11ea-9f60-1b8d14bed082.shtml?refresh_ce-cp*
Ma in realtà Immuni è stata resa disponibile sugli Store iOs e Android solamente a partire dal 1 giugno, e dal 5 giugno la app dovrebbe essere scaricabile sui telefonini in tre regioni pilota — Abruzzo, Liguria e Puglia — per una sperimentazione che durerà una settimana, al termine della quale sarà estesa al resto d'Italia https://www.nextquotidiano.it/immuni-5-giugno-tracciamento-in-liguria-puglia-e-abruzzo/. Giugno sarà dunque il mese decisivo.
C'è solo un ultimo, irrisorio ostacolo da superare: il regolamento europeo impone che il Garante per la privacy vagli e autorizzi la cosiddetta DPIA (Data Protection Impact Assessment, in italiano Valutazione di Impatto sulla protezione dei dati personali) prodotta dal titolare del trattamento dei dati, cioè dal ministero della Salute. Una formalità burocratica, insomma, che secondo alcuni avvocati non sarebbe nemmeno così obbligatoria, se non fosse che stiamo parlando di un documento che dovrebbe garantire la riservatezza e la protezione dei dati e delle informazioni sanitarie.
Inizialmente era anche girata la voce che l'app potesse essere stata avviata in modalità sperimentale all'interno degli stabilimenti di Maranello della **Ferrari**, dove sono impiegate circa 4.000 persone, prima di essere diffusa pubblicamente, tramite un accordo tra Ferrari, un pool di virologi ed esperti del settore e con il patrocinio della Regione Emilia Romagna nell'ambito del progetto *Back on Track ("Torna in pista")* che ha come obiettivo ufficiale la "sicurezza dell'ambiente di lavoro" al riavvio delle attività produttive. Ma poi fonti del governo, dei sindacati e della stessa Ferrari hanno

negato di stare impiegando Immuni. O meglio, come ha spiegato in un'intervista Giorgio Uriti, segretario Fim Cisl per l'Emilia centrale, a Maranello "*se ne stanno* valutando tre, *tra cui quella nazionale*", che se non andiamo errati è proprio Immuni (https://www.wired.it/internet/web/2020/05/07/contact-tracing-ferrari-immuni). Qualunque sia la scelta di Ferrari, l'uso di un'applicazione di tracciamento è tuttavia prevista proprio dal **protocollo** *Back on track* sottoscritto con i sindacati Cgil, Cisl e Uil, con l'obiettivo di mettere a disposizione di Regione Emilia-Romagna ed aziende l'esperienza maturata, evidentemente con l'intenzione di introdurre app simili sui luoghi di lavoro (https://www.wired.it/economia/lavoro/2020/04/30/ferrari-fase-2-coronavirus).
Non a caso, già da aprile la stampa aveva reso noto come Bending Spoons si fosse avvalsa nello sviluppo della sua app anche della supervisione tecnica, tra gli altri, di John Elkann, presidente di **FCA**, la vecchia Fiat, proprietaria di Ferrari (https://www.quattroruote.it/news/industria-finanza/2020/04/17/coronavirus_arriva_l_app_immuni_ferrari_in_prima_linea.html)
e (https://www.economyup.it/automotive/ferrari-contro-il-coronavirus-il-test-dellapp-immuni-e-non-solo/).
Intanto il Sindaco di Milano, Giuseppe Sala (che si è dichiarato non solo estimatore ma anche amico di Colao) aveva già proposto la sua città come "area test" per la ripartenza e la sperimentazione della fantomatica "Fase 2".
Ad inizio giugno, quindi, non solo Immuni è stata resa disponibile per lo scaricamento dagli Store di Apple (iOS) e Google (Android) ma la sua sperimentazione è partita in diverse regioni d'Italia.
Il governo, per fare accettare l'app di tracciamento, pensa ad una campagna di comunicazione di massa sia sui canali standard che sui social network, *"per far cambiare abitudini"* agli individui, secondo la ricetta del ministro per l'Innovazione tecnologica, Paola Pisano.
Secondo alcuni sondaggi, fino a 23 milioni di abitanti italiani sarebbero disponibili a scaricare l'applicazione. Ma dopo tre settimane dal pubblico lancio, Immuni era stata scaricata "solo" da 3 milioni e mezzo di persone, circa il 5% della popolazione dell'Italia (https://www.affaritaliani.it/cronache/app-immuni-e-flop-scaricata-da-solo-3-5-milioni-persone-5-degli-italiani-680398.html).

"FASE 2"

Con i contagi in diminuzione e la crescente pressione di Confindustria, Confagricoltura, Confesercenti ed altre categorie padronali desiderose di riprendere a "far girare l'economia", "riaprire le fabbriche" e "far ripartire la produzione" (dato che le previsioni del Fmi stimano una caduta del 9,1% del Pil italiano), dal Governo sono incominciate a trapelare voci sulle misure per quella che è stata definita la "Fase 2" dell'emergenza, incominciata ufficialmente il 4 maggio con una serie di riaperture mirate, quando cioè fabbriche (a dire il vero mai state chiuse), negozi, bar e ristoranti hanno potuto riaprire rispettando alcune disposizioni.
Milioni di persone sono così ritornate al lavoro. Cantieri edili e manifatturiero sono le produzioni riaperte per prime, perché incredibilmente quelle con l'indice di rischio contagio più basso nelle tabelle presentate dall'Inail (stiamo parlando di circa 4 milioni di lavoratori!). Ma circa 100 mila aziende hanno riaperto anche prima, dopo aver ottenuto deroghe dai prefetti attraverso le autocertificazioni.
Altri milioni di abitanti, invece, molto più fortunati di chi è uscito dal confinamento domestico solo

per tornare al lavoro, sono andati in vacanza. Il governo ha voluto garantire la possibilità di far andare in vacanza gli italiani questa estate, perché c'è bisogno che spendano. Lo chiedono gli imprenditori e i commercianti! Ecco allora che dal governo qualche mente brillante se n'è uscita con l'idea di un "bonus vacanze" e di un "bonus bicicletta" per incentivare gli acquisti e soprattutto far ripartire il settore del turismo, in crisi a causa dell'emergenza Coronavirus.
Il problema è come andarci in vacanza, con la difficoltà di evitare gli assembramenti in spiaggia! Dunque, ingressi scaglionati negli stabilimenti balneari, prenotazioni, chiusura totale o parziale delle spiagge libere, controlli con steward e personale appositamente addestrato e distanziamenti tra gli ombrelloni. É stata fatta anche l'assurda proposta di separare sdrai e ombrelloni tramite barriere in plexiglass, poi abbandonata per palese idiozia (https://www.fanpage.it/politica/come-sara-la-fase-2-del-coronavirus-cosa-succede-dal-4-maggio-per-negozi-bar-uffici-e-vacanze).
Riaperte lo sono state anche le aree verdi e i parchi ma gli "assembramenti" rimangono proibiti.
La fiducia del governo viene riposta nella risposta della popolazione a queste nuove disposizioni, dato che anche in presenza di queste riaperture rimarranno stringenti le misure anti-contagio, a cominciare dal famoso "metro di distanza" per evitare assembramenti nei locali, nei negozi ma anche all'aperto. La "fila" diventa la normale modalità di accesso a prestazioni pubbliche ed esercizi commerciali, e così sarà probabilmente per molti mesi a venire, mentre i lavoratori che hanno contatti con il pubblico, ma anche gli avventori, dovranno continuare a indossare mascherine. Uffici, negozi e bar con divisori, termoscanner per entrare o per spostarsi con i mezzi pubblici, niente più riunioni lavorative "reali" ma solo on-line ed agevolazione del tele-lavoro e delle video-chat. Ecco la fantomatica "Fase 2"!
Anche se a metà aprile era incominciata a circolare la notizia che il governo italiano intendesse sostituire l'autocertificazione cartacea per gli spostamenti con una digitale, attraverso un'apposita app, la realtà è che a partire dal 3 giugno anche l'autocertificazione cartacea è stata abolita.
Ci si sposterà, quindi, senza alcuna limitazione, ed anche gli ultimi spostamenti vietati, quelli tra Regioni, sono stati alla fine consentiti.
Ad escogitare tutte queste misure per il rilancio economico nel 2020-2021 è stato il cosiddetto "comitato di esperti in materia economica e sociale", la "task force" assunta dal Governo Conte guidata dal manager **Vittorio Colao**.
Per 10 anni a capo della seconda compagnia telefonica più grossa al mondo, cioè **Vodafone**, Vittorio Colao, laureato alla Bocconi, Cavaliere del Lavoro dal 2014, top-manager aziendale, nel 1999 era stato amministratore delegato della divisione italiana di Vodafone, tra il 2001 e il 2004 amministratore delegato di Vodafone per Europa meridionale, Medio Oriente e Africa, nel 2004 ha lasciato Vodafone per diventare amministratore delegato di Rcs MediaGroup, ma nel 2006 è tornato nella stessa società con il ruolo di vice amministratore delegato per l'Europa, mantenendo la carica per due anni, per poi diventare amministratore delegato del gruppo. Colao ha lasciato la carica di amministratore delegato di Vodafone nel 2018 ma è rimasto a vivere a Londra con la famiglia. Attualmente è "senior advisor" del fondo americano General Atlantic. Colao è un sostenitore accanito dello smart working, che ha largamente introdotto a Londra in Vodafone.
Il Decreto del Presidente del Consiglio dei Ministri così recita: "*Art. 1 (Comitato di esperti) 1. Presso la Presidenza del Consiglio dei Ministri è istituito un Comitato di esperti in materia economica e sociale con il compito di elaborare e proporre al Presidente del Consiglio misure necessarie per fronteggiare l'emergenza epidemiologica Covid-19, nonché per la ripresa graduale nei diversi settori delle attività sociali, economiche e produttive, anche attraverso l'individuazione di nuovi modelli organizzativi e relazionali, che tengano conto delle esigenze di contenimento e prevenzione dell'emergenza. 2. Il Comitato opera in coordinamento con il Comitato Tecnico Scientifico di cui all'articolo 2, comma 1, dell'ordinanza del Capo Dipartimento della Protezione Civile n. 630 del 3 febbraio 2020*".
Un "*Comitato di esperti in materia economica e sociale*" quello di Colao, assunto dal Capo Dipartimento della Protezione Civile, Angelo Borrelli, con competenze principalmente economiche, imprenditoriali e di "organizzazione del lavoro" (leggasi sfruttamento) piuttosto che mediche, che detterà l'agenda al governo per tutto ciò che riguarda il prossimo futuro delle nostre vite.

Dei 17 componenti del nuovo organo consultivo (al netto del commissario straordinario Arcuri e di Borrelli, “membri di diritto”) metà sono esperti di materie afferenti all’economia.
Un vero e proprio “governo tecnico” dell’emergenza. Ecco da chi è composto:
Roberto Cingolani, fisico, responsabile per l’innovazione tecnologica per il gruppo di aerospazio, difesa e sicurezza di Leonardo (ex Finmeccanica). E’ stato il primo direttore scientifico dell’Istituto italiano di tecnologia (Iit) di Genova, che ha guidato dal 2005 al 2019. Nel 2016 ha lavorato alla nascita dello Human Technopole di Milano, il progetto per una cittadella di Scienza della vita.
Riccardo Cristadoro è il senior director del Dipartimento di economia e statistica della Banca d’Italia e consigliere economico del presidente del Consiglio. Tra il 2012 e il 2017 è stato responsabile della divisione Mercati emergenti e Commercio mondiale. I suoi interessi di ricerca includono l’econometria applicata, l’economia digitale e l’economia internazionale.
Giuseppe Falco è amministratore delegato per il Sistema Italia-Grecia-Turchiasenior e partner e managing director del Boston Consulting Group. È inoltre membro delle practice Energy e Industrial Goods a livello globale. Si occupa di digital trasformation per importanti realtà aziendali.
Franco Focareta, molisano, avvocato, è docente di Diritto del lavoro all’Università di Bologna «Alma Mater Studiorum». E’ un esperto di diritto sindacale e diritto della previdenza, che ha insegnato negli ultimi anni nell’ateneo bolognese.
Enrico Giovannini, professore di Statistica economica all’Università di Roma «Tor Vergata», è stato capo-statistica dell’Ocse dal 2001 all’agosto 2009, poi presidente dell’Istat dall’agosto 2009 all’aprile 2013. A fine aprile 2013 fino al 22 febbraio 2014, Enrico Letta lo ha chiamato come ministro del lavoro e delle politiche sociali.
Giovanni Gorno Tempini, vecchio amico di Colao, è il presidente di Cassa Depositi e Prestiti, di cui è stato in passato anche amministratore delegato. L’elenco degli incarichi che ricopre attualmente è lungo: è presidente di Fila da agosto 2019. Fa parte del consiglio di amministrazione di Intesa SanPaolo, Avio, Willis Tower Watson e della Fondazione Airc per la Ricerca sul cancro. È advisor per l’Italia del fondo di private equity Permira e della Società di consulenza partners. Dal giugno 2017 è nella Giunta di Assonime. Inoltre insegna alla Bocconi di Milano e alla Cà Foscari di Venezia.
Mariana Mazzucato, è un’economista romana, cresciuta negli Stati Uniti, con doppio passaporto. Attualmente è la direttrice e fondatrice dell’Institute for Innovation and Public Purpose presso l’University College London. Giuseppe Conte l’ha chiamata come consigliera economica. Propugnattrice di tecnologia e competitività, fa parte del Consiglio per il Futuro della crescita e della competitività del World Economic Forum di Davos, al quale partecipa abitualmente.
Enrico Moretti, laureato alla Bocconi ed ora professore di Economia all’università di Berkeley, in California. Il suo libro «La nuova geografia del lavoro», sulle trasformazioni del mercato del lavoro statunitense, è stato tradotto in 7 lingue.
Riccardo Ranalli, piemontese, dottore commercialista e revisore contabile dell’omonimo studio con uffici a Torino e a Milano, è uno dei massimi esperti in ambito aziendalistico nella materia della «crisi di impresa». Ranalli è stato anche docente del Corso della Scuola Superiore della Magistratura presso la Corte di Cassazione, apri pista per le strutture territoriali della formazione decentrata.
Marino Regini, professore emerito di Sociologia economica all’Università Statale di Milano, dove insegna corsi di sociologia economica e di political economy. Ha svolto numerose ricerche sui temi delle relazioni industriali, dei sistemi di istruzione superiore e del mercato del lavoro, e più in generale dei rapporti fra le istituzioni sociali e politiche e il sistema economico. E’ stato direttore di «Stato e Mercato» e fa attualmente parte del comitato editoriale di questa rivista.
Raffaella Sadun è docente di Business Administration alla Business School di Harvard. La sua ricerca si concentra sull’economia della produttività, del management e del cambiamento organizzativo.
Stefano Simontacchi, bocconiano, avvocato, è presidente dello studio legale Bonelli Erede, dove coordina, tra l’altro, il gruppo di lavoro che si occupa di fiscalità internazionale, prezzi di trasferimento e corporate governance. Siede nei consigli di Rcs MediaGroup, Prada, ISPI, Cordusio

Sim, Fattorie Osella e Assoeilizia e Isituto Leone XIII. All'attività legale, Simontacchi affianca l'insegnamento: dal 2000 al 2019 è stato docente dell'Advanced LL.M. in International Taxation dell'Università di Leiden in Olanda e nel 2011 è stato nominato direttore del Transfer Pricing Research Center Leiden. E' inoltre presidente della Fondazione Buzzi.
Oltre a questi, tutti eminenti ricercatori, esperti e manager nel campo economico-aziendale, ci sono poi: **Fabrizio Starace,** direttore del Dipartimento di salute mentale e dipendenze Patologiche dell'Ausl di Modena e presidente della Società italiana di epidemiologia psichiatrica; **Elisabetta Camussi,** professoressa di Psicologia sociale all'Università degli Studi di Milano «Bicocca»; **Giampiero Griffo** coordinatore del Comitato tecnico-scientifico dell'Osservatorio nazionale sulla condizione delle persone con disabilità; **Filomena Maggino** è professoressa di Statistica sociale all'Università di Roma «La Sapienza». Dirige il Social Indicators Research journal (Springer) oltre ad essere presidente e cofondatrice dell'Associazione Italiana per gli Studi sulla Qualità della Vita (Aiquav) (https://www.corriere.it/economia/lavoro/20_aprile_12/ecco-squadra-colao-far-ripartire-paese-fase-2-9ad74558-7c8c-11ea-9e96-ac81f1df708a.shtml).
Fino a qui le misure attuate nel periodo della discesa del contagio. Ma se l'epidemia dovesse ripartire? Quel che è certo è che parte del piano per la "Fase 2" del comitato di esperti e del governo risiede proprio nell'app di tracciamento dei contatti, ovvero Immuni, l'app lanciata a partire dal 1 giugno. Colao non ha dubbi, in caso di un nuovo aumento dei contagi seguito alle riaperture: *"l'approccio non dovrà essere nazionale e neppure regionale, ma microgeografico: occorre intervenire il più in fretta possibile, nella zona più piccola possibile (…). Gli italiani devono abituarsi a convivere con il problema. Molte imprese si stanno attrezzando per inserire i test nelle loro procedure di sicurezza interne (…), a livello individuale abbiamo l'App, a livello di grandi numeri lo screening"*. Secondo Colao l'app sarà efficace *"se la scarica la grande maggioranza degli italiani (…), se quest'estate l'avremo tutti o quasi, bene; altrimenti servirà a poco"* (https://www.corriere.it/politica/20_aprile_29/coronavirus-colao-un-apertura-ondate-testare-sistema-l-app-entro-maggio-oppure-servira-poco-731741c6-8993-11ea-8073-abbb9eae2ee6.shtml).
Resta sempre aperta la possibilità, infatti, che in caso di necessità *"aree più o meno vaste del Paese possano tornare indietro"*. Lockdown locali, insomma, che potrebbero essere decisi in tre casi: un nuovo picco di contagi, la mancanza di posti letto negli ospedali Covid o nelle terapie intensive, la scarsità di dispositivi di protezione personali come le mascherine. Lo si evince da un documento della task force guidata da Colao consegnato a fine aprile al presidente del Consiglio, Giuseppe Conte, in cui si trovano appunto le linee guida per la "Fase 2". Il documento sottolinea come uno dei problemi per la "Fase 2", specie nelle grandi città, sia quello dei trasporti pubblici. Da qui l'idea di scaglionare quanto più possibile gli orari di ingresso e di uscita dai luoghi di lavoro e, in prospettiva, anche delle scuole e delle università. Inoltre si invita a sospendere le limitazioni al traffico e le ztl all'interno delle grandi città (https://www.corriere.it/politica/20_aprile_22/coronavirus-fase-2-ecco-l-agenda-graduale-colao-blocchi-locali-se-ritorna-l-allarme-8091983a-845a-11ea-8d8e-1dff96ef3536.shtml).
Sempre riferendoci alla "Fase 2", si è infatti ipotizzato che l'app di tracciamento possa prima o poi trovare un uso nella gestione del flusso di persone sui mezzi pubblici.
E Immuni potrebbe essere introdotta, non troppo a sorpresa, anche per la ripresa dell'attività calcistica (e di altri sport) in modo da monitorare il contagio tra gli sportivi (https://www.tuttosport.com/news/calcio/2020/04/18-68955383/lapp_immuni_sar_utile_ai_giocatori_ecco_perch/).

Dati tecnici e analisi della documentazione fornita da Immuni

il 14 maggio 2020 su GitHub, come detto, è stato pubblicato il repository per l'app Immuni, ovvero la documentazione dettagliata, con l'architettura dell'applicazione.

Potete trovarla qui:
https://github.com/immuni-app/documentation
https://github.com/immuni-app/documentation/blob/master/Technology%20Description.md

Riassumendo:

Immuni sarà un software open source con licenza GNU Affero General Public License versione 3.

L'app Immuni per iOS sarà disponibile per i dispositivi che hanno il sistema operativo iOS 13, con aggiornamento 13.5 per il funzionamento delle Api di Apple e Google.
Ad oggi, Apple non ha annunciato l'intenzione di rilasciarla per le versioni precedenti di iOS.
Ogni comunicazione con il server viene stabilita tramite HTTPS.
L'app è stata scritta usando Swift 5.2 e XCode 11.5.

L'app Immuni per Android sarà disponibile per dispositivi con Android 6 (Marshmallow, API 23) o versioni successive. Affinché A / G Framework funzioni, l'utente deve aver aggiornato Google Play Services alla versione 20.18.13 o successiva. Pertanto, l'app Immuni per Android non funzionerà se il cellulare non dispone di una versione sufficientemente recente di Google Play Services.
Ogni comunicazione con il server viene stabilita tramite HTTPS.
L'app per Android è stata scritta usando Kotlin 1.3 e Android Studio 3.6.

Innanzitutto, la persona deve accettare l'informativa sulla privacy e i termini di servizio e confermare di avere almeno 14 anni se desidera utilizzare l'app.
Anche l'A / G Framework (cioè le Api di Apple e Google) richiede l'autorizzazione dell'utente prima di poter essere utilizzato.
Sulla documentazione, si può leggere che *"Immuni è una soluzione tecnologica incentrata su un'app per smartphone iOS e Android. (…) Quando due utenti si avvicinano sufficientemente l'uno all'altro per un tempo sufficiente, i loro dispositivi registrano reciprocamente l'identificatore di prossimità a rotazione nella loro memoria locale. Questi identificatori sono generati da chiavi di esposizione temporanee e cambiano più volte all'ora. Queste chiavi vengono generate casualmente e cambiano una volta al giorno. Quando un utente risulta positivo per SARS-CoV-2, il virus che causa COVID-19, ha la possibilità di caricare su un server le sue chiavi di esposizione temporanea recenti. Questa operazione può avvenire solo con la convalida di un operatore sanitario. L'app scarica periodicamente le nuove chiavi di esposizione temporanea e le utilizza per ricavare gli identificativi di prossimità a rotazione degli utenti infetti per il passato recente. Quindi li confronta con quelli memorizzati nella memoria del dispositivo e avvisa l'utente se si è verificato un contatto rischioso"*.
Un po' più sotto, è scritto che *"per essere sicuri che solo gli utenti che sono effettivamente risultati positivi carichino le proprie chiavi sul server, la procedura di caricamento può essere eseguita solo con la collaborazione di un operatore sanitario autenticato. L'operatore chiede all'utente di fornire un codice generato dall'app e lo inserisce in uno strumento di back-office. Il caricamento può avere esito positivo solo se il codice utilizzato dall'app per autenticare i dati corrisponde a quello inserito nel sistema dall'operatore sanitario"*.
Riguardo alla piattaforma di Apple e Google (le famose API) si dice che *"(…) Per implementare la sua funzionalità di tracciamento dei contatti, Immuni sfrutta il framework di notifica*

dell'esposizione di Apple e Google (consultare la documentazione di Apple e la documentazione di Google). Ciò consente a Immuni di superare alcune limitazioni tecniche, essendo quindi più resistente di quanto sarebbe altrimenti possibile”.
Sulla questione del server: *“Oltre alle chiavi di esposizione temporanee, l'app Immuni invia anche al server alcuni dati di analisi. Questi includono informazioni epidemiologiche e informazioni tecniche e sono inviati allo scopo di aiutare il Servizio Sanitario Nazionale a fornire un'assistenza efficace agli utenti, per garantire il corretto funzionamento del sistema (…) in conformità con l'art. 6.2.b e 6.3 del Decreto Legge 28/2020”. Queste informazioni aggiuntive sarebbero “essenziali affinché il Servizio sanitario nazionale gestisca efficacemente il sistema, compresa la fornitura di assistenza sanitaria ottimale agli utenti”.*
Le Informazioni epidemiologiche sono: il giorno in cui si è verificata l'esposizione, la durata dell'esposizione, informazioni sull'attenuazione del segnale utilizzate per stimare la distanza tra i dispositivi durante l'esposizione, informazioni sulla probabilità che l'infezione si verifichi in base a quando si è verificata l'esposizione.
Tra l’altro *“esistono due momenti in cui l'app può inviare informazioni di esposizione al server” e cioè “al momento di valutare il rischio di trasmissione (il caricamento può avvenire dopo che l'app ha scaricato nuove chiavi dal server e valutato il rischio di trasmissione per l'utente, in base ai recenti contatti con utenti positivi SARS-CoV-2. In questo caso, i dati epidemiologici vengono caricati automaticamente) e al momento del caricamento delle chiavi di esposizione temporanee (quando un operatore sanitario comunica all'utente la sua positività a un test SARS-CoV-2, verranno caricati anche tutti i dati epidemiologici disponibili dei 14 giorni precedenti. In questo caso, il caricamento dei dati deve essere avviato dall'utente e approvato dall'operatore sanitario)”.*
Quindi nel secondo caso (con persona risultata positiva ad un tampone) i dati epiemiologici e clinici vengono caricati dalla persona interessata, previa approvazione dell’operatore sanitario, ma nel primo caso (con persona risultata a contatto con potenziali infetti) i dati del tracciamento vengono caricati nel server in maniera automatica.
Quindi, se capiamo bene cosa tutto ciò vuole dire, nel caso l’app valuti che ci sia un forte rischio di esposizione per una persona non ancora contagiata carica sul server gestito da Sogei e dal Servizio sanitario nazionale i dati in maniera automatica.
Sempre sul server: *“Tutti i dati, archiviati sul dispositivo o sul server, vengono eliminati quando non più rilevanti (generalmente entro poche settimane dalla raccolta e comunque entro il 31 dicembre 2020). Il Ministero della salute sarà il responsabile del trattamento dei dati, quindi deciderà quali dati raccogliere e come usarli esattamente. In ogni caso, i dati saranno utilizzati esclusivamente allo scopo di contenere l'epidemia di COVID-19 o, in forma completamente anonima o aggregata, per la ricerca scientifica”.* Anonima o aggregata? Non è proprio la stessa cosa!
I dati inviati al server includono anche informazioni sulla corretta configurazione del dispositivo (ad es. se il Bluetooth è attivo oppure no) e *“quando si caricano questi dati sul server, viene inclusa la provincia di domicilio dell'utente. Grazie a questi dati, è possibile stimare il livello di adozione dell'app in tutto il paese, non solo misurato dal numero di download, una metrica ampiamente priva di significato, ma dai dispositivi che funzionano effettivamente. Questa informazione è fondamentale, poiché sappiamo che l'utilità di Immuni dipende dalla sua diffusione all'interno della popolazione. Supportato da questi dati, il Servizio Sanitario Nazionale sarà in grado di prendere decisioni migliori quando si tratta di una serie di aree critiche per rendere Immuni il più utile possibile nel contrastare l'epidemia e fornire un'assistenza ottimale al paziente”.*
Quindi, dopo aver ripetuto fino allo sfinimento nell’intera documentazione su Immuni, che l’app

“rispetta la privacy dell’utente” e che l’app non saprà nulla del luogo in cui si è verificato un contatto a rischio, ecco che invece alla fine la documentazione ci dice che *“l'app procede a raccomandare agli utenti a rischio cosa fare. (…) Le raccomandazioni esatte dipendono dall'area in cui l'utente vive, poiché politiche diverse possono applicarsi a aree diverse. Per indirizzare l'utente nella giusta direzione, l'app raccoglie la provincia di domicilio durante il processo di onboarding”*.
Il vero motivo per cui Immuni raccoglie l’informazione della provincia di domicilio, attraverso i primi numeri del CAP, è facile da capire ed è funzionale per chiudere e rendere zona rossa una fetta di territorio in cui si registrino più contatti qualificati come a rischio. Una “cartografia” di dispositivi mobili concentrati in una certa area geografica, per esempio, potrebbe autorizzare l’intervento dell'autorità al fine di vietare o contenere gli assembramenti. E i CAP ormai non identificano più solamente una città ma, all’interno di questa, differenziano tra loro i quartieri ed alcune strade. Un bel modo per controllare la posizione delle persone, certo meno invadente del GPS ma pur sempre idoneo per l’uso che se ne vuol fare.
Eppure si continua a ripetere che Immuni non raccoglierà alcun dato e rispetterà la privacy. Questa strategia serve a *“Guadagnare e mantenere la fiducia degli utenti (…) per assicurarsi che l'app possa essere ampiamente adottata”*. E lo scrivono anche, nero su bianco!
Ma tutta la faccenda dell’anonimato è una chimera: *“Per proteggere la privacy dell'utente, i dati raccolti sulla loro esposizione a utenti potenzialmente contagiosi hanno alcune limitazioni. Ad esempio, la durata dell'esposizione viene misurata con incrementi di cinque minuti e limitata a 30 minuti per la somma di tutti i contatti con un utente infetto in un determinato giorno. Inoltre, Immuni non ha modo di determinare la presenza di più contatti in giorni diversi con lo stesso utente infetto”*. Certo, questo è stato studiato appositamente per evitare il replicarsi di alcune situazioni venutesi a creare specialmente nei paesi asiatici, dove l’introduzione delle app di tracciamento hanno dato vita ad una vera e propria caccia all’untore. Ma sarà sufficiente l’accorgimento dei 30 minuti come tempo limite per la somma dei contatti con una persona infetta? Sicuramente no! Se il mio cellulare mi indica che ho avuto un contatto a rischio ad una determinata ora di un determinato giorno, più volte in uno stesso giorno, facilmente potrò risalire alla persona contagiata con cui sono stato vicino quel giorno, anche se sul cellulare non compare il suo nome. Anche un bambino lo potrebbe capire! Ma per gli sviluppatori di Immuni e per il governo, noi non siamo bambini ma addirittura neonati.
Inoltre, sempre sulla questione della privacy, la documentazione oltre a dire che *“i dati memorizzati sul dispositivo sono crittografati”* e che anche *“tutte le connessioni tra l'app mobile e il server”* lo sono, si afferma che *“l'app non raccoglie dati personali che rivelino l'identità dell'utente. Ad esempio, non raccoglie il nome, l'età, l'indirizzo, l'e-mail o il numero di telefono dell'utente”*
E l’identificativo ID del dispositivo, non quello casuale fornito dal server, ma quello interno del cellulare? Se non viene citato, un motivo ci sarà!
Se questo ancora non bastasse, dovete sapere che in più sui dispositivi Android, oltre all’attivazione del Bluetooth, il servizio di ***“notifiche di esposizione”*** di Apple/Google (A / G Framework, le API) richiede espressamente anche l’attivazione della geolocalizzazione della posizione (ovvero del GPS) per far funzionare l’app. E questo sebbene la documentazione di A/G Framework affermi esplicitamente che non utilizzerà effettivamente i dati sulla posizione...ma allora perché chiede di attivare il GPS, dato che il tracciamento dei dispositivi non funziona con questo ma col Bluetooth!?
Quindi anche se è vero che l’app Immuni non richiederà l’autorizzazione per la posizione, sui dispositivi Android a questo ci penserà l'A/G Framework a livello si sistema. Dunque anche l’uso del solo Bluetooth è una balla!

Parte della funzionalità di Immuni, infatti, come abbiamo già detto è fornita direttamente dal sistema operativo dei rispettivi cellulari tramite le Api Apple e Google (l'A/G Framework): il database locale sullo smartphone sarà totalmente gestito dal sistema operativo, così come i dati archiviati su di esso. Questo vuol dire che se magari alcuni dati ed alcune informazioni non potranno veramente essere carpite dalla app Immuni, lo saranno senz'altro dai sistemi operativi dei propri smartphone che gestiscono le ***"notifiche di esposizione"***, di proprietà delle due multinazionali statunitensi. Nelle informative tecniche di Immuni, si legge infatti che "L'intero flusso di autorizzazione viene attivato dall'app e gestito dal sistema operativo".

***

MA PERCHÉ IL BLUETOOTH?

Ci sono app di tracciamento che adoperano il GPS o il Wi-Fi, altre il codice QR, altre il web, altre ancora un misto di queste tecnologie. Immuni, come altre app di tracciamento, userà il Bluetooth. O per meglio dire, la tecnologia Bluetooth Low Energy (B.LE), uno standard per le trasmissioni radio senza fili (wireless) a corto raggio che utilizza poca potenza di trasmissione per ridurre al minimo l'impatto del funzionamento dell'app sul consumo della batteria.
Si era parlato all'inizio, per l'app italiana, di soluzioni miste che potessero unire al tracciamento con il **B.LE** anche quello basato sulla geolocalizzazione e Bending Spoons, l'ideatrice della app "Immuni", aveva inizialmente adottato proprio questo approccio, estendendo la collaborazione per lo sviluppo di Immuni alla società GeoUniq, esperta in geolocalizzazione, salvo poi eliminare ogni riferimento al GPS nel progetto presentato al Ministero, visto il clima sfavorevole dell'opinione pubblica verso questa soluzione.
Noi conosciamo il Bluetooth principalmente come strumento che permette la comunicazione tra dispositivi che possiedono chip compatibili, in grado di collegare per esempio la play list musicale dello smartphone allo speaker wireless.
La tecnologia prenda il nome dal re danese Harald Blåtand, vissuto nel X secolo dopo Cristo, detto "Dente blu": grazie alle sue smanie di conquista, il sovrano creò un unico impero, collegando popoli diversi tra loro. Come il Bluetooth, che collega tra loro dispositivi diversi.
Per questo motivo nel 1994 un gruppo di ingegneri di **Ericsson** scelse questo nome quando creò la tecnologia Bluetooth (Qui la storia e come funziona nel dettaglio il Bluetooth: https://www.key4biz.it/come-funziona-il-bluetooth/103092/).
Il Bluetooth Low Energy (B.LE), è invece una tecnologia a radiofrequenza messa a punto a cominciare dall'anno 2010, presente come funzione nei telefoni IOS dal 2011 e in quelli Android dal 2012 (https://blog.beaconstac.com/2018/08/ble-made-simple-a-complete-guide-to-ble-bluetooth-beacons/).
Le app che usano questa tecnologia lo fanno per essere in grado di scovare altri smartphone nelle vicinanze. Attraverso un'app di tracciamento con Bluetooth attivato è possibile ottenere le 3 informazioni fondamentali per il *data tracing*:

1) qual è il dispositivo con il quale si è stati in contatto
2) a che distanza
3) per quanto tempo
La distanza tra due smartphone viene stimata dall'intensità del segnale.
La tecnologia Bluetooth è in grado di misurare la distanza tra due telefoni in modo molto accurato utilizzando le onde radio, per esempio rilevando se due telefoni sono distanti meno di tot metri e per più di tot minuti.
Per poter far funzionare “Immuni” non basterà, quindi, semplicemente la disponibilità di uno *smartphone* collegabile a internet, condizione comunque necessaria per poter scaricare l’app dagli stores ufficiali, ma anche che la tecnologia del cellulare supporti almeno lo standard Bluetooth 4.0 LE utilizzato dalle API dedicate di Google ed Apple (lo standard Bluetooth impiegata da Apple e Google non è molto diverso da quello che Apple sta già utilizzando per il suo servizio “Trova il mio iPhone/iPad”; tale servizio utilizza il Bluetooth per inviare segnali, anche quando il dispositivo non è connesso a Internet).
Dato che ritorniamo a parlare delle due multinazionali americane, diciamo anche che, per ora, sembrerebbe che il sistema operativo di Apple, a differenza di quello di Android, non consenta di eseguire il tracciamento dei contatti basato su Bluetooth in background cioè ad applicazione non aperta sullo schermo (equivale a dire solo apparentemente spenta). Questo significa che, per funzionare, le app per iOS dovrebbero rimanere sempre aperte sullo schermo, compromettendo la durata della batteria. Per questo, il governo di Parigi si sta rifiutando di aderire al protocollo e alla piattaforma fornita da Apple e Google, fino a che Apple non riduca, come chiesto dal governo francese, queste restrizioni di iOS per consentire un accesso più profondo da parte dell’app di tracciamento all’hardware, per ottenere il pieno accesso al Bluetooth anche quando un’app è in background.
Sembra un affare apparentemente secondario ma chi vuole a tutti i costi estendere le app di tracciamento ha fatto bene i suoi conti: se il funzionamento di un’app consumerà troppa batteria sul cellulare, anche chi l’avrà scaricata tenderà a disinstallare l’applicazione. Una cosa che i governi e le aziende sviluppatrici vorrebbero assolutamente evitare.
Ma vediamo cosa apprendiamo dalla documentazione di Immuni a proposito della tecnologia B.LE:
“Il sistema è più preciso. A differenza della geolocalizzazione, che, in molti contesti, ha una precisione dell'ordine delle decine di metri, i segnali Bluetooth Low Energy consentono di catturare i contatti che si verificano entro un raggio di pochi metri dall'utente. (…) La batteria viene utilizzata in modo più efficiente. Esistono soluzioni di localizzazione efficienti a batteria. Tuttavia, Bluetooth Low Energy tende ad essere eccezionale quando si tratta di efficienza energetica. Questo è importante perché è ragionevole aspettarsi che la velocità di disinstallazione dell'app sia correlata al consumo della batteria. Non sono richiesti dati di geolocalizzazione. Grazie a Bluetooth Low Energy, i contatti vengono tracciati senza tenere traccia della posizione degli utenti. Ciò potrebbe far sì che l'app venga accolta più favorevolmente dalle persone e potrebbe facilitare l'adozione più ampia, aumentando l'utilità di Immuni”.
https://github.com/immuni-app/documentation
Lo stesso discorso fatto per la geolocalizzazione, che tra l’altro non funzionare molto bene in luoghi chiusi, vale anche per le celle/antenne della telefonia mobile, che possono trovarsi posizionate a molti metri di distanza tra loro, addirittura chilometri fuori dai centri urbani. Dato che non basta sapere se due persone sono state nella stessa cella telefonica, ma bisogna verificare anche se sono state o meno alla distanza di un metro e per un tempo ragionevolmente lungo, il tracciamento tramite celle non è sufficientemente accurato.
Il Bluetooth LE dunque consuma meno batteria ed è più accurato e preciso del GPS e del Wi-Fi.

Almeno fino a quando questi strumenti non saranno potenziati realizzando le reti 5G (anche se occorre dire che gli smartphone moderni utilizzano comunque sempre anche la rete cellulare per la posizione ed il Wi-Fi non è mai davvero disattivato ma solo inibito nel suo funzionamento).
Una soluzione tecnologica a portata di mano è conseguentemente il Bluetooth, che al momento viene descritto come molto più preciso per il *contact tracing* e che dovrebbe consentire per esempio di riconoscere se al supermercato abbiamo fatto insieme la fila alla cassa rimanendo alla "giusta" distanza di sicurezza. Il Bluetooth rimane operativo anche dove il GPS non arriva, il wi-fi "non prende" e le celle sono troppo estese.
Come ha *spiegato Antonio Sassano*, presidente della *Fondazione Ugo Bordoni*, una delle aziende che ha partecipato alla call del ministero dell'Innovazione in contrapposizione a Bending Spoons, proponendo anch'essa un'app basata sul Bluetooth: *"Il Bluetooth consente di riconoscere se al supermercato abbiamo fatto insieme la fila per il pane o alla cassa e se non siamo stati sempre a distanza di sicurezza. La cella o il WIFi non sono in grado di effettuare questa distinzione e il GPS potrebbe non essere disponibile al chiuso" (*https://www.key4biz.it/antonio-sassano-fub-obbligatoria-e-basata-sul-bluetooth-la-app-della-fub-contro-il-covid-19/297013/).
Anche il Garante italiano per la Privacy ha avallato l'utilizzo del Bluetooth, affermando che tale tecnologia: "restituendo dati su interazioni più strette di quelle individuabili in celle telefoniche assai più ampie, parrebbe migliore nel selezionare i possibili contagiati all'interno di un campione più attendibile perché, appunto, limitato ai contatti significativi".
In più, se l'obiettivo è quello di proibire gli assembramenti pubblici, oggi un segnale Gps potente consente di raggiungere una precisione di circa 10 metri. Sicuramente accurato ma non abbastanza per determinare se le persone si tengono a meno di un metro di distanza dagli altri.
Infine, il Bluetooth ha il vantaggio, non secondario, di rispettare le linee guida fornite dalla Commissione Europea (il GDPR), appositamente studiate perché, come abbiamo detto, hanno pensato che un controllo troppo invasivo tramite il GPS potesse scoraggiare lo scaricamento di questa applicazione sul proprio smartphone.
Insomma, la scelta del Blutooth piuttosto che il GPS o altre tecnologie serve sia perché è efficace sia per fingere un rispetto dell'anonimato individuale che invece non ci sarà.
L'uso del Bluetooth, infatti, tra i tanti pregi che sono stati considerati dai controllori sociali, ha anche una miriade di criticità.
Al di là del fatto che venga usato o meno il GPS, infatti, una volta che verrà scaricata, la app conserverà sul dispositivo mobile di ciascuna persona ma anche sul server una lista di codici identificativi di tutti gli altri smartphone che hanno scaricato Immuni e ai quali la persona è stata vicino. L'avvocato esperto di privacy, Fulvio Sarzana, seppur non ostile a queste tecnologie a differenza nostra, ha reso bene l'idea: *"le app di tracciamento possono coinvolgere l'uso di bluetooth o di GPS. In entrambi i casi va sgomberato il campo da un equivoco, i dati trattati ed inviati eventualmente all'ente incaricato di gestire la relativa banca dati sono dati personali che non possono essere definiti anonimi ma solo pseudoanonimi. In altre parole, da quei dati è possibile comunque risalire ad una persona, ai suoi contatti, ai suoi spostamenti"* (https://www.ilsole24ore.com/art/torna-pista-gps-ecco-app-pole-position-il-contact-tracing-AD4CjEK).
Un'altra grossa vulnerabilità è che richiedere che tutti vadano in giro con il Bluetooth costantemente acceso per poter comunicare tra cellulari è di fatto equivalente a chiedere di lasciare aperta la porta di casa. Nel mondo reale, in cui la proprietà privata viene celebrata come fosse una divinità, in molto pochi lo farebbero dato che questo equivarrebbe ad esporre le case al rischio di intrusione. Lo stesso però accade nel mondo digitale, con la differenza che qui tutto accade senza la nostra

percezione diretta. È stato giustamente fatto osservare che oramai chi volesse carpire i dati non ha bisogno di essere un hacker professionista, dal momento che gli strumenti per farlo si trovano sul mercato con gran pubblicità e a prezzi piuttosto abbordabili.
E chi non possiede un cellulare abilitato con la tecnologia B.LE? Questo è un altro bel problema riscontrato da chi vuole introdurre nella società le tecnologie di tracciamento. Infatti i cellulari più vecchi non supportano il Bluetooth Low Energy di nuova generazione. Come fare, allora, se si vuol seguire lo studio condotto dai ricercatori del Big Data Institute dell'Università di Oxford, che afferma che il 60% della popolazione di un paese dovrebbe essere coinvolto dal tracciamento affinché questo sia ritenuto efficace? Bisogna stare molto attenti, perché la soluzione proposta dagli "esperti" del settore è quella di indossare braccialetti abilitati col B.LE. Ora per fortuna è solo allo stato di proposta – raccolta però in maniera propagandistica da regioni a vocazione turistica come la Liguria – ma chissà che i governi non ci facciano davvero un pensierino, sull'esempio dei paesi asiatici dove questa tipologia di sorveglianza è già diventata obbligatoria.
Un'altra criticità riscontrata nel Bluetooth è la velocità del trasferimento dati, più lenta rispetto al sistema Wi-Fi. Oppure i problemi di interferenza: i dispositivi Bluetooth funzionano con una banda sulla stessa frequenza utilizzata da molti altri dispositivi wireless e se molti dispositivi nella stessa area utilizzano tutti lo stesso tratto di larghezza di banda i segnali si "scontrano".
In più il segnale Bluetooth (almeno il 5.0, il più attuale) ha un raggio di azione di 200 metri all'esterno e dai 10 ai 40 all'interno e attraversa anche i muri, e ciò comporta il rischio elevato di cosiddetti "falsi positivi". Ad esempio, in un condominio, una persona potrebbe venire scambiata per soggetto a rischio contagio dall'app di tracciamento, anche se si trova in casa sua e dall'altra parte di un muro rispetto al possessore dell'altro cellulare. Si verrebbe così tracciati come potenziali positivi quando nella realtà non c'è stato nessun contatto.
Per minimizzare i falsi positivi, la Comunità europea ha avvertito che è necessario inserire delle "soglie" che permettano di escludere soggetti a più di un metro e mezzo di distanza fra di loro. Ma stiamo pur certi che quello dei falsi positivi sarà un problema che il Bluetooth non potrà mai eliminare del tutto.
In alcuni luoghi densamente popolati (alcuni quartieri, supermercati, grandi aziende, mezzi del trasporto pubblico) ci sarebbe un'esplosione di falsi positivi, che renderebbe del tutto inattendibile l'applicazione. Con il Bluetooth è possibile tracciare un contatto a prescindere da dove questo è avvenuto, per cui in maniera assurda non farà alcuna differenza l'avere avuto un contatto con un passante incrociato brevemente per strada o con un collega con cui si passano intere ore assieme al lavoro (su questo argomento vedi l'analisi dell'associazione La Quadrature du Net, pubblicata sul loro sito il 14 aprile - https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid - che evidenzia l'inaffidabilità della tecnologia Bluetooth e la sua mancanza di precisione nel tracciare i contatti con persone testate come "positive", specialmente nelle aree densamente popolate).
Il raggio di rilevamento del Bluetooth sembra inoltre variare troppo da un dispositivo all'altro (dipende dal modello e dal marchio del dispositivo) e la sua precisione non è necessariamente sufficiente per offrire risultati affidabili. Il suo segnale varia in potenza a seconda del chip, della batteria e del design dell'antenna.
Che il Bluetooth non sia proprio questo strumento super-affidabile come ci vogliono far credere, ce lo dice anche un estratto dalla medesima documentazione di Immuni: *"Più lunga è l'esposizione e più vicino è il contatto, maggiore è il rischio che si verifichi una trasmissione del virus. Un contatto che dura solo un paio di minuti e si verifica a diversi metri di distanza sarà generalmente considerato a basso rischio. Il modello di rischio potrebbe evolversi nel tempo man mano che*

saranno disponibili ulteriori informazioni su SARS-CoV-2. Va notato che la stima della distanza è soggetta a errori. In effetti, l'attenuazione di un segnale Bluetooth Low Energy dipende da fattori come l'orientamento dei due dispositivi l'uno rispetto all'altro e gli ostacoli (compresi i corpi umani) che si trovano nel mezzo. Sebbene lo sfruttamento di queste informazioni sia probabilmente utile per aumentare l'accuratezza delle valutazioni di Immuni sul rischio di contagio, con qualche frequenza si verificheranno valutazioni errate"(https://github.com/immuni-app/documentation).
Però, incoraggiante vero?
In Irlanda, i ricercatori del Trinity College di Dublino, il professor Douglas Leith e il dott. Stephen Farrell, hanno testato la capacità Bluetooth dei telefoni per le app di tracciamento dei contatti. Hanno preso le misure in diverse località di Dublino - in un supermercato, su una carrozza ferroviaria, seduti a un tavolo da riunione e camminando all'aperto in una strada cittadina. Ne hanno dedotto naturalmente che la misurazione della distanza corporea tramite Bluetooth non è così accurata: *"quando ci siamo seduti attorno a un tavolo con i telefoni in tasca, misurando l'intensità del segnale abbiamo riscontrato come fosse molto bassa anche con persone sedute una accanto all'altra"*, hanno affermato i due, aggiungendo che le persone dovrebbero posizionare i loro telefoni sul tavolo quando si siedono vicini.
Alla prima chiamata lanciata congiuntamente il 25 marzo scorso dal Ministro per l'innovazione tecnologica e la digitalizzazione, il Ministro dello Sviluppo Economico e il Ministro dell'Università e Ricerca, non a caso erano state proposte diverse soluzioni che pur proponendo l'uso del Bluetooth affiancavano quello del GPS. Anche Immuni all'inizio, come abbiamo detto, prevedeva l'azione combinata di GPS e Bluetooth. Questo perché un sistema misto, secondo i controllori sociali, renderebbero ovviamente un app di tracciamento strumento ben più "efficace". L'efficacia risiederebbe nella disponibilità di una maggior quantità di dati personali ottenibili con un sistema misto. I dati GPS, aggiunti a quelli raccolti col Bluetooth, disegnerebbero una mappa fisica con la posizione aggiornata delle persone su di essa. Ma ovviamente sarebbe un approccio molto più invasivo, in grado di individuare con certezza non solo i contatti avuti ma anche tutti gli spostamenti e i luoghi in cui ci si trova e violerebbe inoltre i regolamenti previsti dallo stesso GDPR.
I promotori di "Immuni", così come le istituzioni europee, hanno forse preferito fare marcia indietro per quanto riguarda la geolocalizzazione, dato il clima "anti GPS" attuale, per puntare tutto sul Bluetooth. Ma le leggi, i regolamenti, le norme si sa, possono sempre cambiare. Come la cautela delle persone verso queste tecnologie.

***

MA CHI C'È DIETRO L'APP "IMMUNI"?

La app di tracciamento italiano è stata realizzata da un apposito team, che si è avvalso della collaborazione con l'**Università La Sapienza di Roma**, della direzione tecnico-scientifica del presidente dell'Accademia dei Lincei, Giorgio Parisi e della valutazione tecnica dell'ex commissario per l'Agenda Digitale, Diego Piacentini, nonché di quella di Giuseppe Vaciago, avvocato esperto della gestione dei dati sensibili. L'app era già stata annunciata a marzo, senza citare il nome, ma chiamandola GEO-CROWD-VID-19, sia su alcuni siti specializzati (https://www.wired.it/internet/web/2020/03/24/coronavirus-app-contact-tracing), sia dall'Onlus Ascolto di P.Za Sant'Agostino 1 a Milano (https://onlusascolto.org), che citava tutti i partecipanti al progetto. **Ascolto Onlus**, appositamente creata, si è occupata di parte del reperimento dei fondi economici per far partire il progetto.

Il team ha compreso:
- Bending Spoons Spa
- Centro Medico Santagostino
- Arago
- Jakala
- Geouniq

Vediamone una società per volta.

GEOUNIQ

Partendo da quest'ultima, **GeoUniq** (www.geouniq.com) è una start-up italo-francese di Mobile Location Intelligence, ossia analisi di dati sulle abitudini comportamentali (viaggi, consumi, interessi) dei consumatori tramite gli smartphone.
Nata da Telecom ParisTech e HEC Paris, rappresenta oggi uno dei *"player con la migliore copertura in Italia"* con la bellezza di 9 milioni di cellulari tracciati tramite geolocalizzazione.
Ha sede legale a Parigi, una sede di ricerca a Pisa e un ufficio a Milano. Fondata nel settembre 2014 a Londra da Antonino Famulari (che ne è anche l'amministratore delegato), Kevin Dolgin e Martin Hogan, è specializzata in dati di localizzazione ed ha sviluppato un programma capace di individuare la posizione di un cellulare (compreso il piano del palazzo a cui si trova) con un errore di soli 10 metri. E' stata la prima startup italiana a entrare in *"Station F"*, l'incubatore parigino più grande d'Europa. Proprio da diversi programmi di aiuto all'innovazione del Governo francese è arrivato il primo incentivo economico alla società, che poi si è aperta a svariati investitori.
Le analisi raccolte tramite la geolocalizzazione sono vendute ad aziende di diversi settori, tra cui negozi, agenzie immobiliari, banche, assicurazioni. Dalle stesse parole di Famulari: «Vendiamo l'analisi dei dati e la composizione del pubblico di luoghi fisici. Il cliente paga in funzione del numero di punti di interesse (Poi) che intende monitorare, seguire. Tracciamo milioni di device e raccogliamo miliardi di posizioni al mese» (*Tratto dall'articolo"Noi, startup italiana a Station F", pubblicato su* Millionaire *di febbraio 2018.* https://www.millionaire.it/noi-startup-italiana-a-station-f/).
Nell'ottobre 2019, una quota del 25% della start-up è stata rilavata da **Jakala,** il primo gruppo

italiano specializzato nella cosiddetta “martech” (la tecnologia applicata al marketing) che ritroviamo anche dentro la cordata di imprese che ha sviluppato l’app di tracciamento Immuni. Ma a seguito della decisione di usare ufficialmente il Bluetooth e non il GPS come funzionamento per il tracciamento di Immuni, GeoUniq non figura più tra quelle di maggior peso in questa impresa. Che sia stata comunque inserita nel team un’azienda che sviluppa strumenti di geolocalizzazione, fa però capire molto bene che il sistema di tracciamento di “Immuni” è stato calibrato in modo da poter adoperare anche il GPS qualora questo fosse richiesto in futuro.

BENDING SPOONS

Nata nel 2013 in Danimarca dall’idea di quattro “nerd” italiani (Luca Querella, Francesco Patarnello, Luca Ferrari e Matteo Danieli) e un danese (Tomasz Greber), spostatasi poi nel centro di Milano nel nuovo quartiere Garibaldi-Porta Nuova, oggi **Bending spoons Spa** - che ha scelto per il proprio nome i cucchiai piegati con il pensiero, ispirandosi a una famosa scena del film Matrix - è uno dei primo sviluppatori di app per iOS (il sistema operativo di Apple) in Europa.
La società opera principalmente nel settore dello sviluppo di applicazioni per dispositivi mobili (smartphone e tablet) fornendo, con le proprie applicazioni, servizi che spaziano dal fitness al fotoritocco, dal salvataggio di password ai giochi. Ha al suo attivo applicazioni molto diffuse scaricate da circa 200 milioni di utenti e circa 270.000 nuovi utenti al giorno. Il gruppo è entrato nel 2018 tra le prime dieci aziende al mondo per download di app, davanti a giganti del Web come Netflix o Spotify.
Conta circa 48 soci (per la gran parte veneti ma anche polacchi, ungheresi, bulgari, danesi e messicani) e 140 dipendenti, età media di 28 anni, tra cui ovviamente molti ingegneri informatici provenienti aziende come Google, Apple, McKinsey e il Cern eche godono di amache appese ai muri, spazi relax con divani, tv e consolle di videogiochi, sala pranzo comune con pasti per i dipendenti ordinati via app e vacanze collettive pagate. Il processo di selezione per entrare a lavorare nell'azienda è rigidissimo. Solo lo 0,3% delle domande pervenute vengono accolte.
L’amministratore delegato è Luca Ferrari, uno dei cinque fondatori originari dell'azienda.
L’azienda ha fatto segnare oltre 90 milioni di fatturato nel 2019, il doppio dei profitti dell’anno precedente. La svolta è stata a luglio 2019, quando Bending Spoons ha aperto il suo capitale, cedendo il 5,7% a un pool di investitori esterni: H14, NUO Capital, StarTip.
Nei primi mesi del 2020 ha perfezionato la sua crescita con l’acquisizione di Grindr, la app di appuntamenti nata nel 2009 per favorire gli incontri tra persone gay e bisex.
Vedi:
https://www.ilsole24ore.com/art/la-holding-berlusconi-jr-punta-scalare-app-gay-grindr-ACCsiaDB
https://www.repubblica.it/economia/2020/04/17/news/bending_spoons-254269162/
https://www.corriere.it/economia/aziende/le-storie/cards/bending-spoons-app-immuni-numeri-societa-che-un-anno-ha-duplicato-fatturato/bending-spoons-societa-app_principale.shtml?refresh_ce-cp

La sede di **Bending spoons Spa** è nello stesso edificio che ospita l'Hollywood, la più famosa discoteca di Milano, al quarto e quinto piano al 15 di Corso Como ed ha una sede secondaria a Copenaghen.
La società ha partecipazioni societarie in molte altre. Il 18 luglio 2018 è stato approvato il progetto di scissione parziale della società mediante assegnazione di parte del proprio patrimonio societario a una società beneficiaria di nuova costituzione, denominata Bombonera srl con sede anch’essa Milano. Sempre nel corso del 2018 la società ha acquisito la partecipazione nelle società danesi Megara Ivs (100% del capitale); Easy tiger apps Ivs; Life fertility tracker Ivs.
Alcune società partecipate, Bending Spoons Apps Ivs e Life fertility tracker Ivs. forniscono servizi

di licenza alla società madre. https://www.ilsole24ore.com/art/bending-spoons-spa-milanese-che-traccera-covid-19-movida-disco-e-matrix-ADplprK

L'azionariato è così composto: l'80% è in mano ai quattro fondatori di Bending Spoons Luca Ferrari, Francesco Patarnello, Matteo Danieli e Luca Querella mentre un 10-12% fa capo ai collaboratori. Tra coloro che possiedono quote azionarie della società, con il **5,7%** del capitale complessivo, ci sono aziende in cui, come detto, compaiono grossi nomi dell'imprenditoria italiana e non solo quella:

- **H14**
- **NUO Capital**
- **StarTip**

H14 S.p.A. è la holding di Barbara, Eleonora e Luigi Berlusconi (figli di Silvio Berlusconi e Veronica Lario) che è proprietaria del 21% circa del capitale del gruppo Fininvest ed è a capo di altri investimenti tra i quali figurano nomi del calibro di FlixBus. La galassia Mediaset-Fininvest è molto attenta alle attività di Bending Spoons: Mediamond, ovvero la concessionaria per la pubblicità sulle properties editoriali di Mondadori e sulle properties digitali di Mediaset, ha avviato un anno fa una nuova partnership con Bending Spoons che consente all'app "Live Quiz" di Blending Spoons di entrare nel network adv di Mediamont.

StarTip è invece controllata al 100% dalla Tamburi Investment Partners S.p.A. (https://www.tipspa.it/it/), il braccio finanziario del banchiere Gianni Tamburi che concentra tutte le sue partecipazioni in start-up e in società attive nel segmento del digitale e dell'innovazione ed è direttamente correlata a nomi quali Alkemy, Buzzoole, Digital Magics o Talent Garden, e vive quindi sotto lo stesso tetto di un portfolio investimenti che annovera Amplifon, Moncler, iGuzzini, Hugo Boss, Ferrari ed Eataly.

Nuo Capital, che ha già investito in molte altre aziende italiane (almeno 8 in tre anni) è infine una holding cinese di investimenti della famiglia PAO/Cheng di Hong Kong. Ha sede a Milano ed è guidata da **Tommaso Paoli**. "Nello specifico a Steven Chen, nipote di Sir Y.K. Pao, uno degli uomini d'affari cinesi più famosi che, negli anni '50 del secolo scorso, arrivò a possedere la più grande flotta commerciale al mondo. Alla morte del fondatore nel 1991 l'immensa fortuna legata alla società World Wide Shipping andò agli eredi. Nuo Capital non è altro che uno dei tanti rami di questo impero. Fondata nel 2016 Nuo Capital, agevolata dalla banca d'affari cinese **Gca Altium**, guidata in Italia da **Carlo Dawan**, è entrata con una quota di minoranza del 30% nel gruppo **Ludovico Martelli** (60 milioni di euro di fatturato nel 2018), azienda toscana della famiglia Martelli leader nel mercato italiano della rasatura che commercializza prodotti in 60 paesi (proprietaria di brand storici come la crema da barba **Proraso,** i dentifrici di "lusso" **Marvis**, la linea di shampoo **Schultz**, le creme depilatorie **Oxy**, le linee **Sapone del Mugello** e **Valobra**, ecc). (Vedi: https://www.ilsole24ore.com/art/il-30percento-pro-raso-portafoglio-cinese-nuo-capital-AC76qAt).
Altre quote della holding italo-cinese vanno dall'arredamento con Sozzi Arredamenti al vino sia con l'ecommerce Tannico sia attraverso una partnership insieme a Terra Moretti passando per la tecnologia con Artemest. Nuo ha messo nel 2017 (in target con Cassa Depositi e Prestiti) uno zampino anche in Elite, la piattaforma di Borsa italiana che lavora per sviluppare eccellenze imprenditoriali italiane e portarle poi alla quotazione borsistica. La piattaforma è nata nel 2012 con la collaborazione di Confindustria, Tesoro e ministero per lo Sviluppo economico.
La partecipazione dell'holding cinese nell'azionariato di Bending Spoons ha fatto parlare qualche sovranista da strapazzo di un problema di sicurezza nazionale (vedi:

https://www.secoloditalia.it/2020/04/app-immuni-urso-fdi-indaga-il-copasir-vuole-vederci-chiaro-anche-sui-predatori-cinesi/). Ma il ruolo delle imprese cinesi nel mercato globale è un dato conosciuto da tempo. Compagnie cinesi, private e di stato, sono già presenti da anni sul mercato europeo ed italiano (ma anche statunitense, africano, asiatico, ecc…).
C'è già, quindi, quella 'colonizzazione predatoria' di cui si è parlato in termini allarmistici nei confronti di imprese che operano in settori strategici (produzione e approvvigionamento energetico, telecomunicazioni, infrastrutture, metallurgica pesante, agroindustria, farmaceutica, ecc…). É il gran gioco di vendite, acquisizioni, scorpori e scalate finanziarie. É il sistema capitalista globale, bellezza! E il capitalismo italiano ne è parte integrante, facendo la stessa cosa che fa quello cinese ma in altri territori (in Libia, per esempio). Lo si può accettare o lo si può combattere, ma non si può far finta di sorprendersi per il suo funzionamento (https://www.startmag.it/innovazione/bending-spoons-chi-sono-i-soci-anche-asiatici-dellapp-anti-covid-19/).

Dal consuntivo 2018 emerge che **Bending Spoons** ha finanziamenti tramite le maggiori banche italiane come *Intesa Sanpaolo*, *Unicredit*, *Ubi Banca*, *Banco Bpm*, *Bper*, *Banca Sella* e *Credito Valtellinese*.

IL CENTRO MEDICO SANTAGOSTINO

Il **Centro Medico Santagostino** (https://www.cmsantagostino.it/it), che a dispetto del nome non è di proprietà ecclesiastica, è una ricca rete di poliambulatori specialistici privati impegnati nella digitalizzazione dei processi ospedalieri ed è stato fondato nel 2004 da **Oltre Venture**, fondo d'investimento milanese che ne detiene una partecipazione del 15%. Da pochi mesi vede l'ingresso come socio di maggioranza (del **Fondo L-GAM**, "società d'investimento partecipata dalla famiglia regnante del Liechtenstein e da altre importanti famiglie imprenditoriali europee, americane e asiatiche". Il **Fondo L-GAM** ha acquistato l'85% del Centro, ovvero le quote degli azionisti privati di **Società e Salute Spa**.
Se Bending Spoons si è occupata di sviluppare l'app, in particolare il Centro Medico Santagostino si è occupato di mettere a punto il "diario clinico", la componente dell'app "Immuni" che "raccoglierà alcune informazioni cliniche rilevanti". Luca Foresti è l'amministratore delegato del Centro, con esperienze nella finanza e nell'imprenditoria digitale.
Il Centro ha chiuso il 2019 con un fatturato in crescita del 29% rispetto all'anno precedente, con circa 40milioni di euro. Gli investimenti totali nel 2019 sono stati pari a 5,5 milioni.
Il **CMS** ha diverse sedi, succursali e ambulatori presenti a Milano, Sesto San Giovanni, Buccinasco, Rho, Monza, Nembro, Bologna e Brescia.

OLTRE VENTURE – detiene il 15% delle azioni. Il capitale della società è suddiviso tra Luciano Balbo (presidente), Lorenzo Mario Allevi (amministratore delegato), Oltre Venture S.r.l., Adriana Versino, Compagnia di San Paolo, Banca Nazionale del Lavoro, Fondo d'investimento Italiano S.r.l, Hdi Assicurazioni Spa, Azimut Enterprise Srl, Cleops Srl, Creazione di Valore Srl, Etica Sgr Spa, F3f Spa, Faro Srl. Finda Spa, Fondazione Sviluppo e crescita, Ca Indsuez Fiduciaria Spa, La Conte Srl, Lubafin Srl, Mais Spa, Sofrinex holding Srl, Tetrafin Srl, Trois I-Inestissements industriels internationaux Sa, Fondazione Social Venture Giordano dell'Amore, Future Srl, Fondo pensione nazionale Bcc/Cra. A questi si aggiungono azionisti di minoranza, tra cui compaiono diverse fondazioni.

Il FONDO L-GAM - possiede l'85% del centro, è una società d'investimento partecipata dalla famiglia regnante del Liechtenstein e da altre importanti famiglie imprenditoriali europee, americane e asiatiche. Il fondo, che investe investe in società in cui l'impegno di capitale varia da 40 a 95 milioni, è nato nel 2013 per volontà di Ferdinando Grimaldi (ex senior partner di Bain Capital e di Investcorp), Yves Alexandre (ex capo degli investimenti europei di Investcorp) e Felipe Merry del Val (ex senior partner di Bain Capital) (https://www.startmag.it/economia/centro-medico-santagostino-chi-sta-dietro-lapp-anti-covid-19-di-bending-spoors/).

JAKALA Spa

Jakala è un colosso milanese dell'e-marketing con oltre 200 milioni di euro di fatturato nel 2018, fondato, guidato e controllato da Francois e Matteo de Brabant (oggi la famiglia de Brabant è azionista di maggiornaza con il 44%) e specializzato in gestione e analisi di dati, che nasce nel 2000 e "combina marketing e tecnologia applicati al mondo dell'engagement, della fidelizzazione e dell'incentive".
Nel 2000 Jakala aveva come socio di maggioranza Europ@web, al tempo holding di Arnault. Poi negli ultimi due anni ha visto entrare nuovi soci.
Nel 2014 si è fusa con la società specializzata nello sviluppo di strategie di marketing personalizzate **Seri System**, diventando **Seri Jakala**.
Nel 2015 la società di consulenza **IT Value Lab** è entrata nel gruppo e nel 2018 le due aziende si sono fuse nel **Gruppo Jakala** (https://www.jakala.com/).
Nel 2018 l'azionariato si quindi arricchito attraverso un "club-deal" organizzato da **The Equity Club** di **Mediobanca** private banking: così al suo interno, seppure attraverso una holding, figurano tra gli altri **Renzo Rosso**, le famiglie **Dompè** e **Branca**, i **Lucchini**, **Giuliana Benetton** e la stessa **Mediobanca** (https://www.ilsole24ore.com/art/coronavirus-salotto-buono-app-immuni-mediobanca-berlusconi-jr-ADYBWxK?refresh_ce=1).
Altri soci di minoranza sono **PFC** (holding della **famiglia di Paolo Marzotto**, col 10,5%), il fondo di private equity paneuropeo **Ardian Growth** (7,5%), di nuovo la **H14** dei figli di **Berlusconi** (2,5%) e **Davide Serra** (2,7%).
Ha poi rilevato nel 2019 una quota del 25% di **GeoUniq**, società italo-francese che sviluppa tecnologie di geolocalizzazione per dispositivi mobili. *"Questa operazione consolida la leadership di Jakala sui servizi di Location Intelligence & Analytics a livello mondiale, arricchendo i servizi di data driven marketing & sales, in grado di supportare la crescita della top line dei nostri clienti"* - ha dichiarato per l'occasione Stefano Pedron, A.D. Jakala - *"La partecipazione in GeoUniq rappresenta la prima tappa di un percorso strategico più ampio"*.
Quella di GeoUniq costituisce la seconda acquisizione del 2019 per Jakala, che nel giugno aveva comprato anche **Volponi**, un'azienda per la raccolta punti e premi nella grande distribuzione, con sede a Macerata e con un giro d'affari di circa 30 milioni di euro; tra i suoi maggiori clienti Conad e Sigma.

La sede centrale di **Jakala** è in Corso di Porta Romana 15 a Milano.
Le altre sedi italiane sono a Roma in Via Salita di S. Nicola da Tolentino 1 e a Torino in Via F. Santi 1 / 2 (ma ha sedi anche in una decina delle più grandi capitali del mondo)

Volponi Spa, Via Ugo Foscolo, 5/A, 62010 Montecassiano, Macerata

ARAGO

Nel progetto di Immuni entra anche la tecnologia della tedesca **Arago** di Hans-Christian Boos (https://hiroai.co/about/). Il nome di Arago emerge anche dalla relazione del gruppo di esperti responsabile dei profili giuridici dei progetti.
Specializzata in intelligenza artificiale e business automation, Arago ha sede a Francoforte, ed è stata fondata appunto da Chris Boos, imprenditore nel settore tecnologico e membro del Digital Council tedesco, con l'incarico di consigliare il governo tedesco nel promuovere politiche di informatizzazione del Paese. Negli ultimi mesi però, il nome di Boos si è diffuso soprattutto al di fuori dei confini della Germania, grazie al progetto Pepp-Pt, il consorzio europeo che avrebbe dovuto stabilire le linee guida europee per il tracciamento dei dati prima dell'ingresso in campo della piattaforma di Apple e Google.
Dai documenti del ministero dell'Innovazione si scopre infatti che in origine l'azienda di Boos ha avuto un ruolo centrale nel progetto di Bending Spoons, "Immuni", che integrava proprio la "*tecnologia di tracciamento contatti basate sul Bluetooth low energy (Le) di Arago*".
Ai tempi della relazione, Bending Spoons aderiva a Pepp-Pt, anche se oggi il logo dell'azienda non compare più sulla pagina di presentazione on-line del consorzio europeo.
Boos ha presentato Pepp-Pt il primo aprile. E al suo interno figurava già una prestigiosissima lista di partner, tra i quali appunto allora Bending Spoons. Boos è stato ed è attualmente la testa di pepp-PT, oltre a essere ritenuto responsabile del semi-naufragio dell'iniziativa, che oltre alla competizione con i due colossi americani si è sfaldata sotto il peso delle accuse di scarsa trasparenza.

SEDE: ARAGO GmbH, Eschersheimer Landstr. 526-532 60433, Frankfurt am Main, Germany

In conclusione, sono d'obbligo alcune considerazioni: con il download di "Immuni" i dati scaricati dall'applicazione sono al vaglio non solo del governo, ma corrono il rischio di finire in qualche modo – corruzione, compravendita dei dati, hakeraggio - anche nelle mani di società private. In questo caso della maggiore società di applicazioni per smartphone italiana (Bending Spoons), di una catena di ambulatori privati (il Centro Medico Santagostino) e di una megasocietà di marketing pubblicitario che opera nel settore dei big-data (Jakala), oltre che di buona parte del salotto buono del capitalismo italiano tra cui i figli di Silvio Berlusconi.
Scusate se ci balena il legittimo sospetto che queste società potrebbero riutilizzare i dati sanitari della popolazione italiana per finalità ben diverse che la tutela della salute!

CHI È SOGEI?

La corsa per chi doveva gestire il server pubblico del Ministero della Sanità con i dati raccolti dall'app di tracciamento Immuni è stata tra due società a partecipazione statale: **Sogei** (che gestisce i dati per l'amministrazione fiscale) e **Sia** (società attiva nei servizi tecnologici di pagamento controllata da).
La prima al 100% controllata dal ministero dell'Economia e delle Finanza e la seconda controllata con oltre l'80% da CDP Equity, holding di investimenti di Cassa Depositi e Prestiti (Per approfondimenti https://www.sia.eu/it).

Alla fine il governo italiano ha preferito la seconda, Sogei appunto.
Sogei - Società Generale d'Informatica S.p.A. - nata nel maggio del 1976, ha preso in carico la realizzazione dell'Anagrafe Tributaria, per gestire in modo automatizzato le attività di controllo e di monitoraggio del prelievo fiscale, dopo che una riforma fiscale del 1974 aveva innalzato il numero dei contribuenti italiani da 4 a 25 milioni di soggetti.
Acquistata da Telecom Italia nel 1997 e privatizzata, Sogei è tornata nuovamente in mano pubblica nel luglio 2002 con l'acquisizione dell'intero capitale sociale da parte del Ministero dell'Economia e delle Finanze, che la controlla appunto al 100%.
Sogei si occupa oggi del processo di digitalizzazione della Pubblica Amministrazione e dello Stato. Gestisce l'intero Sistema informativo della fiscalità e l'automazione dei processi operativi e gestionali del Ministero e altre pubbliche amministrazioni. Clienti di Sogei sono: Agenzia del Demanio, Agenzia Dogane e Monopoli, Agenzia delle Entrate, Dipartimento del Tesoro, Ragioneria Generale dello Stato, Dipartimento delle Finanze, Guardia di Finanza, Dipartimento dell'Amministrazione Generale, ma anche i Ministeri dell'Interno, della Giustizia, dell'Istruzione, dei Beni Culturali e del Turismo, la Corte dei Conti, l'Avvocatura Generale dello Stato, il Dipartimento per la programmazione della politica economica, l'Agenzia per la Coesione Territoriale, l'Agenzia per l'Italia Digitale (AgID) e infine Equitalia Giustizia. Sogei gestisce quindi una mole a dir poco gigantesca di dati, molti dei quali personali, che possono anche venire incrociati tra di loro (http://www.sogei.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/150).
Sogei detiene pure una partecipazione azionaria nel capitale sociale della **GEOWEB S.p.A.** (https://ex.geoweb.it), società costituita dal Consiglio Nazionale Geometri e Geometri Laureati per "semplificare l'attività professionale degli iscritti alla categoria e il rapporto con la Pubblica Amministrazione, nonché costituire nuove opportunità di lavoro". "Tali servizi vengono erogati a favore dei soci e dei clienti, siano essi pubblici, privati o appartenenti ad altre categorie e ordini professionali".
Quindi Sogei, che ricordiamo è controllata totalmente dallo Strato, ha a che fare però attraverso una partecipazione in Geoweb con imprenditori privati a cui eroga servizi. Attraverso la partecipazione di Sogei, Geoweb offre "La disponibilità dei servizi telematici da e verso l'Agenzia delle Entrate" come le "visure catastali e le ispezioni ipotecarie" ai propri clienti "i quali possono operare dal proprio studio in tempo reale, per ottenere informazioni e certificati, scambiare documenti e messaggi, consultando e aggiornando, ove necessario, le banche dati di interesse" (http://www.sogei.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/922).
Dai server della Sogei passano i dati delle dichiarazioni dei redditit degli italiani e, dal primo gennaio 2012, pure tutti i movimenti dei conti correnti. Chi si fida perché il server sarà pubblico, non capisce che in fondo non cambia nulla! Il mix di pubblico e privato nella società capitalista è di fatto indistricabile. Su Sogei ricordiamo un'indagine per corruzione e finanziamento illecito ai partiti, sul sistema con cui, nel periodo che va dal 2002 al 2010, venivano affidati gli appalti milionari della Spa controllata dal ministero dell'Economia. La società di Stato aveva girato in nove anni lavori per circa 25 milioni di euro all'Edil Ars dell'imprenditore Angelo Proietti. Secondo le accuse, gli appalti (assegnati senza gara, a trattativa privata) erano ottenuti grazie alle pressioni dell'ex braccio destro di Giulio Tremonti, Marco Milanese, amico di Proietti (in cambio l'uomo aveva ristrutturato gratuitamente la casa romana in via di Campo Marzio affittata da Milanese aTremonti), il tutto con la complicità dell'ex presidente della Sogei, Sandro Trevisanato.
Ma è poi vero che i dati sono gestiti interamente da società pubbliche?
Nel 2010, Sogei ha commissionato un accordo chiamato Oio, Open Infrastructure Offering) da 135,4 milioni di euro con procedura secretata nel 2010 con la multinazionale Usa **IBM** per la

fornitura di infrastrutture informatiche, servizi professionali, software e licenze d'uso. Nell'accordo c'era anche lo sviluppo del "Progetto Mirò", relativo alla realizzazione della «smart security area», un piano di sicurezza per proteggere gli hardware che custodiscono i dati sensibili delle persone. L'intero progetto non solo era «secretato», ma affidato da Ibm attraverso un subapalto alla ditta Ciss srl, che ha avuto circa 6 milioni di euro. Un'operazione autorizzata dalla Sogei nell'ottobre del 2010. Ma la Ciss (Centro installazioni sistemi di sorveglianza, nata nel 2002) è un'altra azienda controllata direttamente da Proietti il quale, attraverso la Ap holding, possiede il 55 per cento delle quote di questa srl. Nel 2010 Proietti, attraverso la solita Edil Ars, ottiene da Sogei anche il rinnovo (sempre a procedura secretata) del contratto per la manutenzione dei palazzi e degli impianti per circa 2,5 milioni di euro.
Nell'agosto 2011, dopo le prime indiscrezioni sull'inchiesta, l'allora ministro Tremonti decise di cambiare i vertici della Sogei che lui stesso aveva nominato: l'ad Marco Bonamico, vecchio amico di Proietti (tanto da assumere in Sogei la figlia di Angelo) e il presidente Sandro Trevisanato (https://espresso.repubblica.it/affari/2012/11/29/news/sogei-la-procura-di-roma-indaga-1.48439). Dopo una lunga gestione di Cristiano Cannarsa, l'attuale presidente è Biagio Mazzotta e l'amministratore delegato Andrea Quacivi.
Nel 2013 l'Autorità per la vigilanza sui contratti pubblici (oggi ANAC) pubblica il referto di un'indagine sugli appalti di Sogei dal 2006 al 2011 iniziata in precedenza, che si conclude con numerosi riscontri di irregolarità e con l'invio degli atti alla Procura della Repubblica ed alla Procura della Corte dei Conti.
Ricordiamo poi anche i crash del server di Sogei per le domande di rottamazione delle cartelle esattoriali, con la piattaforma dell'Agenzia delle Entrate-Riscossione in tilt a ogni scadenza fiscale a fronte del numero di richieste di accesso (https://www.ilfattoquotidiano.it/2018/05/15/rottamazione-cartelle-sito-dellagenzia-delle-entrate-a-singhiozzo-da-venerdi-per-le-troppe-domande-serve-una-proroga/4357020/).
Davvero volete affidare i vostri dati a Sogei (quelli riguardanti la vostra salute), più di quanto non stiate già facendo?

Sogei S.p.A. - Sede Legale Via M. Carucci n. 99 - 00143 Roma

Chi è PagoPA S.p.A.

Pago Pa è una società partecipata dallo Stato creata allo scopo di diffondere il sistema di pagamenti e servizi digitali in Italia attraverso **PagoPA** (www.pagopa.gov.it.), la piattaforma unica per i pagamenti digitali verso tutte le Pubbliche Amministrazioni ed i gestori di pubblici servizi e le società a controllo pubblico (escluse le società quotate). La società è nata per effetto del Decreto Legge "Semplificazioni" del 14 dicembre 2018, convertito in legge il 12 gennaio 2019, che prevede l'istituzione di *"una società per azioni interamente partecipata dallo Stato"*, vigilata dal Presidente del Consiglio dei ministri o del Ministro delegato.
PagoPa gestisce anche "IO", l'app per i servizi pubblici e la Piattaforma digitale nazionale dati (PDND). Nella propria "mission" PagoPa S.p.a. scrive che *"una società deve rispondere alle regole del mercato"* (https://www.pagopa.gov.it/it/pagopa-spa/).
Una bella presentazione per una società pubblica, non c'è che dire!

Vedi: Piattaforma Digitale Nazionale Dati (https://pdnd.italia.it).

IO, *l'app dei servizi pubblici in Italia* (https://io.italia.it).

PagoPA S.p.A. sede legale Piazza Colonna 370, Roma, CAP 00187

***

IL TRACCIAMENTO DEI CONTATTI IN ITALIA, LE "CONCORRENTI" DI IMMUNI

Fin da subito si sono levate accuse di poca chiarezza rivolte al progetto di Bending Spoons, a cominciare da quei competitor di "Immuni" che si sono contesti la possibilità di sviluppare l'app nazionale di tracciamento italiana.

Tra le app che hanno partecipato al bando del governo italiano, arrivata seconda in finale con "Immuni" è stata "**Covid Community Alert"** (sui giornali la troviamo anche con nome di "**CovidApp"**) un progetto open source per Android ed IOS del team internazionale **Coronavirus Outbreak Control** (https://coronavirus-outbreak-control.github.io/web/index_it.html).
Covid Community Aler fa parte inoltre della **TNC Coalition** (https://tcn-coalition.org/partners-and-members), una rete federata e cosmopolita di giovani ingegneri e tecnologi bramosi di entrare con tutti e due i piedi in un mondo fatto di chip e algoritmi e di cui fa parte, per esempio, anche la Coalition Network che collabora con il MIT di Boston (il "Protocollo TNC", infatti, è stato rilasciato sotto licenza MIT).
L'app Covid Community Alert è stata rilasciata sotto il protocollo "**SafeTogether" ecosystem** (https://safe-together.github.io/specification/).
Mente del progetto per Covid Community Aler e di SafeTogether è Luca Mastrostefano, affiancato dal supporto del veronese Giuseppe Stefano Quintarelli.
Quest'ultimo è imprenditore nel digitale, scrittore oltre che ex parlamentare di Scelta Civica di Mario Monti. Appare anche nel consiglio direttivo dell'**Associazione Copernicani** (https://copernicani.it/) una delle compagini, con circa 200 soci tra professionisti privati e politici, responsabili della campagna *#IoRestoACasa* ed anche promotrice dell'iniziativa *FlexibleWorking*, una piattaforma on-line che fornisce esperienza per allargare il tele-lavoro nelle aziende durante il periodo di emergenza Coronavirus.
Dal 2014 Quintarelli è anche presidente del comitato di indirizzo di Agenzia per l'Italia Digitale (**AgID** – Via Liszt 21, Roma https://www.agid.gov.it/), l'agenzia pubblica istituita dal governo Monti nel 2012 per perseguire alti livelli di innovazione tecnologica nella pubblica amministrazione.
Su wikipedia di Quintarelli si può leggere che *"è uno dei pionieri nella introduzione di Internet in Italia"* (addirittura!) e che *"ha teorizzato Internet come una dimensione dell'esistenza, in cui si creano e sviluppano relazioni sociali ed economiche e la nascita di un nuovo conflitto di classe tra intermediari ed intermediati che avvolge e sovrasta il tradizionale conflitto tra capitalisti e proletari"*. Ma anche che è membro del Gruppo di esperti ad alto livello sull'intelligenza artificiale della Commissione Europea.
Luca Mastrostefano, residente a Londra, dove lavora come ingegnere informatico in un fondo di investimento per startup europee (la **InReach Ventures,** https://www.inreachventures.com/), è invece il presidente di una società con sede a Brescia di marketing digitale e comunicazione b2b

(Business-to-business, una locuzione utilizzata per descrivere le transazioni commerciali elettroniche tra imprese), l'agenzia di comunicazione e pubblicità **Gruppo Wise** che realizza video-spot e siti internet e che che ha chiuso il 2019 con circa 1,5 milioni di euro di fatturato (Via Creta, 31, Brescia, 25124 Brescia - https://www.gruppowise.com/).
Covid Community Alert del consorzio Coronavirus Outbreak Control, sarebbe interoperabile tra le nazioni che la richiedono: l'app ed il consorzio sono nati dal lavoro di 35 esperti di sei paesi diversi che lavorano da quattro continenti, dal Brasile (dove sta collaborando con il CNR del paese) alla California, fino all'Italia. Tra lo staff degli sviluppatori dell'app ci sono gli italiani Carlo Martini, programmatore web toscano di origine ma romano di adozione, co-fondatore di **MioAssicuratore**, il primo broker assicurativo personale online in Italia (Via Gaspare Spontini 22, 00198 Roma); Antonio Romano, capo tecnologo di **Rebrandly**, azienda di marketing e pubblicità con sede a Dublino; il romano Domenico Lupinetti, grafico che lavora per AirBnb, Google e Microsoft.
Nel sito si dice che il consorzio collabora, tra gli altri, con Raffaele Perego, Direttore della ricerca di ISTI-CNR; Stefano Leonardi, professore all'Università la Sapienza di Roma; Giuseppe Attardi, professore di Computer Science all'Università di Pisa; Davide De Nardis, ricercatore alla Becar Srl azienda di elettronica industriale di Monteveglio a Bologna; Enrico Fagnoni, presidente di LinkedData.Center; Fabio Cassanelli & Emanuele Bartoli che si occupano di cyber security per la società "Be Shaping the Future" che offre servizi digitali per banche ed assicurazioni ed ha svariate sedi in capitali europee (in Italia, a Roma in Viale dell'Esperanto 71 e a Milano in Piazza Affari 2). Inoltre ha il supporto della stessa Associazione Copernicani; dei campus universitari Pi-Campus di Roma (https://picampus.it) fondati da Marco Trombetti; del docente Oreste Pollicino della Bocconi di Milano e di altri ancora.
Direttamente coinvolta è proprio l'**Associazione Copernicani**, di cui socio è l'ex parlamentare Quintarelli, che come leggiamo in inglese in un post sul loro blog *"sostiene gli sforzi senza fini di lucro di un ampio gruppo di volontari internazionali per sviluppare tecnologie che aiutano e supportano i professionisti nella loro lotta contro COVID-19"* avendo lanciato anche una raccolta fondi attraverso MamaCrowd, piattaforma italiana di crowdfunding, per sostenere l' *"Ecosistema SafeTogether" (https://mamacrowd.com/project/una-tecnologia-per-ripartire)* e chiusa il 17 aprile quando ormai sembrava chiaro che il governo avesse scelto Immuni e non CovidApp/Covid Community Aler (https://copernicani.it/blog/2020/04/13/safe-together-using-technology-to-support-fight-against-covid-19/)
A sua volta l'intero Coronavirus Outbreak Control fa parte dei gruppi che a livello internazionale stanno usando il protocollo *"SafeTogether"*, quello che pomposamente amano chiamare il loro "ecosistema", che alle spalle ha il colosso **Microsoft** e l**'Università di Washington.**
Oltre all'Associazione Copernicani di Quintarelli e a Coronavirus Outbreak Control di Mastrostefano, apprendiamo dell'adesione al protocollo *"SafeTogether"* anche di **LinkedData.Center** (Via Leonardo da Vinci, 10 Lecco - https://en.linkeddata.center) società specializzata in irnfomatica ed A.I. di cui presidente Enrico Fagnoni; **gOv.it civic hacking community** (https://copernicani.it/il-software-g0v-it/); **Comdata** grossa società di soluzioni digitali aziendali con oltre 10 000 dipendenti in Italia e più di 20 centri operativi (https://italy.comdatagroup.com/it/chi-siamo/le-nostre-sedi); **Politecnico di Milano** (Piazza Leonardo da Vinci 32, 20133 Milano - https://www.polimi.it) e di altre grosse aziende che operano a livello internazionale: **Inforcert** (https://www.infocert.it); **Keyless** (https://keyless.io/); **SIA S.p.A** (https://www.sia.eu/it); **TeamSystem** (https://www.teamsystem.com); **Tesla Consulting** (https://www.teslaconsulting.it); **SiamoSoci – MamaCrowd** (https://mamacrowd.com). Tutte le notizie relative le potete trovare al link: https://safe-together.github.io/specification/
Il sistema di Covid Community Alert/SafeTogether si basa su due distinte app: **CovidApp** che pure appoggiandosi sul Bluetooth per il tracciamento della prossimità e la notifica dell'esposizione, prevede anche una condivisione opzionale della posizione GPS e **CoviDoc** per i medici che funziona con scansione del codice QR del paziente e registro dello stato di salute (diario clinico) da aggiornare giornalmente, inoltre il sistema prevede un pannello web di controllo per gli epidemiologi con impostazione dei parametri che attivano le notifiche.

Per discolparsi della geolocalizzazione in CovidApp, dal consorzio fanno sapere che*"lo scopo è quello di allargare le maglie del tracciamento con GPS (100 metri invece dei 10 abituali) per cercare di rendere questa tecnologia più accettabile, aggirando l'ostilità di parte dell'opinione pubblica e per rispondere alle critiche che parlano di sorveglianza di massa"*.
Per imporre la quarantena, il sistema si basa sul controllo telefonico da parte di un call center e attraverso un riconoscimento biometrico eseguito localmente su smartphone (qui il video: https://www.youtube.com/watch?v=nScyb1bLXn8&feature=youtu.be). Si prevede poi una sorta di autocertificazione di immunità attraverso il cellulare. Inoltre il protocollo proposto, dichiarano sul sito, è la base per mettere in piedi ulteriori servizi, come ad esempio la possibilità di raccogliere segnali anche grazie a dispositivi dell'internet delle cose (https://www.wired.it/internet/web/2020/04/10/coronavirus-app-tracking-task-force/?refresh_ce=).
Al contrario di Immuni, l'archiviazione dei dati di Covid Community Alert, anche se fa parte della coalizione TNC che ufficialmente consiglia un metodo di archiviazione decentralizzato, avviene anche in maniera centralizzata, per di più su giornali specializzati si è scritto su server di proprietà di **Amazon web service**.
Nel sito del consorzio si legge che il tracciamento fornito sarebbe più efficace di quello di altri standard come ad esempio "TraceTogether" di Singapore ed altre, offrendo un monitoraggio *"del 38% in più rispetto a soluzioni Bluetooth tradizionali (…). La nostra tecnologia è in grado di monitorare anonimamente dal 91.2% al 98.5% di tutte le interazioni tra cellulari contro il 71.7% delle tecnologie tradizionali"*.
Ad oggi le app del consorzio hanno trovato impiego solo in Brasile, dove si è iniziata l'integrazione con i servizi informatici del paese. Sono in attesa di autorizzazione in Polonia, Canada e nello stato di New York. Le società che partecipano a questa impresa internazionale di tracciamento non hanno comunque perso la speranza di applicare il loro standard anche in Italia: *"Il nostro codice continua a essere a disposizione delle autorità sanitarie che lo vogliono ispezionare, se in Italia penseranno di averne bisogno potranno usarlo. (…) Abbiamo mostrato una demo funzionante di una soluzione che si può integrare anche nelle altre app. Quelle regionali, per esempio, perché non si può chiedere ai cittadini di scaricare l'app della Lombardia e poi quella nazionale. In Brasile stiamo lavorando così"*.
https://www.corriere.it/tecnologia/20_maggio_06/app-immuni-l-ingegnere-covidapp-sorpresi-dall-esclusione-eravamo-pronti-test-6c809f60-8f83-11ea-bb7f-d3d655d2211a.shtml
Le app del consorzio sono tradotte in Italiano, Inglese e Portoghese e il consorzio le sta traducendo nelle 10 lingue più parlate al mondo per facilitarne l'adozione.
La documentazione in inglese si trova qui: https://github.com/Coronavirus-Outbreak-Control/

Oltre ai due finalisti **"Immuni"** e **"CovidApp"/"SafeTogether"** (che si sono presentate divise, pur risultando lavorare in stretto rapporto), altre quattro proposte avevano superato il turno ed erano state scelte dal governo italiano come semi-finaliste per il progetto di contact tracing nazionale (vedi la relazione del gruppo di esperti del governo su https://innovazione.gov.it/assets/docs/SGdL6%20-%20Relazione.pdf):

- "**ProteggInsieme"** della **Whatif srl**, società di sviluppo web ed app (Viale Europa 28 64023, Mosciano Stazione, Teramo), basata sul protocollo "BlueTrace" del governo di Singapore, è stata scartata dal gruppo di esperti del governo italiano perché non avrebbe abbastanza esperienza nel tracciamento con la tecnologia Bluetooth;
- "**TrackmyWay"**, della **Antares Vision spa**, società quotata del Bresciano (Via Del Ferro 16 - 25039 Travagliato - Brescia) che, pur avendo "*esperienza comprovata nel campo del tracking digitale di oggetti in movimento tramite tecnologia GPS*" (pacchi, prodotti e farmaci per le aziende, soprattutto), scrivono i tecnici, non ne ha altrettanta nel campo del contact tracing con Bluetooth, ed in più propone un modello di archiviazione solamente centralizzato; l'azienda ha da poco lanciato anche "TRACK MY HEALTH", una soluzione per imprese ed istituzioni che prevede un mix di termoscanner e controlli biometrici completamente automatizzati per l'ingresso-uscita di persone da

spazi pubblici e per il rispetto delle distanze interpersonali generando, in automatico, segnali di allarme in caso di situazioni o comportamenti anomali. Può fare un conteggio sulla presenza del numero persone e controllare la presenza o meno della mascherina sul volto.
- "**COMBAT"** di **TIM - Telecom Italia Spa**, che si articola su dati estratti dalle celle telefoniche (già in uso da parte delle Regioni) in combinazione ad una app di tracciamento.
Ricordiamo che TIM si avvale abitualmente per stoccare i dati dei clienti morosi (numeri dei cellulari del cliente ed altre informazioni fornite dall'utente) del server di S.I.Mo.I.Tel., banca dati interoperatore per le compagnie telefoniche che vi hanno aderito, gestito dalla società CRIF S.p.A. con sede legale in Bologna, Via Fantin n. 1-3. Chissà se in questo server non potrebbero finire anche i dati del contact tracing di TIM, nel caso l'app di tracciamento COMBAT superasse lo stato di proposta per diventare veramente disponibile.
Tim, assieme a Vodafone, Orange, Telecom Austria, China Mobile e altri grossi gruppi di TLC, fa parte di Next Generation Mobile Networks Alliance, un raggruppamento che spinge per l'adozione della tecnologia 5G, Tra chi sostiene finanziariamente l'Alliance ci cono tutte le più grandi multinazionali, da Apple a Facebook, Ericsson, Huawei, Intel, Lenovo, Lg, Nokia e molte altre (vedi https://www.ngmn.org/about-us/our-partners.html).

A rispondere al bando del MISE, sempre con un sistema basato sul Bluetooth - la app "**StopCovid"** (https://www.key4biz.it/come-funziona-la-app-stop-covid-della-fub-video/297537/) - c'è stata anche la **Fondazione Ugo Bordoni (FUB)**. Nata nel 1952 in seno al Ministero delle poste e delle telecomunicazioni ed oggi soggetta alla vigilanza del Ministero dello sviluppo economico, la FUB attiva nel campo della ricerca e dell'innovazione tecnologica, con presidente **Antonio Sassano**, fra i massimi esperti di tracciamento di frequenze e dati, uno dei più accesi propugnatori dell'adozione del 5G in Italia.
Sassano è quello che in un'intervista (https://www.privacyitalia.eu/antonio-sassano-fub-obbligatoria-e-bluetooth-ecco-la-nostra-app-contro-il-virus/12942/) afferma che *"sarà necessario monitorare tutte le persone in movimento e raccogliere dati sulle loro interazioni (…) prima ancora di sapere se una di queste persone è o si rivelerà positiva al test"* costruendo *"una ragnatela di collegamenti che legheranno ciascuno di noi con le persone con le quali siamo venuti in contatto nei 20 giorni precedenti"* e che permetta *"in un certo istante di sapere come sono raggruppati gli italiani"* e *"se un gruppo cresce troppo rapidamente nel tempo abbiamo un "assembramento" possiamo intervenire"*.
Quindi un modello che va al di là anche del modello coreano, come dice ancora Sassano: *"Il modello coreano traccia i positivi e coloro che hanno interagito con loro. Il nostro traccia tutti"*. *"in conclusione la nostra applicazione traccia i sani (…) non viene attivata dall'individuazione di un contagiato (…) a posteriori"*
"Ovviamente memorizzeremo, se disponibili, anche la posizione e la cella ma non saranno queste le informazioni importanti. L'informazione decisiva è il contatto a distanza ravvicinata (…) Ovviamente l'uso dell'app dovrebbe essere obbligatorio per muoversi nella fase post-crisi. Invece di verificare se abbiamo l'autorizzazione cartacea, le forze dell'ordine dovrebbero verificare se l'app sta funzionando e non è stata manomessa. Per questo motivo, credo saranno necessari interventi di Legge. In particolare, per rendere obbligatorio il portare con sé un cellulare con una versione di Bluetooth". Ovviamente!
Indirizzi FUB:
- Sede Legale - Viale del Policlinico 147, 00161 Roma (RM);
- Viale America 201 (c/o Ministero dello sviluppo economico), 00144 Roma;
- Villa Griffone Via Celestini, 1, 40037 Pontecchio Marconi (BO).

Un altro progetto che ha partecipato alla call del governo, basato sempre sul Bluetooh, è quello del **Gruppo Vetrya**. Luca Tomassini, è il fondatore, presidente e Amministratore Delegato del grosso gruppo italiano tra i leader riconosciuti nello sviluppo di servizi digital, piattaforme cloud, internet degli oggetti ed intelligenza artificiale per le più famose corporation italiane e mondiali. Intervenuto ai microfoni di Radio 1: "*Noi come Vetrya, abbiamo aderito alla call del Ministero dell'Innovazione presentando "***Pj19** *Tracer" la soluzione basata sulla tecnologia Bluetooth. Se la nostra soluzione dovesse essere scelta dal Governo, potrebbe essere pronta in una settimana o dieci giorni in via sperimentale, per andare in esercizio in venti giorni"* (https://www.key4biz.it/app-e-tracciamento-tomassini-vetrya-bisogna-partire-presto-nostra-soluzione-pronta-in-7-giorni/299366/).
Pj19 è stata sviluppata con **Sogei**, che è la società del Ministero dell'Economia e delle Finanze e col supporto del **CNIT**, il Consorzio Nazionale Interuniversitario per le Telecomunicazioni (Sede legale: Viale G.P. Usberti, 181/A Pal.3 - 43124 Parma https://www.cnit.it/) che consorzia 37 università italiane a cui si aggiungono 8 unità di ricerca presso il CNR, per un totale di 45 unità di ricerca. Il CNIT è attivo in molti aspetti che si occupano di ricerca legata al 5G: partecipa a e coordina diversi progetti EU H2020 su 5G; quattro di questi si sono classificati al primo posto nelle rispettive graduatorie; è stato membro eletto della 5GPPP (https://5g-ppp.eu/), una iniziativa che unisce la Commissione Europea e il settore dell'ICT in Europa per finanziare con 1,4 miliardi di € la nuova generazione di reti e servizi di telecomunicazioni; partecipa alla sperimentazione MISE 5G nell'area metropolitana di Milano; partecipa a progetti EU H2020 sulle applicazioni di 5G, tra cui veicoli autonomi e sistemi intelligenti di trasporto. Direttore del CNIT è il prof. Nicola Blefari Melazzi, Università di Roma, Tor Vergata, mentre presidente è il prof. Gianni Vernazza del Dipartimento di Ingegneria Navale, Elettrica, Elettronica e delle Telecomunicazioni (DITEN) all'Università di Genova.
Grazie poi all'esperienza maturata per lo sviluppo di "Pj19" Vetrya ha sviluppato il successivo "**Pj20"** (https://www.pj20tracer.it/) ovvero un dispositivo Bluetooth indossabile (al collo come una collana oppure al polso come un orologio) progettato come soluzione digitale per il monitoraggio in tempo reale della distanza tra le persone in ambito aziendale e professionale.
Quando due o più dispositivi bluetooth Pj20 tracer e/o l'app Pj20 tracer si avvicinano al di sotto di una determinata distanza (per esempio 1 metro) la persona sarà avvertita da un suono, una vibrazione o una segnalazione luminosa. Non richiede alcuna infrastruttura di rete ma in alternativa al dispositivo indossabile può essere utilizzata anche una specifica app installata sul proprio smartphone. Tutti gli eventi vengono registrati nella memoria del dispositivo e in quello dell'applicazione.
Il **Gruppo Vetrya**, fondato nel 2010 a Orvieto, ha sedi anche in California, Brasile, Malesia, Spagna, Uk e da poco anche in Russia. È presente negli Stati Uniti attraverso Vetrya US Inc., con sede a Palo Alto (CA), sul mercato del sud-est asiatico attraverso la società Vetrya Asia Pacific Sdn. Bhd. con sede a Kuala Lumpur Malesia, in America Latina con la società Vetrya do Brasil con sede in Brasile, a Rio de Janeiro, sul mercato iberico con Vetrya Iberia Sl a Madrid e sul mercato inglese attraverso la società Viralize UK Ltd, Londra.
Possiede un campus di 40.000 mq in via dell'Innovazione 1-2 ad Orvieto, in Umbria, dove è anche la sede del Gruppo.

Un'altra app per il contact tracing in Italia è la "**Digital Arianna" (DiAry)**, progetto che l'**Università di Urbino** ha intrapreso in febbraio con il supporto tecnico dello spinoff universitario **DIGIT srl** (https://digit.srl) e coordinato dalla cattedra di Sistemi di Elaborazione delle

Informazioni della stessa università. Sito ufficiale del progetto: https://covid19app.uniurb.it/
Mentre l'app "Immuni" utilizzerà la tecnologia Bluetooh, DiAry punta sulla geolocalizzazione. *"Rileva automaticamente la posizione e gli spostamenti dell'utente e ne conserva memoria locale (cioè sul dispositivo personale), campionando la posizione in modo intelligente, cioè solo quando cambia significativamente"* e permette di *"etichettare tutti i luoghi in cui si ferma per almeno 5 minuti e ne mantiene memoria riconoscendoli nei giorni successivi, calcola statistiche giornaliere del tempo trascorso in ciascun luogo o in movimento, riconoscendo se gli spostamenti avvengono a piedi, in bicicletta o su veicoli a motore"*.
Conserva sul dispositivo personale tutti i dati che raccoglie, con l'eccezione di informazioni statistiche che possono essere conferite ad un server, su richiesta dell'utente.
Con "Immuni," fanno sapere da Urbino, non ci sarà concorrenza ma una prevedibile integrazione: *"due strategie diverse ma che possono interfacciarsi per diventare complementari"*. Se "Immuni" registra ogni contatto ravvicinato tra cellulari di persone diverse, DiAry mantiene memoria dei luoghi in cui ogni giorno sostiamo, con *"errori di posizionamento dell'ordine di 5 metri, ma all'interno degli edifici o in strade molto strette è meno accurato"* (dal sito di DiAry https://uniamo.uniurb.it/app-uniurb-diary-covid19).
"*Abbiamo sempre sostenuto che debbano essere usate in modo integrato tecnologie complementari, localizzazione e Bluetooth,* — ha detto il prof. Alessandro Bogliolo, responsabile del progetto DiAry. — *Noi abbiamo investito prima di tutto sulla localizzazione per fare leva sulla responsabilità individuale, ma con l'intenzione di adottare un approccio integrato. Quando il governo ha scelto Immuni e optato per il Bluetooth, abbiamo deciso di non integrarlo in diAry, per attendere di interfacciarci ad Immuni, quando sarà disponibile"* (https://covid19app.uniurb.it/fase2-usiamo-digital-arianna/).
C' insomma il rischio che "DiAry" possa divenire prima o poi il diario clinico di "Immuni" e per mezzo della localizzazione con GPS possa poi arrivare a risalire alla persona fisica e ad imporre la quarantena.
Dal 23 marzo l'applicazione è stata testata su 250 volontari e dal 16 è disponibile in versione beta sugli store Android e iOS.
Chi ha congegnato DiAry ha anche ben pensato a degli incentivi pur di farla adottare.
A DiAry è infatti legato un sistema di accumulo punti WOM (acronimo di *Worth One Minute*), con un sistema di *gamificazione* (cioè l'introduzione di elementi tipici del gioco, come i punti, i livelli e la classifica, in un contesto sociale non ludico) dove il punteggio diventa reputazione sociale, sull'esempio di quanto accade in Cina e in altri paesi asiatici.
WOM (https://wom.social) è una piattaforma inclusa tra gli strumenti di innovazione sociale digitale della Commissione Europea che si basa su un sistema di scambio di voucher progettati per *"riconoscere il valore delle azioni che hanno un effetto positivo e per fornire uno strumento di ricompensa"*. Tanto più tempo l'app con GPS è attiva sul proprio telefono e tanto più tempo il sistema di localizzazione rileva che sei fermo nella tua abitazione, tanti più punti accumuli.
Usare l'app con la localizzazione accesa e restare a casa sono cioè azioni ritenute socialmente positive che danno poi diritto a sconti spendibili in esercizi commerciali che mettono a disposizione beni e servizi (https://malamente.info/2020/05/23/immuni-e-diary-perche-le-app-per-il-tracciamento-non-sono-la-soluzione-ma-un-ulteriore-problema/#more-2550).
In Romagna, a Cesena ha sposato con entusiasmo il progetto di "DiAry", di cui si sta facendo "ambasciatore", il professore Mario Alai, che insegna Filosofia all'Università di Urbino.
https://www.corriereromagna.it/coronavirus-docente-cesenate-diffonde-un-app-anti-contagio

"I Feel-you" è invece un prototipo di braccialetto ideato e realizzato dal gruppo di ricerca del Dynamic Interaction Control Lab dell'**Istituto Italiano di Tecnologia (IIT) di Genova** (Via Morego 30, 16163 Genova - https://www.iit.it/it/home) per il tracciamento dei contatti, sfruttando i risultati di ricerca ottenuti nell'ambito del progetto An.Dy dedicato allo sviluppo di una tuta capace di registrare alcuni parametri del corpo umano per la creazione di tecnologie che consentano ai robot di interagire con le persone, e finanziato dall'Unione europea nell'ambito del programma Horizon 2020 (https://www.ilsole24ore.com/art/la-tuta-che-misura-movimenti-corpo-e-permette-collaborare-i-robot-ACXcSSCB).
l'IIT, finanziato dallo Stato per lo sviluppo delle nuove tecnologie, si occupa prevalentemente di nanotecnologie, robotica, scienze della vita e intelligenza artificiale.
L'organizzazione di IIT si basa sui Central Research Laboratories, con sede a Genova, e ad una ampia rete di ricerca composta da 11 centri (per un totale di quasi 60.000 m2) presso alcune delle principali università italiane (Università di Ferrara, Università di Trento, Politecnico di Milano, Politecnico di Torino, Scuola Normale Superiore in Pisa, Scuola Superiore Sant'Anna di Pisa, Sapienza di Roma, Università Federico II di Napoli, Università del Salento di Lecce, Ifom-IEO di Milano, Università Ca' Foscari) e da 2 centri negli USA in collaborazione con il MIT ed Harvard.
"I feel-you" emette una vibrazione e un segnale luminoso quando si supera la distanza di sicurezza tra persone per rispettare la *distanza sociale* in pubblici esercizi, locali commerciali e stabilimenti balneari. ll direttore scientifico dell'IIT, Giorgio Metta, e il ricercatore di IIT coordinatore del progetto braccialetto, Daniele Pucci, hanno precisato che il braccialetto *"non ha un Gps, ma funziona tramite onde radio"*. Ma è inoltre in grado di misurare la temperatura corporea quando supera i 37,5°, di registrare con quali altri braccialetti è venuto in contatto e in futuro potrà rilevare anche la saturazione dell'ossigeno nel sangue.
È un dispositivo che potrà essere utilizzato all'interno di luoghi chiusi oltre che all'aperto, in situazioni dove non è semplice utilizzare altre tecnologie, quali smartphone e termocamere. Potrà trovare applicazione all'interno di villaggi turistici, centri benessere, aree sportive e parchi di divertimento (https://www.ilsole24ore.com/art/ifeel-you-braccialetto-intelligente-la-fase-2-ADNzoRN).
Insomma, controllo totale. Ma cosa potevamo aspettarci da chi, come ingegnere ricercatore nell'ambito dell'interazione uomo-macchina, nel laboratorio Dynamic Interaction Control di IIT si occupa di risolvere i problemi della locomozione robotica umanoide e realizzare robot umanoidi volanti (!).
Presentato dalla Regione Liguria e dal presidente Toti come uno strumento utile a gestire la presenza di turisti nelle spiagge liguri (ci si può perfino fare il bagno in mare), l'IIT sta al momento cercando un partner industriale che finanziando il progetto ne effettui la realizzazione. Per il futuro, i proponenti del braccialetto la vorrebbero proporre anche per *"fabbriche e uffici, ma anche nei villaggi turistici, dove già si viene dotati normalmente di un braccialetto"*.
https://www.mentelocale.it/genova/articoli/84610-braccialetto-iit-sulle-spiagge-vibra-se-non-si-mantengono-distanze-liguria-verso-riapertura.htm
Oltre alla Liguria, l'idea di introdurre braccialetti di tracciamento è venuta al presidente di una scuola dell'infanzia di Castellanza, nel Varesotto, per il distanziamento dei bambini all'asilo, suscitando alcune polemiche (https://www.tpi.it/cronaca/braccialetto-asilo-bambini-distanziamento-polemica-20200508598676/).
Ma anche la Sardegna ha fatto sapere dell'intenzione di adoperare braccialetti simili. Il presidente

della regione, Christian Solinas, sta valutando, con un gruppo di tecnici, la possibilità di acquisire braccialetti da distribuire a duemila persone positive da monitorare a distanza: *"si tratta di dispositivi collegati a una centrale che rilevano in tempo reale la saturazione di ossigeno nel sangue, la temperatura e i parametri cardiaci", oltre ovviamente al segnale GPS (https://www.unionesarda.it/articolo/news-sardegna/cagliari/2020/03/25/controlli-la-sardegna-vara-il-modello-coreano-video-136-1001508.html).*
Non saranno per caso gli stessi braccialetti dell'IIT?

Braccialetto portatile per mantenere la distanza fisica è anche **"Labby Light"** proposto dalla start-up barese specializzata in tecnologie per lo sport e il fitness **MetaWellness Srl** (Via Giuseppe Petraglione 20, Bari – https://metawellness.it/), espressamente pubblicizzato come *"la soluzione per il distanziamento sociale"*. Funziona senza l'utilizzo di app e smartphone, non utilizza GPS o Bluetooth ma onde radio wireless brevettate, mentre sembra che i dati non vengono condivisi con server ma archiviati sul bracciale, che memorizza internamente ID, giorno, ora e tempo di contatto con gli altri braccialetti con cui entra in prossimità. L'utente viene allertato con una vibrazione e luce led quando non è rispettata la distanza. È espressamente congegnato per dipendenti e clienti di aziende: stabilimenti balneari, ristoranti, hotel, centri sportivi, cliniche, uffici, scuole e *"qualsiasi altra attività che preveda l'aggregazione di dipendenti e clienti"*. La start-up ha intenzione di divulgarlo nelle spiagge per la prossima stagione turistica e già diversi stabilimenti balneari hanno dimostrato il loro interesse, per distribuirlo all'ingresso degli stabilimenti.
"Ed è disponibile anche in versione 'stick' da tenere in borsa, in tasca o sulla cintura" (https://www.leggo.it/italia/cronache/fase_2_mare_bracciali_alberghi_spiagge_anti_covid-5205561.html).
Ricordiamo che l'introduzione di questi aggeggi è agevolata dallo Stato Italiano, che ha previsto un credito di imposta al 50% ai privati per l'acquisto di strumenti per arginare il Covid19 sui luoghi di lavoro e in posti pubblici.

Un altro braccialetto portatile che avverte se non si rispettano le distanze tra persone, messo a punto soprattutto per le aziende in vista della "Fase2", è **"Safety Bubble Device SBD"** (https://www.safetybubbledevice.com) ideato dalla **VeSta** (http://www.vesta-corporate.com), una start-up marchigiana che opera nel settore dell'efficienza energetica, con sede operativa milanese al **Polihub** della **Fondazione Politecnico di Milano,** in collaborazione con **Zanini Consulting** (via Cesare Battisti 8, 63821 Porto sant'Elpidio, Fermo).
Spacciato come DPI, dispositivo di protezione individuale per gli ambienti di lavoro (vedi il video https://www.youtube.com/watch?v=D-4o54hps7k) - inseribile in braccialetti in silicone, porta badge, clip da taschino, applicato o cucito su tute e gilet da lavoro – il "braccialetto" vibra o suona a una determinata distanza da un secondo dispositivo, di cui capta il segnale, quando le persone non mantengono la distanza di sicurezza imposta. SBD immagazzina poi le informazioni di contatto tra dispositivi.
Nel caso un dipendente risultasse positivo al Covid-19, le informazioni sui contatti tra dispositivi verrebbero mandati all'autorità competente.
https://www.ansa.it/sito/notizie/tecnologia/hitech/2020/04/21/arriva-braccialetto-misura-distanza_9f753cb8-9d15-4f7f-b68b-51c6dda953fb.html
SEDI:

- PoliHub di Milano: Via Giovanni Durando 39, 20158 Milano (MI)
- Sede legale Vesta: via Burago 6, 20876 ORNAGO (Monza-Brianza)
- Sede operative: via Tiraboschi 36/G, 60131 ANCONA (AN)

Un altro progetto che ha partecipato alla chiamata del governo italiano è **"Covid-19&Mobility"** (https://www.facebook.com/pg/covid19mobility/about/) sviluppato e messo a punto da Francesco Finazzi e Alessandro Fassò, docenti in Statistica all'**Università degli Studi di Bergamo (UNIBG).** Il progetto ha lo scopo di misurare gli spostamenti, il numero delle persone e la distanza percorsa dalle proprie abitazioni, tramire un app già disponibile che dal 2012 ad oggi ha ottenuto più di 5 milioni di download e ha inviato più di 2.900 allerte. Il progetto si basa infatti sul progetto **"Earthquake Network" (**https://sismo.app) ovvero un'app che rileva i terremoti utilizzando le informazioni dello smartphone, che è stata creata per avvisare in tempo reale la popolazione in caso di evento sismico. Esiste dal 2012, lo sviluppatore dell'applicazione per smartphone è Francesco Finazzi dell'Università di Bergamo, e da allora sono stati effettuati più di 5,5 milioni di download in Italia e nel resto del mondo. Dal 2019 Earthquake Network fa parte dei progetti "*TURNkey*" e "*RISE*" finanziati dalla Commissione Europea nell'ambito del programma Horizon2020.
Con la motivazione del Covid19, UNIBG, insieme al Dipartimento di Ingegneria Gestionale, dell'Informazione e della Produzione, a Earthquake Network ed a Steamware, hanno chiesto a chi abita nei comuni della Val Seriana di installare l'app gratuita "Rilevatore Terremoto" per un'indagine pilota sulla mobilità.
Come funziona? Per avvertire gli utenti in zona, l'applicazione deve conoscere la posizione degli smartphone, che ogni mezz'ora il telefono comunica ad un server. Questo vuol dire che per ogni utente è possibile, attraverso il GPS, conoscere le coordinate spaziali del dispositivo. Un dato che consente di sapere con precisione la posizione delle persone, "dato fondamentale in questo momento storico, in cui, per via dell'epidemia da coronavirus, ci viene chiesto dalle autorità pubbliche di rimanere in casa". Chi scarica l'applicazione acconsente al trattamento della privacy.
I dati raccolti consentiranno ai ricercatori di UNIBG di calibrare il sistema per *"informare in tempo reale le persone su variazioni del rischio individuale in relazione alla zona a cui si staranno avvicinando o ai soggetti con cui staranno per interagire"*. Alcune potenzialità di adattamento dell'app al monitoraggio della mobilità pubblicate sulla pagina Facebook di Covid-19&Mobility.
Il server di questa app si trova in una struttura ubicata in Francia e fornita dal provider **OVH**.
Tornando al monitoraggio degli spostamenti degli italiani, lo studio statistico dell'app ha così potuto verificare, per esempio, che si è passati da un 33% di persone che stavano a casa il 10 marzo ad un 77% circa di domenica 22 marzo mentre in media, nei fine settimana, quindi sabato e domenica, il dato si è attestato attorno al 72%, al contrario la percentuale di chi rimane a casa dal lunedì al venerdì si assesta attorno al 65%. Ma lo studio dei dati forniti dall'app ha fornito anche informazioni sulla distanza media percorsa durante questi spostamenti da casa ad altri luoghi, potendo riscontrare i picchi durante i giorni feriali, cioè una media compresa tra 6 e 8 km percorsi.
Insomma, con l'app si può verificare quantitativamente quante persone stanno a casa e quante sono in giro e quindi il rispetto o meno delle ordinanze (https://www.key4biz.it/app-misura-spostamenti-finazzi-universita-degli-studi-di-bergamo-a-casa-il-72-degli-italiani-nel-fine-settimana/298080/).
Inoltre, grazie all'appoggio del Rettore, Remo Morzenti Pellegrini, è stata avviata un'indagine pilota in Val Seriana (BG), zona tra le più colpite dall'epidemia, dove si è chiesto a chi abita i comuni della valle bergamasca di installare l'app Rilevatore Terremoto. Maggiori dettagli sono disponibili sul sito *www.sismo.app/covid*.

#BackOnTrack è invece la app di tracciamento sviluppata dal raggruppamento di imprese guidato da **Netalia** (Via Fieschi 20, 16121 Genova – https://www.netalia.it), cloud provider italiano che propone soluzioni tecnologiche, protezione dei dati e data center per la media impresa e per la pubblica amministrazione. Un'altra società implicata nell'affare è **Italtel** (Via Reiss Romoli - loc. Castelletto - 20019 Settimo Milanese, Milano - https://www.italtel.com/it/), società di gestione sui Big Data e intelligenza artificiale. Offre anche soluzioni per lo smart-warking.
Il Raggruppamento Temporaneo d'Impresa che ha presentato la soluzione è tutto italiano ed è composto oltre che da Netalia e Italtel, anche da **Beta80, SPX Lab, To Be, Helpy, ARMNet, I.RE.**
La app "lavora da sola". Ovvero ti traccia senza dirtelo, acquisendo costantemente dati di localizzazione "*tramite Gps, WIFI, informazioni dalle reti mobili"*.
"L'idea in sintesi è di risalire nella maniera più semplice possibile alla lista dei contatti che ha avuto, nei giorni precedenti, una persona che si dovesse rivelare positiva incrociando dati di posizione che vengono rilevati attraverso strumenti di uso quotidiano come smartphone e tablet", racconta **Federico Descalzo**, responsabile Sviluppo Alleanze e Mercato di Netalia (https://www.key4biz.it/backontrack-la-app-di-netalia-per-combattere-il-virus/297833/).
L'app garantisce, ad uso delle autorità, il tracciamento di una persona specifica grazie al riconoscimento biometrico (iride o volto) che identifica in maniera univoca la persona che viene tracciata. Il progetto inoltre comprende la "chatbot visuale" Minerva, con news ufficiali sull'evoluzione del contagio e contro le "fake news" e pensata per integrare l'autodichiarazione.
Complimenti! È probabilmente questa, e non "Immuni", l'app di tracciamento sperimentata nel progetto-pilota introdotto dalla Ferrari sui dipendenti di Maranello, col supporto della regione Emilia-Romagna. (https://autosprint.corrieredellosport.it/news/formula1/2020/04/08-2907197/coronavirus_ferrari_ecco_il_progetto_back_on_track_/).
Netalia, in cordata con I-Tel Srl (https://www.i-tel.it/it/), società con competenze nei servizi on-line e nella sanità digitale (ma anche nel tele-lavoro), con sedi a Riccione, Bari, Roma e Milano, sta anche studiando un sistema per la tele-sorveglianza dei pazienti in quarantena, anzi, in "isolamento fiduciario obbligatorio", come preferiscono dire (https://www.linkedin.com/feed/update/urn%3Ali%3Aactivity%3A6651808365339004928).

Si è parlato molto anche di app che sostituiscono l'autocertificazione cartacea per potersi spostare da casa. Un'app con queste caratteristiche, spacciata come scelta *green* per non dover consumare carta, è ***"SOS Italia"***, progettata dai soci di **Aidr-Associazione Italian Digital Revolution** (Viale Liegi 14, 00198 Roma – https://www.aidr.itcon), un'associazione di promozione sociale per il sostegno dell' I.A. e della digitalizzazione costituita da avvocati, dirigenti e funzionari pubblici, docenti universitari, medici e professionisti con Mauro Nicastri come presidente.
L'app è stata pensata assieme a **Sielte - Società Impianti Elettrici e Telefonici S.p.A.** (Piazza Tivoli 44, 95030 Tremestieri Etneo, Catania e Via Valle di Perna 1, 00128, Roma RM - https://www.sielteid.it), che è il gestore di SPID ovvero la piattaforma pubblica per le identità digitali e le firme digitali.
È stata proposta per la fast-call al governo italiano, attraverso un video:
https://www.youtube.com/watch?v=ByrxjRFMQ48
Oltre a generare in modo digitale l'autocertificazione, anche questa app consente il tracciamento, qui col GPS attivo anche con cellulare spento, ed è fornita di diario clinico.
Possiamo solo immaginare quale invasività avrebbe una app in cui si devono inserire i dati richiesti

dal modello cartaceo e cioè nome, cognome, ubicazione della residenza, data e ora, codice fiscale, numero documento, luogo di provenienza e di destinazione ed ovviamente la motivazione dello spostamento. In più l'app è predisposta per avere un codice QR Code per essere letto dalle Forze dell'ordine se dotate di un dispositivo idoneo per farlo (https://www.key4biz.it/covid-19-lapp-per-lautocertificazione-con-lo-smartphone-e-spid/297481/).

Un altro competitor di "Immuni" è stata la app gratuita **"Stop Covid 19"** (https://www.stopcovid19.it/it/) della **Webtek**, uno studio di comunicazione grafica, web agency e software house di 30 persone fondata e controllata dal 2008 dal trentenne Emanuele Piasini a Poggiridenti, piccolo paesino a pochi chilometri da Sondrio, in Valtellina (https://www.webtek.it). Partner del progetto è **Anzani Group** (https://www.anzanigroup.com/it/index.aspx), sviluppatore di software ed I.A. con sedi ad Erba, Sondrio, Chiasso e Lugano. Lo studio legale Scardaccione Pelandini di Milano ha fornito la consulenza in materia di dati e privacy.
La app in questione, in questo caso, raccoglie i segnali GPS dei dispositivi mobili per localizzare il dispositivo su cui è installata e memorizzare i dati relativi agli spostamenti e li convoglia in un sistema di intelligenza artificiale che poi li sovrappone per individuare i soggetti venuti a contatto con un contagiato. Le autorità competenti potranno avere accesso ai dati in caso di positività. Oltre alle autorità, nessun utente può visualizzare i dati, nemmeno i propri. Dicono che i dati saranno automaticamente cancellati dopo 30 giorni. La app registrerebbe dati solo quando è accesa.
Già approvata dalle app store di iOs e Play Store di Android, StopCovid19 è progettata per acquisire e raccogliere in un registro digitale le informazioni sugli spostamenti del dispositivo sul quale è installata. Ciascun dato viene associato in maniera obbligatoria al numero di telefono dell'utente e raccolto nei server mantenuti dall'azienda, che attualmente si appoggia ai servizi di **Amazon web service**, come ha spiegato a *Wired* Emanuele Piasini, amministratore delegato della Webtek.
Da quanto abbiamo letto in un'intervista al fondatore dell'azienda, l'app è stata testata dalla regione Umbria e sperimentata da alcune università italiane (https://forbes.it/2020/03/27/coronavirus-app-di-tracciamento-stop-covid-19/).
Intanto a quanto pare Webtek ha già sviluppato l'app in funzione multilingua, di modo da renderla fruibile anche in altri Stati (https://www.repubblica.it/economia/2020/03/17/news/app_coronavirus-251422094/).
SEDI WEBTEK:
- Via Stelvio 24, 23020 Poggiridenti Piano, Sondrio (sala KHub)
- Corso Europa 10, 20122 Milano
- Corso Matteotti 9, 23900 Lecco

Può usare il GPS anche un altro progetto di tracciamento dei contatti: quello sviluppato da **TeamSystem** (Via Sandro Pertini 88, 61122 Pesaro), azienda che sviluppa app, servizi e piattaforme digitali con 356mln di ricavi nel 2018 e circa 1,4 milioni di clienti.
Si chiama "**Healthy Workspace"** (https://www.teamsystem.com/teamsystem-hr-healthy-workspace). Vine dipinto dall'azienda come *"il software per la fase di riavvio delle imprese"*. Più che un'app, è appunto un software sviluppato per essere compreso da vari dispositivi di distanziamento, anche portabili. Si può integrare alle altre piattaforme gestionali di TeamSystem. Oltre a servire per la distanza corporea, rileva e misura la temperatura in fase di accesso sul luogo di lavoro, integrandosi con totem e telecamere termografici. Ha anche questionari automatizzati di

tracciamento per dipendenti e visitatori, da compilare prima di accedere sul luogo di lavoro e che saranno memorizzati sal sistema. Attraverso un portale, la direzione ed il medico competente controlleranno in tempo reale ingressi, misurazioni e adozione dei dispositivi di sicurezza.

L'app "**Sm_Covid19"** (https://www.smcovid19.org/) è sviluppata dall'azienda **SoftMining** (https://www.softmining.it/) che è una spin-off attiva nella sanità on-line e nella progfettazione di farmaci dell'**Università di Salerno.** Amministratore delegato di Softmining è **Stefano Piotto,** professore dell'Università di Salerno.
L'app è sviluppata sotto licenza del MIT (Massachusetts Institute of Tecnology). La sua tecnologia si basa sull'acquisizione dei dati provenienti da diversi sensori dello smartphone (bluetooth low energy ma anche nfc, Google nearby, ultrasuoni e wifi location, oltre a dati di posizione come il gps, la triangolazione delle celle telefoniche e il numero di telefono se si risulta positivi) per costruire una rete dei dispositivi che ha incrociato. Se l'app viene chiusa, si riavvia in automatico. La scansione avviene ogni 60 secondi anche con l'app in background. Propone un monitoraggio costante e permanente degli spostamenti del cittadino e di chiunque lo avvicini. A fine maggio aveva avuto circa 31.000 download.
Allo sviluppo di SM-COVID-19, oltre a SoftMining e Università di Salerno, hanno collaborato: Nexus TLC, MinervaS (TruckY), PushApp, Tolemaica, TTPoint, Digital Magics, Apple Academy, SPX Lab e Biovista (tratto da: https://www.smcovid19.org/team/).
CONTATTI:
Soft Mining: Via Tenente Corrado 22 - 83100 Avellino.
Nexus TLC, PMI attiva nell'ambito dell'internet delle cose: sedi in Via Salvo D'Acquisto 1, 80010 Quarto (NA) e Via Enrico Mattei 16, 25046 Cazzago San Martino (BS).
MinervaS (**TruckY**): TruckY è parte del Dipartimento di Ingegneria Industriale (DIIn) dell'Università degli Studi di Salerno (UNISA) – Università di Salerno, Via Giovanni Paolo II, 132, 84084 Fisciano (SA).
PushApp, software house che sviluppa applicazioni mobili: (https://www.pushapp.me/) sedi in Via Carlo de Cesare 64, 80132 Napoli e Via Gressoney 6, 20137 Milano.
Tolemaica, attiva in geolocalizzazioni: Via San Tommaso d'Aquino 67, 80133 Napoli (https://www.tolemaica.it/).
SPX Lab, società di marketing automation e consulenza software: Piazzetta Andorlini 1/5A, 16124 Genova
Biovista, azienda statunitense che lavora con i big di Biopharma: 2421 Ivy Road, Charlottesville, VA 22903, USA (https://www.biovista.com/).

L'**Istituto Zooprofilattico Sperimentale dell'Abruzzo e del Molise "G. Caporale"** (http://www.izs.it/IZS), che ha svariati laboratori e sedi dislocate nelle due regioni, ha sviluppato un'app per i dispositivi mobili, in grado di tracciare e controllare i casi di contagio da Covid19.
Il 25 marzo l'IZS-AM ha risposto alla call "Scheda Tecnica Tracciamento Contagio" di *Innova per l'Italia* – l'iniziativa del Ministero per l'Innovazione tecnologica e la Digitalizzazione, del Ministero per lo sviluppo Economico e del Ministero per l'Università e la ricerca – presentando **"EPIdemic Control" (EPIC)**, una app per dispositivi mobili per il contact tracking che funziona attraverso Bluetooth Low Energy e registra in maniera automatica e silente qualsiasi contatto ravvicinato con dispositivi dotati della stessa app nel range di alcuni metri. Un codice cifrato degli altri dispositivi e il periodo di contatto sono memorizzati nello smartphone per 21 giorni.
EPIC mette inoltre a disposizione dell'autorità sanitaria un'applicazione centralizzata per l'analisi dei dati che, in caso di positività confermata, consente di fornire un codice di sblocco per trasferire i dati dallo smartphone alle Autorità stesse, che potranno analizzare i contatti avuti negli ultimi 21 giorni dalla persona e mandare un messaggio che gli utenti riceveranno sulla app per seguire le indicazioni suggerite.

Il gruppo che ha sviluppato l'app è guidato dall'Ing. Luigi Possenti, responsabile del Centro Servizi Nazionale Anagrafi degli Animali dell'IZSAM (https://quotidianomolise.com/dal-molise-e-abruzzo-lapp-per-il-tracciamento-dei-casi-da-covid19/).

Un'altra azienda italiana che sta sviluppando tecnologie di contact tracing è la startup **Nextome**, una società barese nata nel 2013 (Via San Francesco 31, Conversano, Bari – https://www.nextome.net), specializzata nel tracciamento di oggetti in spazi chiusi, che già aveva lanciato in via sperimentale un sistema per tracciare i malati d'Alzheimer in una residenza per anziani e il tracciamento di un'altra patologia attraverso pazienti infetti. I software della statup funzionano sia con GPS che con standard Bluetooth Low Energy. Nextome afferma che il suo algoritmo di localizzazione ha un'accuratezza da 1,5 a 2 metri e spesso ha raggiunto fino a 0,5 metri di errore nelle prove sul campo. Integra Google Maps per attivare le mappe esterne quando l'utente si sposta da un'area interna su una esterna. La posizione viene quindi determinata direttamente sullo smartphone dell'utente e inviata regolarmente a un server. La tecnologia Nextome è brevettata negli Stati Uniti, in Europa e a Singapore. Nextome genera entrate fornendo soluzioni tecnologiche ai clienti commerciali.
Per uno dei fondatori, Domenico Colucci, il tracciamento funziona meglio con strumenti alternativi al telefonino: "*Lo smartphone ha molti dati personali. Noi abbiamo utilizzato dei braccialetti a batteria, di cui viene letto l'identificativo, per mantenere più alto il livello di riservatezza*". Come no! Molti suoi prodotti sono comunque brevettati per funzionare su smartphone.

Le catene della Grande Distribuzione Organizzata non sono state a guardare e stanno introducendo app di tracciamento e posizione per i loro punti vendita.
Coop e **Esselunga** hanno già introdotto app e piattaforme digitali per ridurre le lunghe attese e razionalizzare gli ingressi, proponendo una digitalizzazione degli ingressi per organizzare e smaltire le code. Coop ha presentato una piattaforma online, Esselunga una app.
All'Esselunga, in sette punti vendita (a Milano in via Feltre, viale Umbria, via Lorenteggio e, da ieri, via Losanna) è già disponibile la app "**Ufirst"**, che permette di prenotarsi sul momento o da casa: si forma una lista unica, che include chi si prenota da casa e chi sul posto, secondo un ordine progressivo. Poi il cliente riceve una notifica dall'app o un sms quando sta per arrivare il proprio turno: in questo modo, i clienti si recano all'ingresso solo quando arriva il momento di entrare.
"Ufirst è un'app che permette di evitare di perdere il tempo in fila: dal supermercato, al Comune, passando dall'ospedale agli ambulatori, fino ai negozi e alle stazioni ferroviarie", spiega Paolo Barletta, ideatore di Ufirst. *"Ufirst non solo rispetta la regola sulla distanza di sicurezza e sugli assembramenti, ma (…) inoltre con la nostra app, molte aziende potranno organizzare l'arrivo delle persone sul posto di lavoro"*
(https://www.vanityfair.it/lifestyle/hi-tech/2020/04/20/coronavirus-ufirst-app-fila-supermercati-negozi).
La piattaforma è nata nel 2015 e nel 2018 ha acquisito un'altra applicazione Italiana nel mondo degli "elimina code". Oggi Ufirst è il servizio più importante in Italia nella "gestione delle file". Ufirst è disponibile per oltre 600 punti in Italia, tra comuni, ospedali, farmacie, supermercati, soprattutto nel nord Italia.
A Milano, Ufirst ha addirittura offerto alle strutture aperte al pubblico, come negozi, farmacie, supermarket, studi medici, ambulatori ed uffici, il proprio software (*ufirst business*) gratuitamente fino al 30 giugno 2020, per gestire che le file formate dalle persone da remoto non formassero

assembramenti (https://www.repubblica.it/economia/2020/03/14/news/emergenza_coronavirus_l_app_per_prenotare_a_distanza_il_posto_in_fila_si_apre_gratuitamente_per_gestire_le_code-251208865).
Alla Coop (nei punti vendita Ipercoop Bonola, Piazza Lodi e Baggio, e nelle Coop Milano Palmanova e Milano Arona) è invece in funzione il servizio "**Cod@casa"**, stavolta una piattaforma online: ci si prenota in un orario e mostrando il codice (su cellulare o stampato) al personale all'esterno del negozio si può entrare saltando la fila. Dal 6 al 14 aprile sono state oltre 9 mila le prenotazioni effettuate. Il supermercato sta lavorando per estenderlo anche al resto della rete di vendita (https://www.vanityfair.it/news/cronache/2020/04/16/coronavirus-ecco-come-faremo-spesa).

"Filaindiana.it" è un'altra web-app interattiva, sviluppata da **Wiseair** (www.wiseair.it) start-up di sviluppo app, fondata nel 2018 da 8 studenti dei politecnici di Torino e Milano: Nicolò Alabastro, Pietro Avolio, Tommaso Ballardini, Fulvio Bambusi, Francesco Bertani, Francesco Cerizzi, Andrea Maioli e Andrea Torrone.
L'app mostra su una mappa i supermercati della zona per evitare code agli ingressi *"per evitare di andare a fare la spesa incontrando disagi, assembramenti e rischi di contagio"*.
Indica tempi di attesa previsti prima dell'ingresso e una stima in tempo reale del numero di persone in coda. Per ottenere le informazioni ci si reca sulla relativa pagina web. I dati provengono dagli utenti, un pulsante comunica al sistema che ci si trova proprio in quel luogo e si sta attendendo di entrare. L'app, che appena ci si connette parte in automatico tentando di accedere alla posizione, è disponibile sugli store di Google Play, attiva per ora solo in Lombardia e la maggior parte dei supermercati interessati sono situati nelle zone di Milano e hinterland (Il Comune di Milano la ha anche ufficialmente inserita tra i servizi di "Milano Aiuta"). Gli sviluppatori hanno già anticipato però di essere al lavoro per portare la propria opera al servizio di numerose altre zone (https://tech.fanpage.it/questa-mappa-ti-dice-quali-sono-i-supermercati-con-meno-coda-per-fare-la-spesa/).
Intanto Filaindiana si è estesa anche alla Francia, modificando per questo paese il proprio nome in Checkyoo (checkyoo.com).

Per consludere con questa carrellata indecente, citiamo **l'Università di Pavia** che ha ottenuto da **Facebook** all'inizio della pandemia da coronavirus i dati sugli spostamenti degli abitanti italiani a fini statistici. I ricercatori dell'università di Pavia, messi in contatto con Facebook all'inizio di marzo dal ministero dell'Innovazione italiano, attraverso un contratto di licenza, hanno ricevuto da Facebook i dati aggregati sulla mobilità dei suoi server attraverso un programma di mappe (https://dataforgood.fb.com/tools/disease-prevention-maps) che poi l'università di Pavia ha elaborato fornendo una collaborazione essenziale al gruppo di "esperti" nominati dal governo per individuare l'app nazionale di tracciamento italiana, "Immuni".
Tutto questo è avvenuto all'interno del programma ***Data for Good***, sponsorizzato dallo stesso patron di Facebook, Mark Zuckerberg, che mette a disposizione di università, ricercatori e non meglio identificate "organizzazioni non-profit" che hanno sottoscritto con il colosso dei social network l'accordo, una serie di dati utili che comprendono, come afferma lo stesso fondatore del social network, "*dati sulla* mobilità *e mappe sulla* densità della popolazione", ottenute integrando statistiche dei censimenti e immagini satellitari ma anche i flussi di post pubblici sul Covid-19,

diffusi su gruppi e pagine Facebook e da alcuni account di Instagram (attraverso CrownTangle live). I dati sulla mobilità forniti da *Data for Good* possono servire, secondo Facebook, durante catastrofi naturali oppure appunto durante le epidemie, per capire se le popolazioni stanno evacuando alcune zone. A quanto risulta, i dati forniti da Facebook comprendono anche le informazioni sugli spostamenti dal Nord al Sud Italia, avvenuti nella notte tra il 7 e l'8 marzo, quando il presidente del Consiglio, Giuseppe Conte, aveva annunciato la chiusura della Lombardia e di altre 14 province tra Veneto, Piemonte ed Emilia-Romagna (https://www.wired.it/internet/regole/2020/03/17/coronavirus-dati-facebook-privacy/?refresh_ce=).

***

REGIONE CHE VAI, APP CHE TROVI!
IL RUOLO DELLE REGIONI ITALIANE

Nella lotta al coronavirus le regioni italiane si sono mosse in ordine sparso
Alcune hanno già lanciato o selezionato una propria app per fare *contact tracing.*
Un "sovranismo regionale" dove ogni governatore di regione ha stabilito le sue ordinanze e sviluppato le sue diverse tipologie di controllo.

SARDEGNA - Tutto lo staff informatico regionale, che dall'inizio della crisi raccoglie su una piattaforma digitale regionale qualsiasi dato sui contagi e nel quale confluiscono anche le informazioni di quanti hanno dovuto autodenunciarsi in ingresso nell'isola, precisando il domicilio nel quale avrebbero trascorso la quarantena (circa 30mila persone, tra studenti fuorisede e vacanzieri) è stato coinvolto per creare una soluzione che consenta di monitorare la quarantena obbligatoria e georeferenziare gli spostamenti delle 26.127 persone entrate in Sardegna dall'inizio dell'emergenza, prima e dopo il primo DPCM del 9 marzo.
Una piattaforma informatica avanzata, sul modello coreano e cinese, per difendere lo status di Isola "felice", dato che dal punto di vista della diffusione epidemiologica la Sardegna è infatti stata una delle regioni meno colpite dal Covid19. Si è scritto che sistema è stato capace di tenere la situazione sotto controllo minuto per minuto, comune per comune, con approssimazione fino al numero civico.
La app si chiama **Covid 19 Regione Sardegna**, scaricabile su Android e su IOS. Il 24 marzo in conferenza stampa è stato il presidente della giunta regionale, Christian Solinas, ad assicurare che il servizio di geolocalizzazione volontaria sia sbarcato nell'isola. Il sistema di tracciamento è messo a punto da **SardegnaIt,** società *in house* della Regione: "s*tiamo lavorando su due binari: uno è il tracciamento dei dati aggregati forniti da una delle principali compagnie telefoniche (…). Dall'altra c'è il progetto di geolocalizzazione volontaria che si basa sulla disponibilità del cittadino a fornire i dati" (*https://www.wired.it/internet/web/2020/03/28/coronavirus-regioni-tracciamento-privacy/?refresh_ce).
Chi è arrivato nell'Isola, compresi i sardi rientrati, dovuto utilizzarla per compilare il modulo dove indicare il domicilio in cui trascorrere il periodo di quarantena.

Tutti i soggetti in arrivo in Sardegna dal territorio nazionale o dall'estero, e quelli arrivati successivamente al 23 febbraio 2020 dalle zone rosse di cui al DPCM del 8 marzo 2020, hanno avuto l'obbligo di compilare l'autodichiarazione, anche tramite app. Dato che non è stato ancora attuato un decreto del governo per consentire il trattamento dei dati sanitari, il presidente della Regione Sardegna non ha potuto chiedere ai viaggiatori di informare ogni giorno attraverso la app su eventuali sintomi ma, in forza del decreto legge del 9 marzo per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza Covid-19, è stato possibile chiedere il consenso alla geolocalizzazione.
Le informazioni sono state condivise con le Prefetture e gli uffici epidemiologici della sanità regionale, così da verificare se le persone rispettavano effettivamente l'isolamento domiciliare, ma anche per individuare eventuali zone in cui fosse riscontrata una particolare concentrazione di positivi. Il tracciamento ha permesso anche di pianificare i controlli delle forze dell'ordine in vari punti della regione: sono stati resi operativi anche 1.300 agenti della Forestale per garantire il rispetto delle quarantene.
La volontà del presidente della regione, Christian Solinas, sarebbe stata quella di aggiornare la piattaforma per ottenere la comunicazione in tempo reale con i sindaci e con le polizie municipali, il censimento di farmacie e market per la consegne a domicilio e la gestione dei posti letto da remoto attraverso il monitoraggio dell'occupazione in ciascuna struttura ospedaliera (https://www.ansa.it/sardegna/notizie/2020/03/23/coronavirus-regione-26mila-arrivi-tracciabili-con-una-app_f0eba568-b5c2-4c05-979d-1319f0154f10.html).

LOMBARDIA - La Lombardia, la regione più colpita dall'epidemia da coronavirus, è stata anche la prima a sviluppare un sistema di monitoraggio della popolazione, della quale ha seguito gli spostamenti grazie al segnale lasciato dei telefoni cellulari. Si tratta di informazioni aggregate che gli operatori telefonici forniscono – generalmente a pagamento – per finalità di marketing.
La Regione ha acquisito i datiaggregati (solo i numeri, senza nominativi) di Vodafone e Tim sul numero di telefonini che si agganciavano alle antenne. Questo accade perché mentre ci muoviamo, per continuare a funzionare il telefonino passa da una porzione di rete all'altra — le celle, appunto — e così gli operatori telefonici, e le autorità che ne fanno richiesta, poi possono sapere quante persone si sono spostate da un luogo a un altro. Ogni cella viene alimentata da una stazione di telecomunicazione, quella che comunemente chiamiamo antenna, e da ripetitori. Muovendoci lungo le strade della nostra città, il telefono capta il segnale irradiato dall'antenna e rimane nella sua cella finché, allontanandosi, non si avvicina a un segnale più potente del precedente ed "entra" in un'altra cella. La portata dello spazio tra una cella e l'altra è di circa 300-500 metri. Per avere un'idea di quante ce ne siano in Italia possiamo consultare il sito Cellmapper che le mostra su una mappa.
Grazie alle celle quindi si può quindi già localizzare la posizione di un telefono e l'utente non può fare nulla per impedirlo se non spegnere il telefono quando esce di casa o non portarlo con sé.
Antenne e ripetitori infatti sono in grado di misurare la distanza da un cellulare calcolando l'intensità del segnale: più è debole, più è lontano. Se una sola cella permette di conoscere se siamo entro il raggio di una certa antenna o di un ripetitore, facendo una triangolazione tra tre o più di essi si può conoscere la posizione più o meno precisa. Una soluzione a cui stanno ricorrendo anche molti governi all'estero e la stessa Commissione europea, che ha arruolato Vodafone, Deutsche Telekom, Orange, Telefónica, Telenor, A1 Telekom Austria e Telia. In Italia anche TIM-Telecom Italia e Vodafone hanno fornito questi dati.
L'esperienza lombarda è derivata da Expo e dall'analisi di flussi intorno e all'interno della fiera.
Le più grandi compagnie telefoniche italiane – Tim, Vodafone, Wind Tre e Fastweb – avevano

offerto, tramite la loro associazione di categoria **ASSTEL**, la diponibilità a fornire i dati sugli spostamenti dei propri utenti (https://www.corriere.it/cronache/20_marzo_17/coronavirus-cosi-lombardia-controlla-movimenti-via-cellulare-75c3d226-6897-11ea-9725-c592292e4a85.shtml).
Per quanto riguarda la triangolazione con le celle, questa è comunque molto approssimativa, con margini d'errore anche di centinaia di metri (lo dimostrano anche tanti casi giudiziari) che varia a seconda di dove la persona si trova. Le città, per esempio, sono coperte da microcelle che permettono una localizzazione più precisa, hanno decine o anche centinaia di stazioni. Negli spazi aperti o poco abitati, questo metodo invece è più fallace ed è possibile spostarsi per chilometri senza essere rilevati. Troppo complicato, quindi, invece con una app di tracciamento si risolvono tutti i problemi. Basta scaricarla sul proprio cellulare ed il gioco è fatto!
Dalle rilevazioni con le celle telefoniche in Lombardia, dopo i furibondi appelli a "restare a casa", era risultato comunque che la gran parte degli spostamenti avvenisse tra le 18 e le 19 e, in misura minore alle 12 e alle 13. Orari compatibili con gli spostamenti dovuti per le attività lavorative.
In Lombardia è anche stata lanciata un'apposita app regionale, **"AllertaLom"** della digital company della regione Lombardia, **ARIA S.p.A.,** Azienda Regionale per l'Innovazione e gli Acquisti. L'applicazione lombarda, già utilizzata per le allerte di Protezione Civile, non fa che diffondere un questionario sanitario a distanza che le persone devono compilare: in base a quelle informazioni l'organizzazione sanitaria prenderà provvedimenti per il contenimento mirato. Sono stati raccolti oltre 2 milioni di questionari. Ogni utente è infatti invitato a compilare il questionario più volte. La Regione aveva mandato anche degli SMS di massa sui cellulari dei residenti per consigliare lo scaricamento dell'app. A fine marzo l'app era stata scaricata da oltre 800.000 persone (https://www.regione.lombardia.it/wps/portal/istituzionale/HP/DettaglioRedazionale/servizi-e-informazioni/cittadini/salute-e-prevenzione/coronavirus/app-coronavirus).

UMBRIA - la Regione, sull'esempio della Lombardia, si è messa a studiare anch'essa i flussi delle celle telefoniche. I dati sono stati forniti da Tim e Vodafone. Ma l'Umbria ha anche pensato di introdurre un'app di tracciamento dei contatti: "**StopCovid19"**, sviluppata dalla società di Sondrio, **Webtek**, tra quelle che erano già disponibili sul mercato. L'app consente di ricostruire l'intera catena di contatti di una persona collegando gli altri dispositivi a cui è stata vicina per mezzo della localizzazione con GPS.

LAZIO - In Lazio l'app si chiama **"LazioDrCovid"** (http://www.regione.lazio.it/rl/coronavirus/scarica-app/) e mette in contatto chi ha sintomi riconducibili al coronavirus, o sono stati in contatto con persone affette, con il proprio medico di base. Non fa quindi vero tracciamento ma piuttosto funziona come diario clinico.

Il Comune di Roma Capitale ha invece inaugurato un portale su Internet nel quale segnalare "*assembramenti di persone che ritieni in contrasto con le regole dell'emergenza sanitaria": i*l Servizio unico segnalazioni (Sus) o delazioni.
Già nell'aprile del 2017, l'odierno segretario del Partito Democratico, Nicola Zingaretti, nelle veste di presidente della Regione Lazio, presentò la nuova App scaricabile gratuitamente **"SaluteLazio"** realizzata da LAZIOcrea, per consultare su mappa, con GPS, le strutture sanitarie più vicine presenti nel territorio laziale: Pronto Soccorso, Ambulatori di cure primarie, Centri vaccinali, Case della Salute, Guardia Medica e Farmacie di Roma e Provincia. L'App informa sul numero di pazienti in attesa, in trattamento e in osservazione breve, suddivisi per codice di triage. In questo modo è possibile consultare il numero e l'indice di accessi di ogni singola struttura in base al grado

di affluenza (https://www.agi.it/regioni/lazio/sanita_zingaretti_presenta_nuova_app_salute_lazio-1673351/news/2017-04-11/).

LIGURIA – Nel Comune di **Genova** si è seguita la strada della Regione Lombardia, facendo ricorso ai dati aggregati delle celle telefoniche, forniti dagli operatori telefonici. Il presidente della Regione Liguria Giovanni Toti pensa anche a un braccialetto per tutti i bagnanti e frequentatori delle spiagge regionali, che emetta un suono o una vibrazione quando ci si avvicina ad un altra persona.

TOSCANA - La tattica della Regione guidata da Enrico Rossi punta sui QR Code. L'infermiere ne fornisce uno al paziente, che può essere adoperato col cellulare per comunicare i parametri dello stato di salute.

VENETO - Tracciare tutti e rivolgersi a Israele per la "*verifica degli spostamenti con controlli intelligenti*", ecco quale avrebbe dovuto essere la ricetta per il presidente del Veneto, Luca Zaia. "O la rendiamo obbligatoria o, altrimenti, la app non funziona (…) Secondo me quando le forze dell'ordine ci fermeranno dovranno verificare se abbiamo la mascherina, i guanti e anche la app accesa" (https://www.genteveneta.it/attualita/coronavirus-zaia-la-app-va-resa-obbligatoria-per-funzionare-deve-averla-il-60-degli-italiani/).
Il presidente della Regione veneto, il leghista Luca Zaia, aveva annunciato la creazione di una app regionale, precisando che sarebbe stata obbligatoria. La app veneta, a quanto riferito dallo stesso Zaia, doveva essere scaricabile gratuitamente, bisognava registrarsi inserendo la mail e codice fiscale e funzionava con tecnologia Bluetooth, registrando gli incontri di due smartphone di una durata maggiore di 15 minuti a una distanza inferiore ai due metri. Qualora una persona risultasse positiva, tramite l'app doveva essere possibile tradurre quei codici numerici in nomi e cognomi, per mappare i contatti e sottoporli a tampone. Alla faccia dell'anonimato. Sarebbe bello sapere come avrebbe fatto chi non ha uno smartphone.Condannato a rimanere in casa o la Regione gli avrebbe comperato il telefonino nuovo?

SICILIA - "Sicilia si cura" è l'app di tracciamento siciliana

CAMPANIA - Anche la Campania del governatore De Luca ha una sua app smartphone. Questa per monitorare l'utilizzo di posti letto utilizzati per il Coronavirus. Si tratta di una applicazione del genere Gis (geographic information system) e serve a tracciare una mappa partendo da dati geolocalizzati e a condividere queste informazioni con terzi che hanno i privilegi d'accesso a questa applicazione e che in questo caso saranno la "task force" regionale per il Coronavirus e le Direzioni ospedaliere. La Regione Campania ha avviato la realizzazione dell'app col supporto tecnico-operativo di **Soresa** nel ruolo di advisor tecnologico (https://napoli.fanpage.it/anche-la-campania-avra-la-sua-app-covid-19-servira-a-monitorare-i-posti-in-terapia-intensiva/)
Il governatore della Campania, De Luca, ha più volte minacciato la chiusura delle frontiere regionali perché: "Il virus degli altri non lo vogliamo".

EMILIA ROMAGNA - c'è da tempo la "**App ER-Salute"**. Registrandosi consente di accedere da dispositivi mobili al sistema di prenotazione e pagamento on line delle prestazioni erogate dalle Aziende sanitarie della Regione Emilia-Romagna

(https://support.fascicolo-sanitario.it/guida/accesso-mobile/app-er-salute)

Ci sono infine le webb-app che i vari Comuni stanno introducendo per controllare e contingentare le modalità di accesso alle spiagge delle località turistiche e dei litorali italiani, con predilezione per le spiagge libere, da sempre usate da chi non ha i soldi per permettersi di passare l'estate negli stabilimenti balneari:

A **Roma** è presente, ma non funzionante l'applicazione **"Seapass"** che il Comune ha adottato per monitorare la capienza delle spiagge libere, ai tempi del coronavirus, per i lidi di Ostia, Capocotta e Catelporziano. Si basa su suddivisione per numeri e colori, con ogni spiaggia denominata con varie sfumature (gialla, rosa, ocra e così via). Il «semaforo» che appare per ogni lido dovrebbe segnalare la disponibilità dei posti in spiaggia. In realtà si tratta al momento di un sito web più che di una App da scaricare su cellulari e tablet: www.seapassroma.it

A **Genova**, in tutte le spiagge libere, a partire dal 6 giugno, oltre ai presidi fissi per il conteggio degli ingressi contingentati, si prevede di introdurre l'app-web **"SpiaggiaTi"**, che in tempo reale indica i posti disponibili in ogni spiaggia. A ogni spiaggia è assegnato un segnaposto virtuale, contrassegnato da un bollino, che è blu quando ci sono ancora posti disponibili e diventa rosso quando si esauriscono. Così è possibile avere una visione di quali sono le spiagge ancora disponibili in blu. Cliccando sul segnaposto della spiaggia desiderata si apre una finestra con una foto della stessa e con i dati puntuali sul numero di persone presenti e posti disponibili. Inoltre è presente la funzione aggiuntiva e facoltativa "Come arrivare": se l'utente dà l'autorizzazione, l'app elabora il percorso con Google Maps. Viene richiesta la posizione GPS. L'applicazione è già disponibile sul Play Store di Androd e presto lo sarà anche sull'Apple Store (https://www.ilsecoloxix.it/genova/2020/05/29/news/spiagge-libere-a-genova-conteggio-degli-ingressi-e-prenotazione-con-l-app-ecco-l-elenco-di-quelle-che-aprono-domani-1.38904594).

A **Napoli**, invece, c'è "**LIDOO"** app-web sviluppata da **Maylab**, startup napoletana, con cui prenotare il posto in uno stabilimento balneare e i relativi servizi. Per accedere alle spiagge di Napoli si potrà accedere prenotando ombrelloni e lettini online, tramite un'apposita app. Scansionare un QRcode presente sullo smartphone dal lettore presente all'ingresso dello stabilimento si avrà accesso al proprio posto prenotato, e il pagamento sarà gestito on line. Si prefigge di essere di supporto ai gestori degli stabilimenti oltre che agli enti pubblici che vorranno aderire. La piattaforma, infatti, oltre agli stabilimenti privati ospiterà anche le spiagge libere comunali (https://www.vesuviolive.it/vesuvio-e-dintorni/341621-lidoo-posto-spiaggia).
Un'altra app, già in utilizzo dal 2011 per visite guidate, concerti ed altri eventi, sarà estesa anche al settore balneare e permetterà di regolamentare l'accesso alle spiagge libere comunali: *"Ai prenotati sarà rilasciato un codice. Il sistema bloccherà le prenotazioni multiple dello stesso nominativo per più spiagge. Oltre a quelle di chi, pur avendo riservato il proprio posto, non si presenterà in spiaggia, provocando un danno agli altri. L'elenco giornaliero degli accessi sarà inviato anche ai gestori dei lidi confinanti, nel caso in cui bisognerebbe attraversarli per poter raggiungere le spiagge comunali di Napoli (…) L'app ha ottenuto l'approvazione anche di alcuni gestori di lidi privati"* (https://www.vesuviolive.it/ultime-notizie/341380-spiagge-napoli-app-comune).

A **Ravenna**, invece, ancora prima dell'app Immuni, da metà aprile una speciale task force ristretta della Polizia Municipale, nell'ambito di un progetto coordinato dalla Prefettura, si è mossa sfruttando l'utilizzo delle tecnologie già disponibili, ovvero videochiamate, foto col cellulare e

geolocalizzazioni tramite Google Maps e WhatsApp per monitorare le persone in quarantena. A fornire i contatti delle persone sotto monitoraggio è l'Ausl stessa, che attraverso la propria banca dati indica i nominativi delle persone risultate positive al virus. In base a quelli, i pubblici ufficiali incaricati di vigilare sul rispetto delle norme effettuano l'accertamento da remoto. Il primo tentativo, se l'utente ha il telefono fisso, è fatto chiamando sulla linea di casa; in caso di risposta appare praticamente scontato che chi si trova dall'altra parte della cornetta stia rispettando le prescrizioni. In alternativa, gli agenti possono videochiamare le persone e chiedere loro di mostrare particolari dell'abitazione che certifichino la loro effettiva permanenza in casa, con un selfie o una videochiamata per dimostrare di trovarsi in un contesto domestico, oppure attraverso l'invio della posizione sfruttando le applicazioni che consentono la localizzazione, appunto come WhatsApp e Google Maps (https://corrieredibologna.corriere.it/bologna/cronaca/20_aprile_14/a-ravenna-primo-esperimento-tracciamento-persone-quarantena-cd714aa2-7e5f-11ea-9291-3792686542db.shtmlù).

Ma App e smartphone sono stati scelti come strumenti anche per distribuire, tramite graduatoria, i cosiddetti "buoni-spesa" dell'ordinanza "cura-italia" (i 400 milioni di euro stanziati dal governo per chi si è trovato senza reddito a marzo).
Ecco le soluzioni dei Comuni di Milano e Roma per erogare il buono.
A **Milano** l'erogazione dei buoni spesa poteva avvenire solo previo utilizzo di applicazione **SATISPAY** su smartphone. Il beneficiario poteva spendere il buono nei punti vendita che aderiscono al circuito, con un elenco pubblicato sul sito del Comune, oltre ad essere visibile sulla stessa app. L'alternativa era quella di utilizzare la carta prepagata SOLDO utilizzabile nel circuito MASTERCARD. Sia Soldo che Satispay hanno offerto la disponibilità delle proprie piattaforme a costo zero per il Comune (ma non a profitto zero per loro).
A **Roma**, invece, chi aveva diritto ai "buoni-spesa" poteva scegliere se scaricare l'applicazione "**TR Roma Capitale**" sul cellulare da un apposito sito (www.edenred.it/innovazione/scarica-app/ticket-restaurant/) o aspettare la distribuzione dei buoni cartacei a casa ma la procedura era molto più lunga (https://www.key4biz.it/buono-spesa-con-carta-prepagata-o-app-le-soluzioni-digitali-di-milano-e-roma-video/300598/).

***

IL CONSORZIO EUROPEO PEPP-PT

L'intero piano delle app nazionali di contact tracing avrebbe dovuto coagularsi attorno ad un consorzio europeo nato ad inizio aprile: il **Consorzio Pepp-PT (Pan-European Privacy-Preserving Proximity Tracing)**, inquadrato come una organizzazione senza scopo di lucro in Svizzera. Lo scopo: facilitare il lancio di app nazionali in tutta Europa in grado di comunicare tra loro.
Una simile proposta era stata fatta anche dal Gruppo dei Garanti europei della Privacy e dalla stessa Commissione Europea. Il Garante della Privacy europeo, Wojciech Wiewiorowski, ha sostenuto che questa fosse l'unica soluzione percorribile.

Al Consorzio PEPP-PT, finanziato da donazioni private, ha partecipato un team di ricercatori di otto paesi europei (Italia, Francia, Austria, Belgio, Danimarca, Svizzera, Spagna e Germania) che si è avvalso della collaborazione di oltre 130 accademici e tecnici e di una trentina fra aziende e istituti di ricerca, molti dei quali come vedremo hanno abbandonato il progetto nel corso del tempo.
Il lavoro collettivo ha portato alla pubblicazione di un protocollo standard per il tracciamento, un codice per app che analizza i segnali Bluetooth tra cellulari. *"Il nostro obiettivo è rendere questa tecnologia disponibile per tutti i paesi, i gestori delle risposte alle malattie infettive e gli sviluppatori nel modo più rapido e semplice possibile"*, si legge sul sito del consorzio (https://www.pepp-pt.org). Il sistema PEPP-PT infatti *"può essere utilizzato anche quando si viaggia tra i paesi"*.
Il ruolo preminente è stato assunto fin dall'inizio da esperti, istituti e società tedesche. I più impegnati sono stati Thomas Wiegand, direttore del **Fraunhofer Heinrich-Hertz-Institut (HHI)** al Politecnico di Berlino, Lothar Wieler, presidente del **Robert Koch-Institut**, che coordina la risposta di Berlino alla pandemia, che ha spinto fino alla fine per far sì che la Germania fosse fra i primi Paesi a lanciare l'idea di un'app per il contact tracing e Hans-Christian Boos, amministratore delegato di **Arago**, società di automazione aziendale ed intelligenza artificiale con sede a Berlino, che è stato uno dei principali promotori del progetto.
Hans-Christian "Chris" Boos, il cervello che sta dietro al consorzio Pepp-PT, è un'imprenditore cinquantenne molto noto nella scena delle start-up tedesche e dall'agosto 2018 è stato uno dei nove membri del consiglio per la politica digitale della cancelleria tedesca.
Nel sito della società con sede a Francoforte, si legge che "Arago è orgogliosa di essere membro e fornitore di tecnologia (la tecnologia grafica e dei server dal suo motore di automazione della conoscenza HIRO) all'iniziativa paneuropea per il rispetto della privacy PEPP-PT" (*https://hiroai.co/pan-european-privacy-preserving-proximity-testing/*).
Altri istituti tedeschi parte di Pepp-PT sono il Tecnical University di Berlino, TU Dresden e University of Erfurt.
Fra le organizzazioni coinvolte all'inizio del progetto sono state anche l'Ecole Polytechnique Fédérale di Zurigo e Losanna in Svizzera, il Politecnico di Lovanio, la Danmarks Tekniske Universitet, il Politecnico di Linz, lo European Laboratory for Learning andIntelligent Systems, Heartbeat Labs, PocketCampus, 3db, Dolphin, le francesi Acticom, Ubique e Inria - Institut National de Recherche en Sciences et Technologies du Numérique, e per l'Italia Bending Spoons, sviluppatrice di Immuni, e la Fondazione Isi di Torino (Isi Foundation).
Un grosso ruolo, anche se defilato, lo gioca il gruppo **Vodafone**.
La comunicazione di Pepp-Pt è invece curata dal colosso Hering Schuppener.
Presente agli incontri online del Pepp-PT, anche Paolo De Rosa, il capo delle funzioni tecnologiche (Chief Tecnology Officer) del Ministero dell'Innovazione italiano, che in passato aveva reso noto come l'app nazionale italiana Immuni potesse essere realizzata sulla base del protocollo di Pepp-PT.
Particolare da non dimenticare, il Consorzio PEPP-PT non è un progetto pubblico ma un raggruppamento di ricercatori e imprese private sebbene la Commissione europea lo abbia esplicitamente menzionato tra le iniziative di interesse nelle proprie linee guida.
Da quanto si sa, questo Consorzio era stato scelto come partner (vedremo in seguito perché diciamo "era") proprio perché modulato per rispettare le linee guida di cui sopra, ovvero protocollo basato su tecnologia Bluetooth, interoperabilità a livello comunitario, scaricabilità su base volontaria e almeno ufficialmente rispettoso della privacy.
Il progetto PEPP-PT è simile al protocollo di tracciamento *BlueTrace/OpenTrace* in uso per l'app "*TraceTogether"* a Singapore ed usando i codici dei paesi può funzionare oltre i confini.

La documentazione di Pepp-PT è stata pubblicata su GitHub: https://github.com/pepp-pt/pepp-pt-documentation
L'istituto di ricerca tedesco Fraunhofer Heinrich Hertz Institute ha lavorato sulla piattaforma tecnologica assieme a Vodafone e altri, reclutando volontari dell'esercito tedesco per misurare il modo in cui i diversi marchi di smartphone comunicano tra loro (https://www.reuters.com/article/us-health-coronavirus-europe-tech/europe-to-launch-coronavirus-contact-tracing-app-initiative-idUSKBN21J4HI).
Il progetto originario del Consorzio Pepp-PT avrebbe dovuto dunque seguire l'approccio della decentralizzazione per quanto riguarda l'archiviazione dei dati tracciati. Avrebbe dovuto cioè non avvalersi di un database centralizzato (server) ma archiviare le informazioni solamente sullo smartphone (approccio decentralizzato).
La Risoluzione del Parlamento europeo del 15 aprile (n.2020/2616(RSP)) aveva chiesto, infatti, espressamente "*che la memorizzazione dei dati sia completamente decentralizzata*" (punto 41).
Ma date le spinte dei singoli paesi, a cominciare dalla Francia ed inizialmente dalla Germania che avrebbero preferito il modello centralizzato sui server da loro gestiti, il Consorzio aveva ripensato l'intero protocollo per affiancare i due approcci, modello centralizzato e modello decentralizzato, con dati archiviati sia sul cellulare che sul server centrale.
La scelta di un approccio "misto" con inclinazione verso la soluzione centralizzata era stata anticipato dalle parole di Christian Boos: *"Un modello centralizzato offre potenzialmente una gestione di gran lunga migliore della pandemia senza infrazioni della privacy. Sarà però una scelta dei singoli stati. È possibile raccogliere gli stessi dati con un modello decentralizzato, cambia solo che più persone dovranno veicolare le informazioni a proposito dei soggetti infetti"* (https://www.punto-informatico.it/pepp-pt-google-apple-app-covid19/).
La scelta di virare verso un modello centralizzato ha provocato però molte critiche tra coloro che si ergono a difensori della privacy ed ha causato la rottura con il progetto che aveva sviluppato lo standard **DP-3T** (**Decentralised Privacy-Preserving Proximity Tracing)**, che fin dall'inizio faceva parte del consorzio e che, separandosene, ha proseguito nello sviluppo di un modello di archiviazione decentralizzato.
Di fatto, ad oggi esistono quindi due standard europei: il modello che offre soluzioni sia decentralizzate che centralizzate su server (quello proposto da PEPP-PT) e l'altro modello apparentemente ancora più decentralizzato con i contatti avuti tra smartphone archiviati "ufficialmente" solo sui singoli cellulari (quello proprosto da DP-3T).
Ma cosa dicono le regole dell'EDPB sull'archiviazione dei dati? Dicono che vanno bene entrambi i modelli, con una preferenza per la decentralizzazione: *"sono previste due opzioni principali: archiviazione locale dei dati all'interno dei dispositivi degli utenti o conservazione centralizzata. L'EDPB è del parere che entrambe possano essere valide alternative, purché con una sicurezza adeguata. Diverse entità possono anche essere considerate responsabili del trattamento a seconda dell'obiettivo finale dell'app (ad es. il titolare del trattamento e dei dati trattati possono essere diversi se l'obiettivo è fornire informazioni in-app o contattare la persona al telefono). In qualunque caso, l'EDPB vuole sottolineare che la soluzione decentralizzata è più in linea con il principio della minimizzazione"* (https://www.key4biz.it/contact-tracing-le-linee-guida-dei-garanti-privacy-ue-per-le-app-anti-covid-19/300368/).
Ma anche una parte consistente del mondo scientifico è orientata verso l'approccio decentralizzato. Tra questi citiamo la *Nexa Center for Internet and Society* del **Politecnico di Torino**, a cui hanno aderito accademici ed esperti di fama europea.
A questo punto, però, occorre spendere qualche parola in più rispetto al significato dei due termini,

centralizzato e decentralizzato.
Cosa significa approccio centralizzato?
Nell'approccio centralizzato il server centrale a cui la app si appoggia, che può essere un server dello Stato oppure gestito da una società privata, assegna a ogni dispositivo un numero o codice identificativo casuale. Questi codici vengono archiviati tutti sul server centrale, che li conserva. È sostanzialmente un data-base, un "cervellone" che ha disposizione tutte le informazioni del tracciamento fatto dall'app. Quando un utilizzatore risulta positivo avvisa l'app che è stato contagiato. Facendo questa operazione invia al server tutti i codici casuali ricevuti dai cellulari che ha incontrato nei giorni precedenti. A quel punto, il server centrale incrocia i codici scambiati dallo smartphone dell'ammalato con quelli ricevuti ed elabora un profilo di rischio per ogni persona. Maggiore è il numero di codici scambiati, più è alto il profilo di rischio. Superata una certa soglia, il server centrale invia una notifica sull'app delle persone avvisandole del pericolo.
Il server centrale è dunque a conoscenza del codice identificativo iniziale dell'utilizzatore dell'app ed anche qual'è il cellulare a cui l'ha mandato e accumula le segnalazioni dei positivi e di chi è venuto in contatto con loro. Nella pratica, entrando nel "cervellone", è possibile venire a conoscenza di tutte le interazioni delle persone contagiate e di quelle che sono entrate in contatto con loro.
Come funziona invece un'app con approccio decentralizzato?
Il server centrale anche in questo caso è presente ma, a differenza dell'approccio centralizzato, non assegna nessun codice identificativo a chi ha installato l'app. È il telefono sul quale è installata l'app a trasmettere dei codici casuali tramite Bluetooth ogni "tot" di minuti agli altri cellulari nei paraggi. Se nelle vicinanze c'è un'altra persona che ha scaricato l'app i loro cellulari si scambiano questi codici e teoricamente solo sui telefoni dovrebbe restare traccia di questo scambio. Gli unici codici salvati sul server sono quelli che il possessore del cellulare carica, si dice volontariamente, dopo essere risultato positivo al virus dopo il test e aver ricevuto un apposito codice dalle autorità sanitarie: solo a questo punto sul server centrale viene caricata la lista coi codici inviati dal cellulare del malato agli altri cellulari. Il server centrale segnala quindi alle app scaricate sui singoli cellulari quali sono i codici che ha ricevuto dall'ammalato. A questo punto ognuno può confrontare i codici di contatto pubblicati sulla propria lista sul cellulare. Se ci sono degli abbinamenti, significa che si è stati nelle vicinanze di un individuo risultato pisitivo.
La differenza con il modello centralizzato è quindi l'assegnazione dei codici identificativi (fatta dall'app e non dal server), la segnalazione al server solo dei propri codici inviati (e non anche di tutti quelli ricevuti) e il luogo dove avviene l'incrocio dei dati (direttamente sullo smartphone e non nel server centrale).
Va chiarito subito, però, che se anche può sembrare che il metodo decentralizzato possa offrire più garanzie di sicurezza, nessuno dei due metodi è davvero immune da rischi. L'approccio centralizzato presenta per forza di cose maggiori rischi perché ha un unico "cervellone" dove vengono aggregati i dati e dove questi sono disponibili. In quello decentralizzato, però, non esiste un punto vulnerabile perché ce ne sono molti. La vulnerabilità è data dagli stessi cellulari, da cui come sappiamo bene è sempre possibile appropriarsi di dati ed informazioni. In più nel metodo decentralizzato si fa affidamento sui sistemi operativi che amministrano e governano i cellulari, che come sappiamo sono di proprietà di multinazionali come Apple e Google.
Se nel metodo centralizzato i nostri dati finiscono per essere controllati dallo Stato, nel metodo decentralizzato lo possono essere dai sistemi operativi di queste società private. Sia l'una che l'altra, prassi che vorremmo evitare.
Per realizzare la creazione di comuni standard informatici europei per il contact tracing, quindi, due

principali scuole di pensiero si sono contese il primato: Pepp-PT, che si basa su un'archiviazione dei dati più centralizzata o comunque "mista", contro DP-3T, creatura dei politecnici di Losanna e Zurigo (Svizzera) e basato su un'archiviazione più decentralizzata (altri standard per protocolli decentralizzati oltre a DP-3T, includono "Whisper Tracing Protocol" della Coalition Network della California, "OpenCovidTrace" che usa gli aggregatori Apple/Google/DP-3T ed è composto da una piattaforma indipendente della comunità open-source guidata da Nebula Ventures, "SafePaths" del MIT Media Lab di Boston, che collabora con Microsoft ed una serie di università americane, ed infine il "Protocollo TCN" del gruppo mondiale federato di giovani tecnologi della TNC Coalition, di cui tra l'altro fa parte sempre la Coalition Network).
Ma dato che, come dice il proverbio, trai due litiganti il terzo gode, a fare la differenza è stata la scelta fatta da Google e Apple di unire le forze per arrivare ad un'interoperabilità delle app sui rispettivi sistemi operativi (che insieme costituiscono il 99,29% dei sistemi operativi usati a livello mondiale). Le due multinazionali per offrire la loro soluzione hanno posto come condizione non negoziabile l'archiviazione decentralizzata, sposando in pieno lo standard di DP-3T.
Intanto sulla base del protocollo di PEPP-PT, a partire dal 23 aprile è emersa una versione tedesca, indicata come PEPP-PT NTK (https://nadim.computer/res/pdf/PEPP-PT_NTK_High_Level_Overview.pdf), ed una versione francese chiamata ROBERT, sorta dalla collaborazione tra il Fraunhofer Heinrich Hertz Institut (HII) e la partecipata statale francese per il digitale INRIA. Le due versioni funzionano in background anche quando il telefono è bloccato e prevedono un approccio centralizzato su un server, ed in pratica sono la stessa cosa con due nomi diversi.
Ma a giugno, ufficialmente, anche la Germania sé passata al sistema decentrato con l'app "Corona-warn-app", mollando il consorzio Pepp-Pt a favore dello schema Google-Apple. Il governo tedesco ha innanzitutto cominciato con l'escludere il Fraunhofer Insitut, propugnatore di un approccio centralizzato, dal progetto nazionale tedesco. Quindi il Fraunhofer Insitut al momento sta lavorando solo a "ROBERT", la variante francese di Pepp-PT, che dovrebbe essere adoperata per far funzionare l'app francese "Stop-Covid" (https://www.startmag.it/innovazione/come-germania-e-francia-traballano-app-di-tracciamento-covid-19/).
Uno dopo l'altro i vari Stati stanno andando tutti in questa direzione, o quasi.
Anche l'Italia, dove la società che ha creato Immuni prima ha abbandonato Pepp-PT e poi ha abbracciato la soluzione di Apple e Google, anche se **Paolo de Rosa,** responsabile tecnologico del dipartimento della ministra dell'Innovazione Paola Pisano e uno dei tre coordinatori della task force che ha scelto Immuni, per tenere il piede in più staffe ha voluto far sapere che in un incontro fra i ministri Ue "è stato ribadito il pieno sostegno dell'Italia a un approccio europeo comune; intanto c'è una continua cooperazione con tutti, da Pepp-Pt a Dp-3t" (https://www.corriere.it/tecnologia/20_maggio_09/app-immuni-de-rosa-pronti-fine-mese-sogei-garante-sicurezza-327c2c4a-91c6-11ea-9f60-1b8d14bed082.shtml?refresh_ce-cp).
Ma ormai i giochi sono fatti. Pepp-PT doveva essere il punto di partenza per tutte le app di tracciamento europee. Ma l'accordo tra Apple e Google hanno modificato il quadro originario (anche se Chris Boos, numero uno del team di Pepp-PT aveva annunciato la propria disponibilità a collaborare con le due società americane). Anche perché la virata del consorzio Pepp-Pt verso il sistema centralizzato non è piaciuta, al punto che oltre 300 ricercatori ed "esperti" del settore di oltre 25 paesi hanno sottoscritto un appello a metà aprile per chiedere agli Stati di aderire ad un approccio decentralizzato per i sistemi di tracciamento dei contatti, appoggiando in maniera palese e dichiarata lo sviluppo delle infrastrutture gestite da Google e Apple, considerate più protettive per la privacy (viene da ridere a scriverlo). Tra i firmatari italiani troviamo 8 professori: Rainer Bauböck

dell'European University Institute di Firenze; Carlo Blundo dell'Università di Salerno; Dario Catalano dell'Università di Catania; Ciro Cattuto dell'Università di Torino; Giovanni Comandé della Scuola Superiore Sant'Anna Pisa; Mauro Conti dell'Università di Padova; Giuseppe Persiano dell'Università di Salerno; Daniele Venturi dell'Università La Sapienza di Roma e Ivan Visconti dell'Università di Salerno.
"Alcune delle proposte basate su Bluetooth rispettano il diritto alla privacy dell'individuo" — si legge nella lettera aperta — mentre altre consentirebbero una forma di sorveglianza del governo o del settore privato che ostacolerebbe catastroficamente la fiducia e l'accettazione di tale applicazione da parte della società in generale" (https://www.startmag.it/innovazione/app-immuni-consorzio-pepp-pt/).
Ancora una volta, il cruccio non è l'intromissione e la compressione delle libertà degli individui ma il timore che, percependosi spiati, questi ultimi poi non scarichino queste tipologie di applicazioni. Tra l'altro, Google e Apple non fanno parte del "settore privato" di cui si parla, forse? O si crede davvero che le due multinazionali perseguano la finalità del bene collettivo e non invece quello del profitto?
Si legge anche che "alcuni che cercano di costruire sistemi centralizzati stanno facendo pressione su Google e Apple affinché aprano i loro sistemi per consentire loro di acquisire più dati", con chiara allusione al governo francese, che sta continuando la sua collaborazione con Pepp-PT. Insomma, il problema sarebbero solamente i governi che vogliono carpire i dati dei propri cittadini, mentre Google e Apple sarebbero robusti paladini della privacy e della libertà individuale. Ma per favore!
Cresce il dubbio che questi ricercatori ed esperti che hanno diffuso questo appello tanto "indipendenti" non devono essere! Tra gli 8 firmatari italiani, spicca il nome del professor Ciro Cattuto, "data scientist e digital epidemiologist" dell'Università di Torino che è anche membro della **Fondazioni Isi,** istituto di ricerca sui big data torinese che faceva parte in origine del Consorzio Pepp-pt, ritirandosi a metà aprile, ed oggi fa parte di DP-3T, cioè il protocollo per il tracciamento più vicino a quello scelto da Apple e Google.
Ma a chi fan schifo sia i governi che le multinazionali, a che pro scegliere tra due mali?

IL RUOLO DI VODAFONE

Tornando ai partner di Pepp-PT, troviamo, come abbiamo visto, anche la multinazionale di telefonia fissa e mobile Vodafone, una delle principali società di telecomunicazioni al mondo per ricavi e clienti (con circa 470 milioni di clienti sulle reti mobili di cui 29 milioni di clienti solo in Italia) e che sta spendendo miliardi per lo sviluppo delle nuove tecnologie, ad esempio la tecnologia 5G e lo studio dei Big Data.
6,5 miliardi solo negli ultimi anni, di cui 2,4 a carico di Vodafone Italia, di cui è amministratore delegato Aldo Bisio, che già nell'estate del 2019 comunicò il lancio del 5G su rete commerciale a Milano e hinterland, Roma, Torino, Bologna e Napoli, con la promessa entro il 2021 di estenderlo a 100 città italiane (https://www.digitalvoice.it/vodafone-per-prima-in-italia-lancia-il-5g-bisio-accendiamo-le-prime-5-citta/) e (https://www.ilsole24ore.com/art/vodafone-testa-5g-nell-automotive-sorpasso-assistito-coda-smart-AClOJ9w?fromSearch)
Aldo Bisio è stato anche sentito dal governo italiano in qualità di portavoce dell'azienda sul tema 5G e contact tracing, l'8 aprile scorso, durante un'audizione alla Camera dei Deputati, IX Commissione Trasporti, Poste e Telecomunicazioni. Bisio, in quel frangente, ne ha approfittato per chiedere al governo "*un immediato adeguamento dei limiti di campo elettro-magnetico al livello*

degli altri principali Paesi europei e necessarie misure di semplificazione, avvalendosi degli istituti già noti al nostro ordinamento dell'auto-certificazione e del silenzio-assenso per consentirci di rafforzare ulteriormente le nostre reti e renderle così pronte a sostenere un traffico in potenza ancora maggiore in futuro" (https://www.key4biz.it/5g-aldo-bisio-vodafone-italia-semplificare-iter-per-nuovi-siti-e-antenne/299527/)
In pratica, Vodafone sta chiedendo ai governi l'aumento dei limiti elettromagnetici e una semplificazione delle procedure per poter installare le antenne e i siti 5G ovunque.
Ma qualche parola Bisio l'ha spesa anche a proposito dell'app di tracciamento: dopo essersi vantato che Vodafone ha messo a disposizione delle istituzioni i dati delle celle riguardanti la mobilità dei suoi clienti in 13 regioni italiane, ha poi continuato affermando che *"grazie alla collaborazione tra il Gruppo Vodafone e università e centri di ricerca, siamo riusciti a sviluppare in poche settimane una app basata sulle tecnologie GPS e Bluetooth, finalizzata al tracciamento di soggetti potenzialmente entrati in contatto con il virus"*, per poi concludere dicendo che *"devono essere le istituzioni nazionali a giustificarne l'esigenza ai cittadini e a confermarne la compatibilità con l'ordinamento vigente. Abbiamo una grande opportunità di costruire una società più digitale"* (https://www.key4biz.it/wp-content/uploads/2020/04/MemoriaVodafoneCovid19FINAL.pdf).
Ora, non sappiamo se Bisio si riferisca ad "Immuni", per cui non risulta un coinvolgimento ufficiale di Vodafone, oppure a quella che sarà lanciata in Germania. É certo però che sia Vodafone sia Bending Spoons, che ha sviluppato l'app, sono stati partner nel consorzio Pepp-PT.
È stato sempre Bisio a chiarire che *"la nostra partecipata tedesca fa parte di questo consorzio e sta lavorando all'app che sarà comunque diversa dal modello coreano e cinese"* (infatti il modello è quello di Singapore).
Ma cosa ha portato Vodafone ad interessarsi al contact tracing?
Sul sito della compagnia (www.vodafone.com/covid19) leggiamo che *"le stime suggeriscono che un vaccino contro il coronavirus potrebbe impiegare 18 mesi per svilupparsi al minimo. Le economie europee non possono permettersi di aspettare così tanto per tornare alla normalità, anche se ciò significa gestire ulteriori ondate di infezione. Vodafone, insieme al resto del settore delle telecomunicazioni, ha svolto un ruolo fondamentale fornendo connettività durante questo periodo oscuro e rendendo il blocco più gestibile e probabilmente tollerabile per le società in modi che sarebbe stato difficile immaginare 30 anni fa prima dell'invenzione di Internet. In prospettiva, il sostegno del settore rimarrà la chiave per i governi e le autorità sanitarie nell'elaborare le strategie di uscita dai blocchi. Un ruolo centrale, in questo contesto, è quello delle app di tracciamento dei contatti (…) In combinazione con i test di massa e altre misure di supporto, può ridurre la probabilità di dover tornare al blocco collettivo. (...) riteniamo che i governi europei debbano scegliere un'unica piattaforma interoperabile affinché i viaggi e altre forme di mobilità possano ricominciare sia all'interno che tra i paesi europei. Dobbiamo disporre di app che supportino la libera circolazione delle persone nell'UE, come una delle quattro libertà attualmente sospese. Se qualcuno che utilizza un'app viaggia dalla Spagna attraverso la Francia e in Italia, ad esempio, deve sapere che verrà comunque avvisato se viene in contatto con persone a cui viene diagnosticato COVID-19, anche se sta utilizzando un'app diversa pensata per la propria nazione. (…) Con questi obiettivi, Vodafone ha aderito al consorzio paneuropeo per il monitoraggio della prossimità (PEPP-PT), che è stato anche recentemente approvato dai governi di sette paesi, tra cui Austria, Francia, Germania, Italia, Malta, Spagna e Svizzera. Sosteniamo fortemente PEPP-PT e incoraggiamo anche altri politici europei a unirsi a questa piattaforma. (…) Il nostro ruolo è stato quello di aiutare il consorzio a testare l'app con diversi sistemi operativi per smartphone. (…) il tracciamento dei contatti è solo uno dei tanti strumenti che i governi possono e dovrebbero*

utilizzare per elaborare strategie di uscita efficaci dai blocchi. In particolare, le mappe sulla mobilità della popolazione che gli operatori di telecomunicazioni come Vodafone sono in grado di trarre dai dati di rete hanno già consentito a governi come Spagna, Italia, Grecia e Portogallo di valutare l'efficacia delle loro misure di quarantena e strategie di distanziamento sociale. (…)"
La stessa Vodafone fa infatti parte anche di un'altra iniziativa, con altre società di telecomunicazioni (Deutsche Telekom, Orange, Telefonica, Telecom Italia-Tim, Telenor, Telia, A1 Telekom Austria) che hanno concordato di fornire alla Commissione europea i dati aggregati sulla posizione dei telefoni cellulare al fine di tracciare la diffusione del nuovo coronavirus (https://www.startmag.it/innovazione/vodafone-telecom-italia-tlc-dati-coronavirus-ue/).

***

DP-3T - Decentralized Privacy-Preserving Proximity Tracing

Come le italiane Bending Spoons e Fondazione Isi di Torino, molti altri istituti, a seguito dell'apparizione delle API di Apple e Google, ed anche per le accuse di scarsa chiarezza lanciate contro la mente del progetto, Chris Boos, hanno abbandonato il consorzio Pepp-PT.
Anche gli sviluppatori e i ricercatori del gruppo DP-3T si sono allontanati da Pepp-PT, denunciandone la scarsa trasparenza, come Marcel Salathé, professore all'EPFL di Losanna, che era stato il cofondatore del consorzio insieme a Chris Boos. A metà aprile se ne è andato anche Michael Veale, docente di diritti digitali dell'Università di Londra e anche lui membro del DP-3T.
Ricercatori provenienti da Belgio, Italia, Svizzera e qualcuno anche dalla Germania hanno via via lasciato Pepp-PT. Il 17 aprile 2020, anche l'École Polytechnique Fédérale de Lausanne (EPFL) e l'ETH di Zurigo, e cioè i primi responsabili del progetto DP-3T, si sono ritirati ufficialmente dal consorzio Pepp-PT, lanciando l'accusa di non rispettare abbastanza la privacy personale.
Successivamente KU Lovanio, il Centro Helmholz CISPA per la sicurezza delle informazioni, il Laboratorio europeo per l'apprendimento e i sistemi intelligenti e l'Università tecnica della Danimarca, si sono ritirati dal consorzio.
Alcune di queste aziende si sono poi riunite all'interno di **DP-3T:** l'École Polytechnique Fédérale de Lausanne (EPFL) che ne è la fondatrice; l'ETH di Zurigo; Ku Leuven; TU Delf; University College London; CISPA; Università di Oxford; **Fondazione Isi di Torino.**
Il progetto DP-3T (Decentralized Preserving Proximity Tracing) è un protocollo decentralizzato open-source per il tracciamento di prossimità che utilizza la funzionalità Bluetooth Low Energy su dispositivi mobili, prodotto dal lavoro di un team di oltre 25 ingegneri e accademici di tutta Europa, originariamente avviato presso EPFL e che ora si è ampliato per includere parti interessate in tutta Europa e oltre.
Situato in Svizzera, l'EPFL accoglie studenti, insegnanti e collaboratori di oltre 120 nazionalità. Con una vocazione internazionale, l'EPFL si concentra su tre missioni: istruzione, ricerca e innovazione e collabora con una vasta rete di partner tra cui, in particolare, altre università e college, scuole secondarie, industrie, imprese economiche e circoli politici. L'EPFL è strutturato in una direzione centrale, 5 facoltà, 3 college, laboratori ed altri centri minori (EPFL PRES, Centre Est, CH-1015 Lausanne - https://www.epfl.ch/en/).
Al progetto DP-3T collaborano oggi anche diversi professori di università sparse per l'Europa: Università di Stanford; Università di Oxford; Université de Toulon; Università di Marsiglia; Università di Porto (FCUP), l'IMDEA Software Institute di Madrid; e per l'Italia Università di

Salerno (Prof. Giuseppe Persiano) e Università degli Studi di Torino / Fondazione ISI (Prof. Ciro Cattuto) (Dalla documentazione di DP-3T: https://github.com/DP-3T/documents).
Lo sviluppo del protocollo di tracciamento di DP-3T è molto simile al sistema di Apple e Google. Dalla documentazione leggiamo che *"il progetto DP3T non è finanziato da Google o Apple. Tutte le spese del progetto di finanziamento provengono dai fondi discrezionali del Prof. James Larus all'EPFL, in previsione di una sovvenzione della Fondazione Botnar"*.
Poi però subito dopo viene ammesso che *"due ricercatori coinvolti nel progetto hanno ricevuto finanziamenti da Google in passato. Nel 2019, la Prof. Carmela Troncoso ha ricevuto un premio per la ricerca sulla sicurezza e la privacy di Google. Nel 2015, lo studente del Prof. Edouard Bugnion ha ricevuto un dottorato di ricerca in Google. Inoltre, il Prof. Mathias Payer ha ricevuto una ricompensa"*.
Carmela Troncoso, programmatrice ed esperta di sistemi di tracciamento, è entrata a far parte dell'EPFL nel 2017 come responsabile del laboratorio SPRING, Security and Privacy Engineering Laboratory (https://www.epfl.ch/labs/spring/) dove si testano e sviluppano strumenti per l'apprendimento automatico per gli ingegneri informatici. Come ammesso anche da DP-3T, è stata onorata da Google per il suo lavoro sull'apprendimento automatico nella privacy e nella sicurezza digitale. Un modo per *"riconoscere gli accademici che hanno dato un contributo importante al campo"*. Non capita a tutti, visto nel corso dell'anno sono stati solo sette i ricercatori illuminati premiati da Google, compresa la Troncoso. Il premio Google consiste in 75.000 dollari in finanziamenti per la ricerca (https://actu.epfl.ch/news/carmela-troncoso-wins-google-security-and-privacy-/).
Non ci deve sembrare strano, allora, se è proprio questa Carmela Troncoso a guidare oggi il team europeo che si è concretizzato nel DP-3T.
Stiamo parlando di una persona che, durante un'intervista, ha tessuto le lodi di Apple e Google con queste parole: *"stanno facendo un grande favore alla privacy degli utenti. (…) Quando parliamo dei dati sui contatti di un intero paese, è importante (…) La soluzione di Apple e Google è fondamentalmente la stessa idea della nostra. Ci sono alcuni piccoli cambiamenti di cui stiamo parlando con loro per vedere le implicazioni. Ma per noi è perfetto"* (https://elpais.com/tecnologia/2020-04-15/la-ingeniera-espanola-que-lidera-la-app-europea-de-rastreo-de-contagios-no-debe-ser-un-estado-de-vigilancia.html?ssm=TW_CC).
Anche sulla documentazione fornita da DP-3T si dice esplicitamente che il loro protocollo e quello fornito da Apple e Google sono praticamente la stessa cosa, e infatti si può leggere che *"Apple e Google hanno rilasciato una specifica congiunta per un sistema di notifica dell'esposizione che preserva la privacy su iOS e Android. La loro proposta è molto simile alla nostra proposta iniziale. DP-3T apprezza l'approvazione di queste due società per la nostra soluzione e ha lavorato con entrambe per implementare la nostra app sulle loro piattaforme"*.
Ma di quale app parla DP-3T? Di quella introdotta in Svizzera, dato che il protocollo è stato usato per cercare di diffondere all'interno della Confederazione elvetica l'app "SwissCovid".
L'app di DP-3T è disponibile pubblicamente su Android e iOS e può essere utilizzata come base per altre app nazionali (Documentazione: https://www.bag.admin.ch/swisscovid-data-protection-statement-and-conditions-of-use).
Le università ETH di Zurigo ed Ecole polytechnique fédérale de Lausanne (EPFL) stanno collaborando con l'esercito e diversi ospedali per testare "SwissCovid" con gli aggiornamenti dei sistemi operativi di Apple e Google. Ad oggi, i dipendenti dei due istituti, dell'esercito, degli ospedali che stanno collaborando al progetto-pilota e delle autorità cantonali possono scaricare l'applicazione dagli store: *"Questa è la prima volta (…) su così vasta scala"*, ha affermato il professor Edouard Bugnion, vicepresidente responsabile dei sistemi informativi dell'EPFL (https://telecoms.com/504574/switzerland-claims-to-be-first-to-trial-apple-and-google-covid-19-apis/). Questo test-pilota è infatti il primo al mondo, su così scala così allargata, che si serve degli aggiornamenti di Google e Apple. A seguire, DP-3T si prepara a rendere l'app disponibile per tutta la Svizzera a cominciare da metà giugno. E non solo in Svizzera: *"il nostro obiettivo è offrire una soluzione che possa essere adottata in Europa e nel mondo"*, ha spiegato Carmela Troncoso.

Dalla documentazione si legge che *“quasi tutti i paesi, in particolare quelli europei, stanno seguendo l'esempio della Svizzera per il lancio della propria applicazione (...) basata su questo protocollo decentralizzato. Ciò faciliterà l'interoperabilità dei sistemi quando si viaggia all'estero”*.
Si sta attendendo solo le modifiche legislative da parte della Svizzera prima di essere lanciato al “grande pubblico”.
“SwissCovid” opera in modo "decentralizzato", a meno che al titolare del cellulare non venga diagnosticato il COVID-19. In questo caso, il suo medico gli fornirà un codice monouso che gli consentirà di condividere volontariamente gli identificatori temporanei del proprio telefono con un server statale gestito dalla Confederazione elvetica. Se il contatto con una persona positiva è stato prolungato (più di 15 minuti) e ravvicinato (meno di 2 metri), genera una notifica che indica all'utente del telefono il giorno di esposizione al rischio e cosa fare dopo.
Il processo di tracciamento è quindi supportato anche in questo caso da da un server centrale che che condivide le informazioni con l'app in esecuzione su ciascun telefono, ma DP-3T afferma sicuro che tramite la crittografia end-to-end il server non sarà in grado di risalire alle persone.
https://medium.com/@jaromil/decentralized-privacy-preserving-proximity-tracing-cryptography-made-easy-af0a6ae48640
C’è sempre però un piccolo inconveniente, derivante dal fatto che le app nazionali possono sempre variare in alcune funzioni rispetto al protocollo a cui hanno aderito, e la responsabile di DP-3T ha l’onestà di ammetterlo:*“anche con il nostro protocollo l'app può, ad esempio, chiamare automaticamente quando qualcuno riceve un avviso di contagio. (…) Ma puoi inviare quello che vuoi: i miei numeri, i metadati. Se vuoi la posizione, la prendi e la metti da parte. Il bluetooth invia solo codici, ma l'app potrebbe rilevare la posizione GPS del cellulare. Ma questo non ha nulla a che fare con il protocollo. Le autorità nazionali possono decidere molte cose”*.
https://elpais.com/tecnologia/2020-04-15/la-ingeniera-espanola-que-lidera-la-app-europea-de-rastreo-de-contagios-no-debe-ser-un-estado-de-vigilancia.html?ssm=TW_CC

LA FONDAZIONE ISI

La Fondazione Istituto per l'Interscambio Scientifico (ISI) - ISI Foundation, Via Chisola 5, Torino (https://isi.it/en/home) è un centro di ricerca torinese pubblico-privato (più privato che pubblico) che da oltre trent'anni opera nei campi dei Big Data, dell'epidemiologia digitale e dell'intelligenza artificiale. Fondato nel 1983 da Regione Piemonte, città di Torino e Fondazione CRT. Presidente della Fondazione ISI è Mario Rasetti; Francesco Bonchi, ex direttore della ricerca presso i laboratori Yahoo! a Barcellona, è il nuovo direttore scientifico.
Oltre alla sede principale di Torino, l'istituto ha una seconda sede – la divisione ISI Global Science Foundation - presso la State University of New York.
Con una nota informativa del Presidente della Fondazione, Prof. Mario Rasetti, sulle attività svolte da ISI in merito al tracciamento dei contatti per la pandemia COVID-19, si viene a conoscenza di quello che fa l’istituto torinese, che lavora principalmente *“tramite le informazioni ricavate dall’analisi di grandi quantità di dati, la misurazione dei comportamenti umani e lo sviluppo di modelli e algoritmi predittivi”*.
Questo lo fa soprattutto *“attraverso l’integrazione di dati sulla mobilità umana e sulla distribuzione delle persone affette dal virus”* al fine di sviluppare una mappa interattiva del contagio basata sui modelli predittivi sviluppati da Alessandro Vespignani, Capo del Comitato scientifico, assieme al gruppo coordinato da Corrado Gioannini che interagisce con gli scienziati della North Eastern University di Boston guidati sempre da Vespignani.
Un altro settore ritenuto molto importante è *“la misurazione dei cambiamenti comportamentali,*

condotta da un gruppo di ricercatori specializzati in Data Science guidato da Michele Tizzoni in partnership con ***Cuebiq,*** *società con sedi in Italia e negli Stati Uniti, attiva nell'area della "location intelligence", che analizza dati anonimizzati* [mah!] *sulla posizione di utenti smartphone per valutare l'impatto delle restrizioni imposte dalle autorità nazionali sulla mobilità dei cittadini italiani"* (https://www.isi.it/en/news-events/nota-informativa-del-presidente-della-fondazione-sulle-attivit-svolte-da-isi-a-contributo-agli-sforzi-conoscitivi-della-pandemia-covid-19-).
Fondazione ISI ha tra l'altro analizzato un campione anonimo di 170mila utenti di smartphone sparsi per l'Italia per monitorare spostamenti e contatti tra le persone e quindi fare un confronto tra quello che succedeva prima della pandemia e dopo, con l'intensificarsi delle restrizioni a partire dal 22 febbraio e fino al 10 marzo. Una ricerca questa, a cadenza quotidiana, in collaborazione con **Cuebiq**, il "location intelligence company" statunitense che raccoglie dati di utenti di smartphone sulla loro posizione attraverso delle app e che solitamente li sfrutta per fini di marketing.
Il coordinatore della ricerca è Michele Tizzoni, della Fondazione ISI (https://www.ilmanifesto.it/alta-diagnostica-e-controllo-sociale-il-modello-corea-del-sud-ribalta-i-numeri-per-ribaltare-i-numeri/).
"Abbiamo monitorato, settimana per settimana, come sono cambiate le abitudini (...) concentrandoci sulle differenze negli spostamenti tra province diverse, le distanze più brevi ad esempio andando a considerare la distanza media percorsa negli spostamenti settimanali degli utenti e poi come sono cambiati i contatti a distanze inferiori ai 50 metri uno dall'altro", ha spiegato Michele Tizzoni, ricercatore della Fondazione ISI, *"informazioni fondamentali per capire come il trend epidemico può essere influenzato da queste politiche restrittive e che sono a disposizione pubblicamente della comunità scientifica, quindi possono essere usate soprattutto dagli epidemiologi, dagli economisti e dai decisori politici"*. Però, accipicchia! Notare: anche dagli economisti!
Secondo lo studio dei dati, risulterebbe che, dall'inizio dell'epidemia spostamenti e contatti si sono ridotti dell'80% circa, con una percentuale più alta per il nord Italia e più bassa al sud, anche se non di tanto: circa 10 punti di differenza. *"Abbiamo visionato i dati* – spiega all'ANSA uno dei ricercatori ISI, Ciro Cattuto – *che ci ha dato Cuebiq, che raccoglie (...) i dati delle applicazioni degli smartphone, riuscendo a localizzarli con un'accuratezza di 10 metri"*. I dati, sono stati poi ceduti da Cuebiq alla Fondazione Isi per il progetto di ricerca.
Da ricordare che, anche se dall'istituto continuano a ripetere che *"come ricercatori ISI non è nostra intenzione lavorare al controllo delle persone positive e all'individuazione dei contatti avuti da queste persone"*, come reso noto dalla ministra per l'Innovazione, Paola Pisano, l'elenco dei 74 esperti che hanno lavorato alla scelta per l'app di tracciamento dei contatti tra smartphone, contempla anche Ciro Cattuto che è proprio uno ricercatori principali di Fondazione ISI.
Il buon Cattuno si è occupato proprio di "Tecnologie per il governo dell'emergenza" con Stefano Calabrese, Carlo Alberto Carnevale Maffè, Alfonso Fuggetta, Andrea Nicolini, Leonardo Favario, Umberto Rosini, Alberto Eugenio Tozzi, Francesca Bria e Simone Piunno, tutti convinti assertori del *contact tracing* (https://www.isi.it/media/286).
La **Fondazione CRT** di Via XX Settembre 31 a Torino, grossa fondazione piemontese, è il principale sostenitore delle attività della Fondazione ISI, che viene anche finanziata da progetti di ricerca della Commissione Europea e da altre fondazioni di origine bancaria, ed è a sua volta membro del **EFC-European Foundation Center** (di cui Massimo Lapucci, Segretario Generale di Fondazione CRT è anche Presidente) ed affiliata anche all'**Associazione delle Fondazioni Bancarie del Piemonte** (https://www.fondazionibancariepiemonte.it/) che riunisce le Fondazioni Cassa di Risparmio di Alessandria, Asti, Biella, Cuneo, Fossano, Saluzzo, Savigliano, Torino,

Tortona, Vercelli, Fondazione CRC e la **Compagnia di San Paolo**.
La Fondazione CRT mette a disposizione risorse economiche per giovani ricercatori del Piemonte e della Valle d'Aosta, attraverso il Progetto Lagrange, attivo dal 2011, finanziato da alcune banche e attraverso il coordinamento scientifico della Fondazione ISI.
Un altro progetto a cui collabora la Fondazione ISI è Ada Lovelace Lab (ALL), finanziato dal Centro di innovazione della banca **Intesa Sanpaolo**. Si tratta di un progetto di ricerca sull'IA (Intelligenza Artificiale).
Fondazione Isi, insieme a Fondazione CRT, European Foundation Centre e The GovLab di Brooklyn (NY), è alla guida di ***"Data for Good"***, programma e centro di ricerca sui Big Data a Torino che ha collaborato con l'italo-americana Cuebiq per gestire e rendere accessibili attraverso una "governance condivisa" i dati del contagio tra ricercatori e sviluppatori di nuove tecnologie (http://www.fondazionecrt.it/fondazione/progetti-internazionali/2020-att-internaz-data-for-good-coronavirus.html). Attraverso modelli predittivi sviluppati con Alessandro Vespignani, a capo del Comitato scientifico dell'Istituto, il gruppo ISI coordinato da Corrado Gioannini, ha interagito con i colleghi della North Eastern University di Boston guidati guarda caso sempre da Vespignani, *"fornendo predizioni sull'evoluzione del contagio epidemico, attraverso l'integrazione di dati sulla mobilità umana e sulla distribuzione delle persone affette dal virus"* col sistema di monitoraggio on line dei cambiamenti comportamentali sviluppato da Michele Tizzoni, ricercatore di Fondazione ISI, e da un gruppo di ricercatori specializzati in Data Science in partnership con Cuebiq (https://isi.it/en/news-events/nota-informativa-del-presidente-della-fondazione-sulle-attivit-svolte-da-isi-a-contributo-agli-sforzi-conoscitivi-della-pandemia-covid-19-).

Cuebiq e *Data for Good*

Non ci sono solo Google, Facebook e Amazon che accedono ai nostri dati su smartphone e on-line per valutare l'efficacia di campagne pubblicitarie e consigliare i loro clienti su come migliorarle. Queste sono solo le più famose ma tantissime aziende, attive soprattutto nel settore della pubblicità online, lo fanno. Una di queste si chiama **Cuebiq**, con una sede a New York, uffici a San Francisco, Chicago e Cina e un importante dipartimento di ricerca a Milano, che può contare su un team di un centinaio di ingegneri e ricercatori nel settore data-science.
L'Ufficio Cuebiq in italia è in Corso di Porta Romana 68, 20122, Milano
Con a capo Antonio Tomarchio, Cuebiq è stata fondata dallo stesso Tomarchio assieme a Walter Ferrara, Filippo Privitera e William Nespoli nel 2016, come spin-off italo-americana dell'italiana **Beintoo**, a sua volta società di marketing italiana fondata nel 2011 attiva pure nel mondo delle piattaforme di monetizzazione in ambito videoludico, che fa campagne di "proximity marketing" per generare traffico online e convogliarlo verso i punti vendita in maniera, per così dire, meno artificiale.
Su Sturtup-Italia possiamo leggere questo profilo aziendale: *"In Cuebiq i viaggi tra Milano e New York sono regolari, e questo permette a chi lavora da noi di costruire una carriera internazionale pur mantenendo la propria base in Italia"*(https://startupitalia.eu/100779-20181120-cuebiq-costruisce-hub-data-expert-milano).
Il 2019 è stato un anno in crescita per la sturtup. Nel maggio 2019 la startup ha ottenuto 27 milioni di dollari di finanziamenti raccolti grazie alla fiducia incassata da Goldman Sachs Principal Strategic Investments (PSI), Nasdaq Ventures, DRW Venture Capital e Tribeca Venture Partners

(alcuni di questi sono pure presenti nel capitale della sturtup, come Tribeca Venture e Balyasny Asset Management) e reinvestiti in ricerca e sviluppo, con una importante quota proprio nel dipartimento di ricerca di Milano (https://bebeez.it/2018/05/24/cuebiq-la-startup-usa-spinoff-dellitaliana-beintoo-incassa-round-27-mln/).
Cuebiq è specializzata nella "business intelligence", una branca di ricerca che consente alle aziende private di comprendere il comportamento e le intenzioni di acquisto dei consumatori tramite l'analisi dei dati. Questo Cuebiq lo fa attraverso la raccolta dei dati sulla geo-posizione ed *"il modo in cui le persone si muovono all'interno dei punti vendita"* per migliorare le performance commerciale dei punti vendita fisici dei propri clienti: negozi, imprese, marchi multinazionali.
Ciò permette alle aziende - almeno 1500 quelle che si sono rivolte a Cuebiq fin'ora - di realizzare campagne pubblicitarie mirate.
Nel 2016 Tomarchio sottolineava che Cuebiq *"rappresenta il futuro della business intelligence. Attraverso i nostri dati, consentiamo alle aziende di qualsiasi dimensione di ottenere informazioni senza precedenti sui comportamenti e i trend dei consumatori nella vita reale; utilizzando la nostra leadership globale nei dati geo-comportamentali, con il lancio di Cuebiq diamo al mercato un nuovo modo di pensare alle capacità della business intelligence"* (https://www.economyup.it/startup/beintoo-lancia-uno-spinoff-in-america/).
L'obiettivo dichiarato di Cuebiq è costituire un *"polo di eccellenza e d'avanguardia in ambito Big Data", che sia "punto di riferimento per i professionisti dei dati in Italia"*.
Ed infatti, oltre a lavorare con le aziende, Cuebiq ha avviato anche un programma battezzato ***Data for Good***, che mette i dati degli utenti a disposizione di chi vuole analizzarli.
Sul sito di **Cuebiq** si legge la pomposa affermazione: *"stiamo fornendo l'accesso ai dati sulla nostra piattaforma alla comunità scientifica al fine di condividere le nostre intuizioni e creare azioni positive al servizio dell'umanità (…) tramite il nostro programma Data for Good"* (https://www.cuebiq.com/about/data-for-good).
Attraverso il suo programma ***Data for Good***, la startup Cuebiq fornisce l'accesso ai dati aggregati sulla mobilità per ricerche accademiche e non meglio identificate "iniziative umanitarie" (tra i partner compare infatti UNICEF).
Cuebiq collabora con ISI Foundation per valutare l'efficacia delle restrizioni sulla mobilità messe in atto in Italia dal governo per l'emergenza coronavirus. Un'analisi dei dati che si concentra in particolare su come i modelli di mobilità e di contatto sono cambiati in Italia a seguito del blocco.
Guidata dal ricercatore della Fondazione ISI, Michele Tizzoni, la ricerca *"COVID-19 risposta alle epidemie: prima valutazione dei cambiamenti di mobilità in Italia dopo il blocco"*, è stata effettuata dai ricercatori Emanuele Pepe, Paolo Bajardi, Laetitia Gauvin, Filippo Privitera, Ciro Cattuto, e con il supporto dell'**Università di Torino**.
Con i dati aggregati provenienti dal programma *Data for Good* di Cuebiq, raccolti da utenti che hanno volontariamente fornito l'accesso ai loro dati di posizione, e relativi a GPS, Wifi e altre fonti come i beacon (il tipo di Bluetooth LE a bassa potenza utilizzato dai nuovi smartphone), questa ricerca mostra in tempo quasi reale gli effetti delle restrizioni in Italia potendo misurare i cambiamenti nei flussi di traffico tra le province, nella distanza media percorsa e nelle sovrapposizioni spaziali di gruppi di utenti in luoghi pubblici (lo studio si è concentrato soprattutto nelle prime tre settimane di intervento, tra il 18 febbraio e il 10 marzo).
"Fondamentalmente abbiamo preso i dati relativi a tutti gli utenti di una data provincia, e attorno ad ogni persona abbiamo calcolato un cerchio di circa 50metri. Se due di questi cerchi si incontrano esiste la possibilità di un incontro (…) L'analisi iniziale è partita proprio dall'Italia (…) aggregando i dati su finestre di 5 minuti"
La ricerca è in grado di valutare quasi in tempo reale gli effetti sulla mobilità delle politiche di "salute pubblica": In pratica, dopo aver identificato la provincia di residenza dei possessori di smartphone (registrando il luogo della maggior parte dei punti dati dell'utente durante la notte), la ricerca ha calcolato il raggio mediano di rotazione della popolazione in ciascuna provincia. In questo modo, per esempio, la ricerca ha anche potuto constatare come, prima dell'epidemia, metà della popolazione viaggiava per più di 5,7 km a settimana mentre nella terza settimana di

restrizioni, metà della popolazione già percorreva meno di 2 km a settimana (dal report degli autori: https://covid19mm.github.io/in-progress/2020/03/13/first-report-assessment.html).
Per saperne di più sulla raccolta dei dati e sul campione per questa analisi, basta dare un'occhiata alla ricerca completa: https://www.cuebiq.com/resource-center/resources/real-time-location-data-reveals-effect-of-lockdown-on-mobility-in-italy/
Sul loro stesso sito, pubblicano una interessante intervista a Brennan Lake, Senior Director of Research Partnerships and Data di Cuebiq, con alcune domande sul programma *Data for Good*.
Dopo aver osannato i suoi trascorsi in una ONG, Lake ci dice che *"presso la ONG, ci veniva costantemente detto di essere più guidati dai dati; ma nei paesi in via di sviluppo, molte raccolte di dati consistono in sondaggi cartacei su comunità difficili da raggiungere. Quindi, ero davvero interessato al potere dei Big data e dei dati sulla posizione per rispondere a domande sociologiche in aree su larga scala. Ero anche molto attratto dal fatto che in una fase così precoce dell'azienda, Cuebiq stava già pensando di restituire e creare valore sociale dai suoi asset di dati"*.
Si, valore sociale ma soprattutto economico!
Alla domanda su che cos'è l'iniziativa *Data for Good* di Cuebiq e come funziona, Lake ci dice ancora che è *"il programma attraverso il quale cerchiamo di migliorare la vita attraverso il nuovo uso dei dati sulla posizione e la mobilità. Lo facciamo per offrire vantaggi a milioni di utenti anonimi che condividono con noi i loro dati di posizione ogni giorno. (…) Collaboriamo con università e ricercatori: ad esempio, abbiamo lavorato con MIT Media Lab per esaminare l'impatto della segregazione economica sullo sviluppo dei quartieri urbani. Collaboriamo anche con l'Università di Washington e altre università per comprendere i modelli di evacuazione prima, durante e dopo le catastrofi naturali"*. Insomma, con la scusa umanitaria Cuebiq sta raccogliendo dati di milioni di utenti, che potrebbero tornare molto utili, non solo ai governi. Ed è un bel problema, dato che nell'intervista si dice che uno dei principali partner di Cuebiq è la Banca Mondiale.
Ma Cuebiq offre anche, alle aziende private, le derivanti *"informazioni sulla mobilità COVID-19 in tempo reale"* attraverso il progetto *"Mobility Insights"* per illustrare come i modelli di mobilità e i comportamenti della popolazione cambiano durante la crisi. Questi dati sono aggiornati quotidianamente, si legge, *"in modo da poter modificare di conseguenza le tue strategie aziendali nazionali e locali"* (https://www.cuebiq.com/resource-center/resources/how-to-use-offline-intelligence-to-manage-brand-health-during-covid-19).
Dall'intervista sul loro sito, veniamo anche a sapere del rapporto tra Cuebiq e il **Politecnico di Milano** che *"si è sviluppato in modo organico, dal momento che molti dei nostri data scientist e team di gestione provenivano dal Politecnico"*. In uno dei progetti, il progetto Safari Njema, finanziato dal Polisocial Award 2018 del Politecnico di Milano, lo stesso collabora con Cuebiq per valutare la *"povertà dei trasporti"* a Maputo, utilizzando dati di localizzazione ad alta precisione per creare nuovi sistemi di trasporto in Mozambico (https://www.cuebiq.com/resource-center/resources/data-for-good-providing-social-value-through-location-data).
Ma dicevamo anche che Cuebiq è solo uno spin-off di un'altra azienda, sempre coinvolta nel marketing digitale. Allora vediamo chi è **Beintoo**, la società a capo di Cuebiq.

BEINTOO - Ha uffici a Milano, Roma e Madrid e ha ricavi annui di milioni di euro.
Dal sito di **Beintoo**: *"L'anima dell'offerta Beintoo è una tecnologia proprietaria, definita SDK, che ci consente di leggere i dati comportamentali offline. L'SDK ci permette, nel pieno rispetto delle normative vigenti, di ottenere la massima accuratezza di analisi, e tradurre i dati in preziosi insights per ricostruire le abitudini e i gusti dei consumatori. Impieghiamo questo tipo di informazioni per supportare i brand sia per fini promozionali sia strategici (…) I dati di geolocalizzazione rilevati vengono utilizzati per costruire business insights basati sulla quantificazione delle visite, sulla frequenza e sul tempo di permanenza presso un punto d'interesse* [ovvero un negozio fisico o uno store on-line]. *In questo modo sarà possibile tracciare una mappa delle abitudini e preferenze dei consumatori, capirne il target di appartenenza e ottenere preziose informazioni per l'ottimizzazione del proprio business. La profilazione degli utenti consente di*

*iniziare una conversazione stabile col consumatore, monitorare in tempo reale il mercato e allineare l'offerta e, talvolta, anche predire l'efficacia di una nuova strategia", m*a anche *"conoscere la percentuale di smartphone che proviene o si dirige, subito dopo la visita in store, presso una specifica categoria di esercizi commerciali"* e monitorare *"il livello di fedeltà dei propri clienti e dei clienti dei propri competitor"* (https://beintoo.com).
Come arriva a tanto, Beintoo? Nel maggio 2019, la compagnia ha presentato la sua "Location Intelligence Platform": una piattaforma che usa la geolocalizzazione e consente di condurre analisi di tipo predittivo e di monitorare un'attività o un territorio circoscritto per fini pubblicitari e per marketing aziendale. Attraverso analisi geolocalizzate, l'azienda è capace di raccogliere informazioni relative a celle ISTAT su chi vive e lavora in una specifica area, il giorno e il tempo di permanenza medio in negozio, l'interesse verso i marchi della controparte, l'audience transitata davanti ad un cartellone pubblicitario per valutare l'efficacia delle campagne pubblicitarie.
"S*iamo stati in grado di identificare, ad esempio, i luoghi in cui la domanda di uno specifico prodotto era piú alta e suggerire conseguentemente l'apertura di nuovi punti vendita su un territorio più adatto a quel tipo di business"* (https://beintoo.com/locationintelligenceplatform/).
Ma sapete da chi è stata acquisita Beintoo, proprio a marzo di quest'anno 2020, in piena crisi coronavirus?
E' stata comprata da **Publitalia'80**, ovvero la branca finanziaria del **Gruppo Mediaset** della famiglia **Berlusconi**. Infatti, "*Publitalia '80 crede fortemente nell'innovazione (…). La partnership con Beintoo è un'ulteriore conferma della nostra strategia, anche in un momento delicato come quello che stiamo attraversando. L'acquisizione di questo nuovo partner ci consente di essere ancora più forti e aggiungere valore alla nostra offerta integrata, includendo nuove piattaforme, dati e tecnologie che permetteranno ai nostri inserzionisti di comunicare con i propri consumatori in modo sempre più efficace»* (commento di Stefano Sala, Amministratore Delegato Publitalia '80, https://beintoo.com/il-gruppo-mediaset-continua-a-investire-in-tecnologia-e-innovazione-publitalia-80-acquisisce-beintoo/).
Sempre dal marzo scorso, Beintoo ha all'attivo anche una partnership con **Amilon**, società italiana leader nel settore delle carte prepagate digitali: "*gli user cookies Amilon* [cioè i dati dei possessori delle card, Ndr.] *ci offrono informazioni specifiche che ci permettono di definire un "intention to buy" certa del consumatore, in quanto sappiamo quanto spenderà, in quanto tempo lo farà e presso quale insegna (…). L'unione (…) ci consente di aggiungere un importante tassello ai nostri dati, permettendoci di conoscere non solo i comportamenti, le abitudini e le preferenze dei consumatori, ma anche di qualificarli in relazione alle intenzioni di acquisto*" (https://beintoo.com/beintoo-e-amilon-siglano-una-partnership-per-realizzare-esclusive-campagne-cross-device-e-promuovono-liniziativa-save-the-shopping-per-lemergenza-covid-19/).
Beintoo a marzo 2020 ha anche condotto uno studio su alcuni dei luoghi fisici più frequentati di Madrid e Barcellona, per capire come si è evoluto il traffico di persone nelle settimane dopo il lockdown per il coronavirus, dal 10 al 18 Marzo. Attraverso la tecnologia di "location intelligence" di Beintoo, sono stati analizzati con GPS gli accessi ai principali aeroporti di Barajas e El Prat e alle principali stazioni di Madrid Sol e Barcelona Sants, per carpire i cambiamenti nelle abitudini di viaggio degli spagnoli e dei turisti. I dati sono stati ricavati da segnali GPS tramite delle app di proprietà di alcuni partner di Beintoo installate sugli smartphone (https://beintoo.com/madrid-e-barcellona-al-tempo-del-covid-19-lanalisi-di-beintoo-ci-rivela-come-cambiano-realmente-gli-spostamenti-degli-spagnoli/). Ma anche in Italia, con un monitoraggio tra il 1 febbraio e il 4 marzo sempre tramite GPS ed app installate sui cellulari, Beintoo ha potuto analizzare gli accessi a ristoranti, a negozi di abbigliamento, a catene di supermercati, agli aeroporti di Malpensa e Linate e alle stazioni Centrale e Garibaldi a Milano, evidenziando i cambiamenti nelle abitudini di consumo dei milanesi (https://beintoo.com/milano-al-tempo-del-covid-19-come-cambiano-realmente-le-abitudini-di-consumo-dei-cittadini/).

Come si vede, il passo da una app installata sul cellulare all'uso commerciale del tracciamento dei dati, il passo è veramente corto.

LE SEDI DI BEINTOO:
- Largo Francesco Richini 2, 20122 Milano
- Officine Farneto, Via dei Monti della Farnesina 77, 00135 Roma
- Calle de Quintana 27 a Madrid

***

IL RUOLO DI APPLE E GOOGLE

I giganti tecnologici degli Stati Uniti come **Apple** e **Google** (ma anche Microsoft e Amazon) cogliendo al volo la possibilità offerta dal nuovo coronavirus, hanno fatto lavorare i loro sviluppatori a un ritmo vertiginoso ed hanno rapidamente proposto le loro innovazioni hi-tech come panacea per superare la crisi sanitaria (https://www.fiercehealthcare.com/tech/apple-google-and-amazon-are-racing-to-battle-covid).
Parliamo di società che già da tempo stavano provando ad entrare nel lucrativo mercato sanitario mondiale. Solo negli Stati Uniti parliamo di investimenti per 3,5 miliardi di dollari negli ultimi tempi.
Apple si è concentrata sulla costruzione di app per la salute (come l'app Health Records) e si sta spingendo sempre più a fondo nella ricerca con Apple Heart Study, lanciando l'Apple Watch dotato di un elettrocardiogramma e dei "kit" per aiutare gli sviluppatori a creare app per iPhone e Apple Watch legate alla salute. Ciò ha portato Apple a generare ingenti entrate in questo settore.
Addirittura gli assicuratori sanitari degli Stati Uniti sono giunti a sostenere l'uso di Apple Watch per i loro clienti. Non è quindi un caso se, a partire da marzo, Apple si è concentrata sulle innovazioni tecnologiche riguardanti il COVID-19. Sul fronte aziendale, Apple sta sfruttando la carenza globale di dispositivi di protezione individuale (DPI). La società ha prodotto scudi facciali in plexiglas, riuscendo a spedire 1 milione di maschere facciali a settimana. Negli Stati Uniti, Apple ha collaborato anche con i Centri per il controllo e la prevenzione delle malattie, la Federal Emergency Management Agency e la Casa Bianca per distribuire nel paese la propria tecnologia di controllo dei sintomi (diario clinico) per cellulari e web.
Per ciò che riguarda **Google**, anche questa mega-corporation si sta concentrando sempre più sulla differenziazione della sua offerta, attraverso la ricerca di intelligenza artificiale in ambito sanitario e nel campo delle scienze della vita. Negli ultimi anni ha assunto noti e importanti esperti sanitari, tra ex dirigenti di cliniche pubbliche e private, nonché funzionari del Dipartimento della salute americano. Ha fornito tecnologie per monitorare il coronavirus al di fuori degli ospedali e software per test diagnostici. Usando i dati di **Google Maps**, ha prodotto mappe che evidenziano le tendenze della mobilità del virus a livello territoriale, con rapporti che misurano se e quanto le comunità stiano rispettando l'imposizione delle ordinanze di confinamento (non solo negli USA, dato che in Italia, Google, usando le informazioni raccolte attraverso la Cronologia delle posizioni delle mappe

satellitari di Google Maps, ha fornito molti dei dati aggregati sugli spostamenti, regione per regione, alle autorità sanitarie e ai centri di ricerca italiani, non esclusi quelli che hanno collaborato alle mappe della diffusione del contagio e allo sviluppo delle tecnologie di tracciamento).
Ma l'esternalizzazione della sanità pubblica alle mega-società private nel quadro dello sviluppo delle nuove tecnologie non finisce certo qui. Già a metà marzo, Google, attraverso la controllata Verily, aveva avviato negli Usa "Project Baseline", una piattaforma mirata ad individuare i casi di coronavirus nell'area californiana della Bay Area e di San Francisco. Un programma di screening che funziona attivando un account Google e che prevede un questionario a cui si accede firmando un modulo di autorizzazione per la raccolta dei dati personali e clinici. In questo modo, sempre più i dati personali entrano a far parte della "merce" a disposizione di queste società, che spesso "offrono" questi servizi e queste tecnologie a titolo gratuito alle società pubbliche, con l'obiettivo di farsi percepire come società benefattrici ma allo stesso tempo stringendo sempre più, come un cappio, il legame di dipendenza tra sanità pubblica ed impresa privata multinazionale. (https://www.repubblica.it/tecnologia/2020/03/16/news/google_triage_a_distanza_per_coronavirus-251432611/).
Ma quello che ci riguarda più da vicino, è che i due colossi della Silicon Valley che hanno in mano il mercato dei sistemi operativi per cellulari - il 27% Apple (iOs) e il 72% Google (Android) - il 10 aprile hanno annunciato con un comunicato congiunto (https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology) una collaborazione per mettere una propria piattaforma a disposizione dei governi e degli sviluppatori per le app di "contact tracing", con una serie di nuovi strumenti che permettono la comunicazione fra i due sistemi operativi superando i problemi di compatibilità che potrebbero causare errori e malfunzionamenti nelle app. Questi strumenti sono le *Application Program Interface* (API), le interfacce di programmazione per le app che consentono a queste ultime l'accesso alle funzioni Bluetooth degli smartphone Android e agli iPhone iOS, e che risolvono alcune delle criticità nel funzionamento delle app in background (in modalità dormiente) dovuti al fatto che mai prima d'ora la tecnologia Bluetooth era stata usata per il tracking.
A poco meno di un mese e mezzo dall'annuncio di questa collaborazione Apple e Google il 20 maggio hanno dichiarato che la tecnologia per l'"*Exposure Notification*" (il modo edulcorato con cui le due società chiamano ora il tracciamento dei contatti) *"è da oggi nelle mani delle autorità sanitarie di tutto il mondo, con cui abbiamo lavorato e che decideranno come usarla"*.
La versione "beta" era invece disponibile già da qualche giorno.
Per Android viene utilizzata l'infrastruttura Google Play Services che aggiornerà gli smartphone con versione Android 6.0 o superiore; per quanto riguarda iOS, invece, il sistema viene aggiornato per iOS 13, ma potrà essere supportato anche dai dispositivi iOS rilasciati negli ultimi 4 anni.
Il servizio di "notifiche di esposizione" è stato quindi reso disponibile tramite l'accesso ai Play Store (di Android e di IOS) o, in molti casi, con un aggiornamento software automatico che è stato scaricato nei cellulari senza bisogno di azioni manuali e all'insaputa dei possessori del cellulare (volendo, per Android è possibile disattivare Google Play Services, responsabile degli aggiornamenti automatici, dalle impostazioni di sistema: aprendo le impostazioni, nella sezione "Applicazioni" cercare la voce relativa e poi premere su "Disattiva". Google Play Services verrà così "congelato" e smetterà di girare in background. Questa procedura però blocca al contempo l'uso di tutte le app che richiedono Play Services per funzionare e moltissime di quelle di sviluppatori di terze parti).
Attraverso l'aggiornamento, da ora il servizio di "notifiche di esposizione al COVID 19" è quindi stato inserito come servizio predefinito sugli smartphone di centinaia di milioni di utenti nel mondo,

spesso senza nemmeno un avviso all'accensione dello smartphone per spiegare il funzionamento di questa nuova voce.
Su Android, il sistema operativo più diffuso in occidente, basta andare su Impostazioni e alla voce Google, aprendola, si vedrà tra i nomi dei servizi offerti comparire anche la scritta "notifiche di esposizione al COVID 19". Su Apple è presente una voce identica, che si trova in Impostazioni > Privacy > Salute. Non esiste la possibilità di disinstallare la funzione di "notifiche di esposizione al COVID-19", anche se bisogna dare l'autorizzazione all'uso.
Per attivare il servizio di "notifiche dell'esposizione", per ora, è comunque indispensabile aver scaricato sul cellulare un'app di tracciamento dei contatti (in Italia è la app Immuni). Senza l'app, per ora, pare che il servizio non funzionerà.
Per cercare di sviare l'attenzione dalla parola "tracciamento", considerata dai più come sinonimo di controllo e di invasione nelle propria sfera personale, per descrivere le funzionalità del proprio servizio/piattaforma, Apple e Google hanno deciso di modificare la terminologia utilizzata: al posto di "Contact Tracing" le due società parlano ora di "*Exposure Notification*", notifiche di esposizione, appunto. Dalle due multinazionali americane, fanno sapere che "*abbiamo collaborato per costruire la tecnologia di notifica di esposizione al contagio che consentirà alle app delle autorità sanitarie di funzionare in modo più accurato, affidabile ed efficace sia su telefoni Android che iPhone. Nelle ultime settimane, le nostre due società hanno lavorato insieme ad autorità sanitarie, scienziati, organizzazioni sulla privacy e leader dei governi di tutto il mondo per raccogliere contributi e indicazioni*".
Rispetto a quanto annunciato inizialmente, ufficialmente al fine di aumentare il livello di protezione della privacy degli utenti, Apple e Google hanno apportato una serie di modifiche alle API, col coinvolgimento appunto di governi, autorità sanitarie e società che si occupano dello sviluppo delle app (va segnalato che Bending Spoons, sviluppatrice dell'italiana "Immuni", ha lavorato con Apple e Google per migliorare l'app sfruttando le API rilasciate dalle due società).
Quando le diverse app nazionali saranno rispettivamente pronte, una volta scaricate sullo smartphone il sistema operativo chiederà se si vuole attivare o meno il '*Covid-19 Exposure notification*'. Se attivata la notifica di esposizione, l'app sullo smartphone comincerà a scambiare via Bluetooth i propri codici con gli altri smartphone che avranno scaricato la medesima app di contact tracing. Il funzionamento è sempre lo stesso: se si scopre di essere stati contagiati da Covid-19 l'applicazione chiederà conferma di voler inviare la lista dei contatti tracciati. Sullo smartphone delle persone con cui il contagiato è entrato in contatto comparirà un banner di notifica: "Possibile esposizione al Covid-19". Aprendola si hanno informazioni su chi ha certificato il contagio della persona con cui siamo entrati in contatto e la data del contatto *(https://www.primaonline.it/2020/05/21/307212/apple-e-google-diffondono-insieme-la-tecnologia-per-app-di-tracciamento/)*.
Una delle principali novità di Apple e Google riguarda le cosiddette "Temporary Tracing Keys", le chiavi casuali di traccia temporanea (precedentemente note come "Daily Tracing Keys", chiavi di traccia giornaliera). La loro natura temporanea non sarà più legata specificatamente a un periodo di 24 ore. É stato anche deciso di cambiare l'algoritmo utilizzato per crittografare gli identificatori casuali che vengono scambiati frequentemente tra gli smartphone. Le due aziende hanno adottato per le Api l'Advanced Encryption Standard: il protocollo matematico adottato dal governo statunitense per i documenti top secret della Nasa. Anche i metadati invitati tramite Bluetooth, e condivisi tra i telefoni, verranno crittografati. In questi metadati sono inclusi vari elementi tra cui il livello di potenza di trasmissione dei dispositivi e il numero di versione del protocollo in esecuzione. Con questi metadati si può identificare un cellulare associando, ad esempio, la potenza

a un particolare modello di smartphone. Ma che un segnale o un identificativo sia casuale e criptato non significa che comunque sia anonimo, come vogliono far credere.
I metadati crittografati verranno memorizzati nel database locale e confrontati con gli identificativi di persone positive al COVID-19 contenuti in una lista scaricata quotidianamente, in questo caso, da un server. Gli “eventi di prossimità” verranno registrati a intervalli di cinque minuti e il tempo di esposizione massimo non andrà oltre i 30 minuti. L'aggiornamento delle API, inoltre, consentirà anche di sapere il numero di giorni trascorsi dall'ultimo evento di esposizione, per determinare dopo quanto tempo potrebbero comparire i sintomi. Infine, è stata aggiunta la possibilità di cancellare la cronologia delle informazioni memorizzate sullo smartphone relative alla notifiche dell'esposizione, identificatori di prossimità a rotazione e chiavi di tracciamento temporaneo. Dati che però non è detto che scompaiano anche dal server in uso al sistema operativo, anzi, è molto facile che lì rimangano impressi. Così il rischio è che i dati oggetto di profilazione possano, a prescindere dalle *policies* degli sviluppatori, rimbalzare sui server di queste multinazionali,...ricordando sempre che inoltre i sistemi operativi memorizzano anche, se attiva, la posizione del GPS, e che molte altre app che scarichiamo sui cellulari funzionano appoggiandosi a Google Maps (pensiamo solo alle tante app per sport all’aperto, che permettono di registrare il proprio percorso durante un'escursione o un giro in bici archiviando distanza, velocità, tempo in movimento, ecc. Google, per esempio, ha sviluppato “My Tracks”, un’app di tracciamento per sport all’aperto che permette di salvare questi dati in un archivio e condividerli direttamente con Google Maps).
Ma la vera particolarità che salta agli occhi è il fatto che il funzionamento del servizio per le notifiche di esposizione di Apple e Google richieda l’attivazione della geolocalizzazione del dispositivo insieme a quella del Bluetooth. L’informazione importante che si può leggere sul servizio si “notifiche dell’esposizione” direttamente dal cellulare, infatti dice che *“la geolocalizzazione del dispositivo deve essere attiva per poter rilevare i dispositivi Bluetooth nelle vicinanze, ma per le notifiche di esposizione al Covid19 non viene usata la posizione del dispositivo”*. Sarebbe interessante, allora, capire come mai viene espressamente richiesta l’attivazione del GPS per funzionare!?! Questo appare un controsenso! I contatti con altri dispositivi Bluetooth vengono rilevati dal Bluetooth del proprio cellulare, e non dal GPS. I dispositivi comunicano tra loro col Bluetooth! Ed allora a cosa (e a chi) serve che il GPS sia attivo, dato che l’unica cosa che può fare quest’ultimo è carpire la posizione geografica di una persona?
Gli sviluppatori di Immuni ed il governo italiano avevano assicurato e spergiurato che il tracciamento dei contatti non sarebbe mai avvenuto tramite la localizzazione col GPS, ed ecco qua che il GPS rientra dalla finestra con il servizio di “notifiche di esposizione” di Apple e Google, necessario per il funzionamento dell’app di contact tracing. Tra l’altro, fonti delle due multinazionali hanno fatto sapere che qualora i governi decidessero che la propria app per il tracciamento dovesse diventare non volontaria ma obbligatoria come si trattasse di un vaccino, loro si adeguerebbero. In quel caso l’unica scelta per chi non volesse aderire al tracciamento, sarebbe quella di non aggiornare il sistema operativo o meglio ancora gettare direttamente tra i rifiuti lo smartphone.
Si dice poi che *“gli ID casuali vengono eliminati dopo 14 giorni”*. Da dove? Solo dal cellulare o anche dai server cloud di Google ed Apple? Difficile che sia la seconda ipotesi. C’è infatti il problema connesso al funzionamento dei servizi cloud e al trasferimento di dati delicati che può avvenire al di fuori della UE: si sa che i dati nel cloud (servizio di archiviazione fornito dalle aziende su internet) non sono su server fissi, ma possono risiedere in server diversi anche nel corso di una stessa giornata, con il rischio di subire attacchi informatici. Ma la vera pericolosità è l’uso stesso che queste multinazionali fanno dei dati forniti, senza contare che le stesse possiedono molte

altre informazioni sui possessori degli account di un dispositivo mobile (per esempio la mail utente, la cronologia delle posizioni, l'account su facebook e molto altro) e incrociando le informazioni fornite dal servizio di "notifiche di esposizione" possono intrecciare questi dati per i loro fini.
Tutte queste situazioni di rischio evidentemente non sono tenute in considerazione dai vari Stati.
Molti degli Stati americani baseranno le proprie app sul sistema Apple e Google. Alabama, North Dakota e South Carolina sono stati i primi a impegnarsi in tal senso e così anche 22 autorità sanitarie nazionali sparse in cinque continenti (https://www.forbes.com/sites/rachelsandler/2020/05/20/alabama-north-dakota-and-south-carolina-to-debut-apple-and-googles-covid-19-contact-tracing/#19fa50721732).
Google ed Apple non hanno fornito dettagli precisi sui paesi inclusi nella lista, ma sappiamo che l'app italiana "Immuni" si baserà su queste API. Lo stesso ministro dell'Innovazione, Paola Pisano, in audizione alla Camera dei deputati il 30 aprile ha confermato che *"l'Italia baserà la sua applicazione sul modello che ci garantisce maggiore affidabilità e funzionamento su tutti i device nonché tutela della privacy, ossia il modello di Apple e Google"*. E probabilmente anche l'app tedesca, che tuttavia non è ancora stata annunciata ufficialmente.
Altri paesi che sicuramente si appoggeranno alle API di Apple e Google, in Europa, sono Austria, Svizzera, Norvegia, Irlanda, Paesi Bassi, Estonia, Lettonia, Canada, Finlandia e Danimarca, anche se pare che diverse soluzioni europee al momento non "comunicheranno" tra di loro. Questo perché, spiegano da Apple e Google, i paesi europei hanno deciso per un approccio "country-level", basato cioè sul tracciamento entro i confini nazionali, mentre ad esempio le app di diversi stati americani, che hanno scelto un approccio macro-regionale, saranno in grado di comunicare l'una con l'altra.
É però abbastanza sicuro che in una fase più avanzata le app possano aggiornarsi ulteriormente per ampliare la compatibilità con le app di altri paesi europei, nell'ottica di una riapertura completa dello spazio Schengen. La soluzione confezionata da Google ed Apple offre infatti per il futuro una piattaforma interoperabile, che è l'obiettivo dichiarato della Commissione Europea per tenere le frontiere aperte.
La collaborazione inusuale tra i nemici-amici Apple e Google si era resa necessaria, spiegano i portavoce delle aziende, per sopperire alle limitazioni tecniche della tecnologia Bluetooth. In particolare, dato che gli iPhone e gli smartphone Android, senza questo sistema, non sarebbero stati in grado di rilevare la presenza del Bluetooth sui reciproci sistemi operativi con facilità, mentre su iPhone non sarebbe stato possibile tenere attivo il Bluetooth quando un'app è chiusa, con queste API invece pare di sì (https://www.lagone.it/2020/05/21/apple-google-arrivano-gli-aggiornamenti-abilitano-le-app-covid-19/).
In pratica, con queste API, Google ed Apple hanno permesso agli sviluppatori di creare app di tracciamento dei contatti che funzioneranno per entrambi i sistemi operativi, risolvendogli molti problemi ma soprattutto imponendosi come soluzione che non poteva essere rifiutata (o quasi).
Il piano di Google/Apple è quello di incorporare il meccanismo di tracciamento direttamente nei sistemi operativi dei cellulari. Apple-Google, in pratica, stanno fornendo il modello mondiale a cui, volenti o nolenti, i vari stati e app nazionali dovranno sottostare, a meno di non volere incorrere in problemi di configurazione, compatibilità e interoperabilità, anche se alcuni stati come la Francia, che da tempo vanno sviluppando una sorta di sovranità digitale nazionale ed europea, hanno palesato il proprio malumore, facendo pressioni sulle due multinazionali (i francesi vorrebbero maggiore accesso alla tecnologia Apple giudicata troppo chiusa mentre sviluppano in proprio la loro infrastruttura di contact tracing).
Altri paesi hanno scelto di lanciare le proprie app di tracciamento dei contatti senza utilizzare Google e la tecnologia di Apple, tra cui Cina, India, Australia e Israele. Anche lo stato dello Utah ha

realizzato la propria app di tracciamento dei contatti che utilizza i dati sulla posizione GPS, a differenza di Apple e Google. Ma il Regno Unito, che aveva scelto il modello centralizzato, e non quello decentralizzato di Apple e Google per l'app di tracciamento sviluppata dal suo sistema sanitario, è tornata sui suoi passi abbandonando l'approccio centralizzato, esattamente come hanno precedentemente fatto anche Germania e Norvegia.
Questi paesi avevano inizialmente evidenziato, allo stesso modo della Francia, alcune problematiche nel sistema operativo di Apple. Sembra che il sistema operativo iOS, difatti, a differenza di quello Android di Google, non consente di eseguire il contact tracing con Bluetooth in background cioè ad applicazione non aperta sullo schermo (solo apparentemente spenta). Quindi, per funzionare, le app per iOS dovrebbero rimanere sempre aperte su schermo, compromettendo la durata della batteria. Per questo, il governo di Parigi sta rifiutando di aderire al protocollo di Apple e Google, almeno fino a che Apple non riduca, come chiesto dal governo francese, queste restrizioni di iOS per consentire un accesso più profondo da parte dell'app all'hardware e il pieno accesso dell'app al Bluetooth anche in background. Sembra un affare apparentemente secondario ma chi vuole a tutti i costi estendere le app di tracciamento nei vari paesi ha fatto bene i suoi conti: se il funzionamento di un'app consumerà troppa batteria sul cellulare, anche chi l'avrà scaricata tenderà a disinstallare l'applicazione. Una cosa che i governi vogliono assolutamente evitare!
Lo standard di Apple e Google semplifica la vita a molti sviluppatori, poiché abbatte i problemi di "comunicazione" esistenti. Tuttavia, ha anche i suoi limiti. Un altro esempio è che sebbene Apple abbia stimato di poter raggiungere almeno 2 miliardi di dispositivi iOS con questo servizio di notifiche di esposizione, l'aggiornamento potrà essere scaricato solo dai telefoni che supportano iOs 13, quindi dall'iPhone 6S del 2015 fino a quelli odierni, mentre quelli più vecchi ne rimarrebbero esclusi. Probabilmente, anche l'aggiornamento per il sistema operativo Android non potrà venire installato sui vecchi cellulari ormai fuori corso (https://www.wired.it/internet/web/2020/04/24/apple-google-contact-tracing/).
Bisogna considerare che per esempio in Italia il sistema operativo più diffuso è Android: circa tre smartphone su quattro usano il sistema operativo di Google. E qui saltano all'occhio alcune difficoltà tecniche. Perché Android cambia, e di molto, a seconda della fascia economica del telefono: più il telefono è economico, più il sistema operativo è vecchio. A tutto ciò va aggiunto che molti smartphone vecchi in circolazione non supportano la funzionalità Bluetooth low energy. Nelle aree più povere del pianeta gli smartphone compatibili sono meno diffusi.
É stimato che circa un quarto degli smartphone attivi nel mondo non ha il tipo di chip che supporta il Bluetooth a basso consumo necessario al tracciamento. Agli smartphone troppo vecchi, e con sistema operativo obsoleto, si aggiungono 1,5 miliardi di persone che usano i telefonini tradizionali, senza app e senza connessione. La situazione varia da Paesi come il Regno Unito, in cui l'80% degli adulti ha uno smartphone, all'India, dove "il 60-70% della popolazione non lo possiede.
Stando all'ultimo rapporto della Gsma, l'associazione mondiale degli operatori mobili, a fine 2019 ad avere uno smartphone erano il 76% degli europei, l'83% dei nordamericani e il 72% dei cinesi. In altre aree i numeri scendono di molto; in Asia Pacifico è il 64%, nell'Africa subsahariana il 45%. Il sistema di tracciamento, inoltre, non funzionerà sui circa 600 milioni di smartphone Android in Cina, che non hanno accesso al "negozio" on-line con le applicazioni di Google, così come sui nuovi smartphone di Huawei (Mate 30, P40) lanciati dopo il bando degli Usa alla Cina e sprovvisti dei servizi Google. Per risolvere parte del problema, Google vuole rilasciare una guida per consentire di replicare il sistema di tracciamento sui dispositivi non supportati (https://www.ansa.it/sito/notizie/tecnologia/software_app/2020/04/21/virus-no-tracciamento-per-2-mld-persone_594ba0ae-5ddc-4678-93f6-d87bd2c4c103.html).

L’uso dell’interfaccia di *Exposure notification* di Google e Apple, come confermato dalle due società, sarà resa utilizzabile solo per un’app alla volta per nazione. In Italia, quindi, solo “Immuni” potrà usarla, mentre le altre app sviluppate dalle concorrenti che hanno trovato impiego in alcune Regioni italiane resteranno a bocca asciutta e continueranno a funzionare solo sulla base della propria tecnologia di tracciamento, con gli inevitabili problemi di compatibilità e comunicazione tra i diversi sistemi operativi.
Le due società hanno anche comunicato che potranno disabilitare la loro interfaccia su base nazionale o regionale. Quindi, appena un governo riterrà giunto il momento di sospendere il contact tracing, i due colossi potranno “spegnerne il bottone” in una regione o in varie regioni, mentre magari a pochi chilometri di distanza, in un’altra regione indicata come più a rischio per un numero di contagiati più alto, il tracciamento potrebbe proseguire.
Ma come fidarci delle rassicurazioni di mega-corporation che vedono il mondo come un qualcosa di loro proprietà? Per dire, ha fatto scalpore negli Stati Uniti la vicenda che coinvolge la società madre di Google, Alphabet, che aveva scelto gran parte del lungomare di Toronto come prototipo per testare il proprio concetto di “città intelligente” iperconnessa (smart-city). Ebbene, il progetto di Toronto è stato chiuso dopo due anni di incessanti polemiche relative alle enormi quantità di dati personali che Alphabet aveva raccolto, una mancanza totale di protezione degli stessi e nessun vantaggio per gli abitanti della città americana. E chissà quanti altri dati società del genere riusciranno a carpire non appena il 5G farà capolino come soluzione predefinita per sviluppare ulteriormente il concetto di smart-city (intanto Apple sta per fare uscire sul mercato il suo primo iPhone 5G, l’iPhone 12 atteso a settembre del 2020).
Apple e Google hanno voluto mostrare, attraverso la loro collaborazione, che non si può fare un’app di contact tracing davvero efficace se non si sta alle loro regole. Se vogliono una app che funzioni su un grande numero di dispositivi, i governi devono attenersi alle direttive dei due colossi hi-tech. Google e Apple hanno così tanto potere da aver deciso quale tipo di protocollo di sistema verrà implementato sul pianeta. Abbracciando l’approccio decentralizzato di **DP-3T** - il responsabile della tecnologia Android di Google ha detto infatti che il loro protocollo è *"fortemente ispirato al protocollo DP-3T"* - limitano sì il potere dei governi che avrebbero preferito un approccio centralizzato, ma allo stesso tempo rafforzano il loro. In entrambi i modelli, centralizzato e decentralizzato, comunque non è chiaro come si possa impedire a un produttore di sistemi operativi di carpire le informazioni e i dati. Apple e Google hanno il controllo dei sistemi operativi. Per loro lavorano i migliori esperti del settore (per esempio, nel 2014 Google ha acquistato Deep Mind, un'azienda di intelligenza artificiale che già all'epoca impiegava alcuni dei principali esperti di intelligenza artificiale del mondo!). È chiaro che potranno, in ogni momento e come lo vorranno, gestire il flusso di dati raccolto attraverso il servizio di notifiche di esposizione.
Come sapremo se smetteranno di tracciarci quando la pandemia passerà? Come fermare qualcosa che si trova direttamente nel sistema operativo? Semplice: non si può, a meno di sbarazzarti di quel sistema operativo (ma varrebbe a dire del cellulare).

****

LE DIVERSE APP INTRODOTTE DAGLI ALTRI STATI EUROPEI

Gli Stati stanno applicando alle misure di contrasto alla pandemia e all'emergenza sanitaria la forma mentis tradizionalmente usata in settori come l'antiterrorismo e/o il sistema penale.
E non è un caso che fra alcune aziende che si sono fatte avanti, in Italia e all'estero, ci siano specialisti nel settore dell'intelligence, come **Cy4gate**, del gruppo **Elettronica**, *"tradizionalmente impegnato in tecnologie avanzate ad uso militare e di sicurezza nazionale"*, come ha spiegato il suo presidente (https://www.un-industria.it/canale/impresa-solidale/notizia/96445/elettronica-group-e-impresasolidale-e-presenta-la), che aveva messo gratuitamente a disposizione del governo italiano una propria piattaforma con tecnologie proprietarie per il tracciamento e incrocio dei dati rilevati dai dispositivi mobili per l'identificazione di picchi di contagio.
In Europa si è fatta avanti con alcuni governi l'americana **Palantir**, che fa analisi sui Big Data, ha stretti legami con CIA, FBI e Dipartimento Usa della Difesa, è stata accusata di muoversi in modo poco trasparente ed è stata criticata per aver aiutato il programma dell'ICE, l'agenzia americana sull'immigrazione, nel giro di vite contro gli immigrati clandestini in America (https://www.businessinsider.com/palantir-ice-explainer-data-startup-2019-7?IR=T).
In **Gran Bretagna,** l'azienda americana Palantir sta già fornendo il suo software di analisi dei dati, **Foundry**, al servizio sanitario nazionale (NHS) per l'emergenza COVID-19, mentre in **Francia** ha un contratto con l'antiterrorismo.
Ora Palantir - che negli Usa ha già lavorato col settore medico e con il Center of Disease Control and Prevention (la principale agenzia sanitaria a livello federale) per monitorare la diffusione del colera ad Haiti nel 2010, e che da tempo punta a penetrare il mercato europeo - starebbe presentando la sua offerta per il COVID-19 a governi di Francia, Germania, Svizzera e Austria.
Tra le sue proposte, uno strumento chiamato **Gotham**, *"noto per aiutare le agenzie di intelligence e le forze di polizia a tracciare individui, come avvenuto con l'ICE"*, e che potrebbe servire per sviluppare app di traccimento per il coronavirus (https://techcrunch.com/2020/04/01/palantir-coronavirus-cdc-nhs-gotham-foundry/?guccounter=1).

La "via orientale" al contact tracing è spesso stata vista come intrusiva, facente parte di società governate da mezze dittature o da dittature vere e proprie. In realtà quasi tutte le idee che oggi si sperimentano in Europa discendono dalle sperimentazioni fatte in Asia, dove è noto che una mole di dati personali sono stati carpiti dai governi e dalle società private sviluppatrici.
Ma ora facciamo una carrellata sulle principali app di contact tracing che sono state o verranno introdotte nei vari stati europei.

FRANCIA - Gli istituti di ricerca **INRIA -** *Institut national de recherche en informatique et en automatique* (ovvero l'istituto pubblico di ricerca nazionale francese specializzato in informatica e matematica applicata) e **Fraunhofer Heinrich Hertz Institut** (tedesco), membri del consorzio europeo **Pepp-PT,** hanno sviluppato e condiviso il loro protocollo di contact tracing che potrebbe essere utilizzato forse dal governo tedesco, sicuramente dal governo francese.
In Francia il protocollo di tracciamento della prossimità attraverso il Bluetooth è stato chiamato

ROBERT (ROBust and privacy-presERving proximity Tracing protocoled), reso noto il 18 aprile. Qui la documantazione: https://github.com/ROBERT-proximity-tracing/documents
ROBERT utilizza codici ID Bluetooth temporanei che cambiano ogni 15 minuti e che rimangono sul dispositivo ma anche sul server. Quando scarichi l'app di tracciamento dei contatti il server centrale genera e invia sul dispositivo dell'utente anche un ID permanente. Il server mantiene inoltre un elenco di tutti gli ID temporanei associati agli ID permanenti.
Le autorità che utilizzeranno il protocollo ROBERT gestiranno non dati anonimi, ma pseudonimi. In sostanza, l'autorità avrà un database centrale di codici ID permanenti con ogni ID che rappresenta una persona.
Se a un utente viene diagnosticato la positività al virus, dando il proprio consenso l'app caricherà sul server centrale l'elenco dei codici di altri utenti con cui hanno interagito negli ultimi 14 giorni. Ci sarà un punteggio di rischio associato a ogni persona. Quando il punteggio di rischio raggiunge una determinata soglia, l'utente viene avvisato (https://www.key4biz.it/contact-tracing-lapp-che-potrebbe-usare-francia-e-germania-e-il-data-breach-di-quella-olandese/301426/).
Bisogna dire che società tedesche e francesi, cioè appartenenti alle due economie più forti della UE, nel campo tecnologico stanno collaborando da diversi anni. Già a settembre del 2019 dalla collaborazione dei due paesi era nato il progetto **Gaia-X,** una piattaforma di servizi cloud europea per non dipendere più dalle aziende americane e cinesi. Con Gaia-X, le forze di polizia, gli ospedali, le istituzioni dei due paesi possono affidarsi a propri server invece che a quelli di Amazon, Google, Ibm o Microsoft. Insomma, una sorta di "sovranismo tecnologico" che guarda ad una ipotetica guerra commerciale dei dati a livello mondiale. Il ministro dell'economia tedesco Peter Altmaier aveva affermato allora che *"i dati diventeranno la materia prima più importante del futuro"*. (https://www.repubblica.it/dossier/tecnologia/onlife/2019/09/28/news/e_ora_germania_e_francia_vogliono_controllare_tutti_i_propri_dati-237185550/)
L'attivazione del protocollo ROBERT sarà propedeutica alla messa in opera dell'app di contact tracing francese, "**Stop-Covid"**, che non userà quindi le API di Apple e Google. All'introduzione di Stop-Covid stanno partecipando: il Governo francese, INRIA, INSERM-Istituto nazionale francese di ricerca medica e sanitaria, il servizio sanitario nazionale, diverse aziende di stato che si occupano dei sistemi d'informazione e grosse società come Dassault Systemes (società di software francese con sede a Vélizy-Villacoublay, che sviluppa progettazione 3D); Capgemini (Capgemini SE è una multinazionale francese che fornisce consulenza, tecnologia, servizi professionali e di outsourcing. Ha sede a Parigi ed ha oltre 200.000 dipendenti in oltre 40 paesi, di cui circa 120.000 in India); Lunabee Studio (società francese sviluppatrice di molte app e con molti clienti); Orange (ex France Télécom, è una multinazionale francese di telecomunicazioni. Ha 266 milioni di clienti in tutto il mondo e impiega 89.000 persone in Francia e 59.000 altrove. È il decimo operatore di rete mobile al mondo e il quarto in Europa dopo Vodafone, Telefónica e VEON).
Anche in Francia, molti media mainstream stanno presentando StopCovid come la soluzione per uscire più velocemente dal confinamento domestico e dalle restrizioni imposte dal governo. L'applicazione sarà volontaria, come spiegato dal ministro della sanità Olivier Véran, anche se c'è chi, come il sindaco di Parigi, Anne Hidalgo, nel suo piano di deconfinamento ha sostenuto l'idea che StopCovid possa fornire un *"certificato di immunità"*, senza contare che il sindaco la menziona come mezzo di controllo per i dipendenti pubblici della Città di Parigi. Mounir Mahjoubi, ex segretario di Stato per il digitale, ha sostenuto l'idea dell'obbligo per raggiungere il tasso di utilizzo del 60% della popolazione. Nella sua analisi, l'imprenditore Rand Hindi è giunto alla stessa conclusione, solo peggio: rendere obbligatorio lo scaricamento e consentire alle autorità di risalire alle persone che ricevono un allarme per "applicare" il loro confinamento! Niente di meno

(https://framablog.org/2020/04/10/stopcovid-le-double-risque-de-la-signose-et-du-glissement).
Il dibattito in Francia sulle tecnologie di tracciamento è presto salito di tono. Domenica 26 aprile, un gruppo di 471 esperti francesi ha firmato una lettera contro il modello centralizzato Pepp-Pt, dal titolo ***"Messa in guardia sulle applicazioni di tracciamento"*** (https://attention-stopcovid.fr), con l'adesione persino di 77 esperti della stessa Inria, la partecipata francese sul digitale che ha lavorato con il Fraunhofer Institut per ROBERT. La lettera affronta una serie di casi critici soprattutto dell'approccio centralizzato, ma anche di quello decentrato DP-3T.
Altre voci contrarie a StopCovid le trovate qui: https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid/
A oltre due settimane dal suo lancio, avvenuto il 2 giugno, l'app era stata scaricata solo dal 2% della popolazione francese. StopCovid inoltre non ha ricevuto il supporto di Apple, quindi non funziona su iPhone.
In Francia è anche girato largamente un *"**Appello per il boicottaggio dell'applicazione Stop-COVID19**"* del collettivo Ecran (*resistere alla gestione e all'informatizzazione delle nostre vite*) e sottoscritto da molti altri collettivi. In questo Appello, si afferma che *"Stiamo per fare un nuovo passo nella tracciabilità sistematica dei viaggi e delle relazioni sociali - almeno, inizialmente, per coloro che lo accettano. I risultati sulla salute sono più che incerti; le conseguenze politiche sono fuori dubbio". Per questo si invita tutti "a riflettere seriamente sulla possibilità di abbandonare il proprio smartphone e ridurre in modo massiccio il loro uso di tecnologie avanzate, tornando alla realtà (…), dovremo difendere i mezzi per incontrarci fisicamente, inventare o trovare luoghi di discussione pubblica in questo difficile contesto in cui si svolgeranno battaglie decisive. Naturalmente, dovranno essere presi accordi che tengano conto dei rischi di contagio. Ma la vita connessa non può sostituire permanentemente la vita vissuta, e i sostituti dei dibattiti con Internet non sostituiranno mai la presenza nella carne, il dialogo di persona"*
(https://www.terrestres.org/2020/04/27/ne-laissons-pas-sinstaller-le-monde-sans-contact/).
Oltre all'app di tracciamento, come riportato da BBC News, la Francia sta anche testando un software di monitoraggio della sorveglianza su autobus e mercati all'aperto per tenere sotto controllo la distanza sociale. Il sindaco di Cannes, David Lisnard, ha dichiarato alla BBC: *"Questa tecnologia non identifica le persone ma ci fornisce solo analisi matematiche per soddisfare le esigenze delle persone"*. Tuttavia, se le regole vengono violate, l'IA invierà un avviso automatico alla polizia e alle autorità cittadine.

GERMANIA - A fine aprile l'Ufficio federale di giustizia tedesco ha avviato procedimenti con minaccia di multe amministrative per la società di Boos, Arago, il cervello dietro a Pepp-PT. Motivo: cifre aziendali non divulgate e trasparenza insufficiente. Mancherebbero i rapporti di gestione economica degli ultimi anni, come prevede la legge in Germania. Inoltre si ipotizza l'evasione fiscale. Arago è stata comprata dalla società d'investimenti statunitense Kohlberg Kravis Roberts (KKR) nel 2014 per 55 milioni di dollari ma sembra certo che dal 2014 la parte finanziaria di Arago, **Machine Investors L.P.,** sia detenuta nel paradiso fiscale delle Isole Cayman, tramite la società lussemburghese Machine S.à.r.l. (https://www.stern.de/politik/deutschland/verfahren-gegen-handy-app-guru-chris-boos-9240196.html).

Sotto la pressione della critica e dell'opinione pubblica, il governo federale tedesco ha quindi preferito annunciare anch'esso un'inversione ad U per quanto riguarda la sua app di tracciamento: il 25 aprile 2020 il governo federale ha cambiato posizione e da allora ha favorito un approccio decentralizzato conducendo uno studio per "un'architettura decentralizzata" che "memorizza solo i contatti sui dispositivi e crea quindi fiducia".

Dunque anche la Germania è passata alla soluzione proposta da Apple e Google e DP-3T. Il governo tedesco ha infatti escluso il Fraunhofer Hertz Institut (HII), componente del Pepp-PT, dal progetto nazionale tedesco. Il Fraunhofer Heinrich assieme alla società francese INRIA, era l'istituto che aveva pubblicato il protocollo tedesco centralizzato PEPP-PT NTK.
Un comunicato stampa del 28 aprile 2020 svelava la prospettiva che l'app nazionale tedesca, che avrebbe dovuto chiamarsi "**Ito-App**" o "**Corona-App"**, fosse rilasciata dal **Robert Koch Institute**. Il Robert Koch Institute (RKI), infatti, fin dal 7 aprile 2020 lavorava allo sviluppo dell'app tedesca (all'inizio assieme a Boos e la sua azienda Arago). Quando ancora il governo tedesco partecipava in maniera ottimistica all'approccio centralizzato di Pepp-Pt, sotto la supervisione di Chris Boos, sono stati realizzati per "Corona-App" una serie di test con 48 soldati nella caserma Julius-Leber di Berlino per determinare l'efficacia e il tasso di errore del sistema. I test, su modelli di smartphone di vari produttori, includono anche esperimenti in luoghi mobili come le metropolitane, e sono stati realizzati dall'Istituto Fraunhofer con l'avvallo dei laboratori di collaudo Vodafone (https://www.computerbase.de/2020-04/corona-tracing-app-pepp-pt-problemen/).
Ma alla fine, sorpresa!, l'app ufficiale scelta dalla Germania è stata un'altra, lanciata il 15 giugno dopo solo 50 giorni di sviluppo (https://www.mesalliance.org/2020/06/18/sap-deutsche-telekom-publish-corona-warning-app-after-just-50-days-of-development-scn/) si chiama "**Corona-Warn-App**" (https://archive.org/search.php?query=creator%3A%22corona-warn-app%22) e lo sviluppo è stato portato avanti da **Deutsche Telekom** in collaborazione con **SAP (Systems, Applications & Products in Data Processing)**, una multinazionale tedesca che produce software aziendali. L'app si basa su Bluetooth, un approccio open source, gestione dei dati decentralizzata e si appoggia alla struttura messa a disposizione da Google e Apple (https://www.punto-informatico.it/corona-warn-app-contact-tracing-germania/). Scaricata più di 6,5 milioni di volte in 24 ore, in pratica, è identica all'italiana app "Immuni" (https://www.startmag.it/innovazione/app-anti-covid-19-germania-stile-immuni). SAP si è incaricata del lato dello sviluppo vero e proprioo, mentre Deutsche Telekom fornisce la rete e la tecnologia mobile e gestirà il "back-end" dell'app.
Ma questa non è l'unica app di contact tracing che è rimasta a lungo in progetto su suolo tedesco. Ce ne sono state diverse altre. Separatamente all'iniziativa del consorzio Pepp-PT, un'alleanza di start-up di Berlino, raggruppate sotto il nome di **"Healthy Together"**(https://www.healthytogether.io), composta da società di gestione dei dati e gruppi assicurativi e finanziari, aveva già dichiarato ad inizio aprile di voler lanciare una propria app di tracciamento dei contatti. L'iniziativa raggruppa alcune delle più grandi aziende del settore digitale e di gestione dei dati come Deloitte Legal, Bird & Bird, Datenscherschutzxperte.de, SKW Schwarz, Usercentrics, CMS, MyData e ReedSmith LLP. I soci fondatori sono Via (una società della Global Citizen Foundation), Finleap (il principale ecosistema Fintech in Europa) e il gruppo assicurativo digitale Wefox Group. I partner sono l'associazione tedesca Federal Association of German Startups e.V., Data4life (un'iniziativa della Fondazione Hasso Plattner), la banca online N26, i portali di viaggio Omio e GetYourGuide (Ottieni la tua guida), la piattaforma di consegna Delivery Hero, il costruttore di società BCG Digital Ventures, lo strumento HR Personio, lo spedizioniere digitale FreightHub e la società di mobilità TIER (Maggiori informazioni sono disponibili su https://gesund-zusammen.de).
Sascha Gartenbach, fondatrice e amministratore delegato di Via, aveva affermato che il gruppo Healthy Together era in contatto con PEPP-PT per collaborare: *"I nostri approcci sono complementari"*. Comunque i membri hanno l'obiettivo di fornire risorse e consulenza digitale anche per lo sviluppo di strumenti digitali che sono già in costruzione.
"**CovApp"** è invece un'app Web sviluppata da **Berlin Charité** e **Data4Life**, con la quale l'ospedale

“ottimizza” i propri processi. L'app contiene un questionario medico che chiede informazioni sui sintomi attuali e sui possibili contatti con positivi. Dopo aver risposto al questionario, l'utente riceve le informazioni se deve effettuare un test o una visita medica - sia esso da un medico di famiglia, presso lo Charité o altrove. CovApp è open source con una licenza MIT, disponibile gratuitamente su GitHub.
Hannover Medical School (**MHH**) è stata invece coinvolta nello sviluppo dell'app “**Geohealth”**, una delle numerose app che si è tentato di introdurre su suolo tedesco.
Dato che non si fanno mancare niente, in Germania vi è anche un altro protocollo aperto per il tracciamento, oltre a quello di Pepp-PT: la **OHIOH-APP** (https://ohioh.de/). L'app della società OHIOH è una piattaforma che utilizzata GPS, Bluetooth e codice QR. Dato che, come scrivono sul loro sito, *“sebbene il posizionamento sia molto avanzato, ha anche i suoi limiti. Un esempio è che non è possibile penetrare pareti e soffitti in calcestruzzo, quindi uniamo altre tecniche come la tracciabilità Bluetooth e il nostro sistema di codici QR”*. Il codice QR serve per accedere a negozi e luoghi pubblici. Una volta impostata, l’app funziona in modo completamente indipendente in background, ed è utilizzabile in tutto il mondo. Il server si trova in Germania. Le aziende che fanno parte di OHIOH fanno parte della **TNC Coalition**, un raggruppamento internazionale di giovani tecnologi nerd che stanno rovinando il mondo (https://tcn-coalition.org/partners-and-members) e di cui fanno parte alcuni dei progetti analizzati in questa collezione degli orrori, come l’app “Covid Community Alert” italiana, la seconda arrivata nella scelta del governo dopo “Immuni”.

AUSTRIA - La Croce Rossa austriaca ha pubblicato l'app di tracciamento **"Stopp Corona"** di **Accenture GmbH** già il 25 marzo. L'app può utilizzare il Bluetooth o un segnale acustico per riconoscere gli smartphone vicini che utilizzano l'app. Questi smartphone sono elencati in modo che l'utente possa utilizzare questo elenco per registrare manualmente le persone. Con l'app tutte le persone con cui si è stati in contatto possono essere informate di un test positivo al SARS-CoV-2. A metà aprile, un aggiornamento ha aggiunto la possibilità di registrare automaticamente (quindi non solo manualmente) i contatti e di inviare un messaggio. Pare che l'app sia compatibile con l’approccio decentralizzato DP-3T.

REGNO UNITO - il progetto iniziale dell’app di contact tracing **“NHS COVID-19”** (https://en.wikipedia.org/wiki/NHS_COVID-19) è stato sviluppato da **Pivotal**, azienda di software della California e dalla divisione digit di **NHSX**, azienda del Servizio sanitario nazionale britannico (https://digital.nhs.uk). NHSX sperava che almeno il 50 - 60% della popolazione scaricasse l’applicazione, mettendo a punto alcuni dettagli: uno dei criteri che sta prendendo in considerazione è il raggio di azione entro i 2 metri.
L'app memorizza all’inizio solo gli eventi di contatto sul dispositivo di ciascun individuo, una volta che un utente segnala se ha sintomi o test positivi, i dati di contatto vengono caricati su un server centrale che memorizza i dati a tempo indeterminato e da cui non può essere cancellato. Questi dati possono anche essere utilizzati per la ricerca sulla salute pubblica, il che solleva nuovamente domande sulla privacy e sulla possibilità di una nuova identificazione delle persone.
Il governo, inoltre, come altre nazioni, ha proposto il "passaporto sanitario" digitale, ovvero si prepara a rendere obbligatoria la presentazione di una certificazione di immunità “Covid-free” per viaggiare. Il ritornello spesso ripetuto è che senza certificati sanitari digitali, semplicemente non sarebbe sicuro tornare al lavoro, al tempo libero o viaggiare. Per fornire il certificato digitale sarebbe utilizzata la biometria facciale, per dimostrare quali lavoratori hanno già avuto il Covid-19 e sono immunizzati. La società britannica **Onfido**, specializzata nella verifica delle identità delle

persone utilizzando proprio la biometria facciale, ha fornito piani dettagliati al governo ed è coinvolta in una serie di colloqui con l'esecutivo su ciò che potrebbe essere implementato in tutta la nazione, visto che ora la tecnologia di Onfido è in fase pilota in altri paesi. Matt Hancock, segretario alla Salute del governo britannico, ha dichiarato che "*si potrà introdurre qualcosa come un certificato di immunità o forse un braccialetto che dice 'io ho avuto il* Coronavirus *e sono immune, non posso trasmetterlo ed è altamente improbabile che lo riprenda*'". Intanto, già messo in pratica da Emirates Airlines, è l'esame del sangue obbligatorio prima del volo (https://www.tuttosport.com/news/attualit/cronaca/2020/04/17-68945950/sun_coronavirus_per_viaggiare_servira_un_certificato_di_immunita_/).
A metà maggio, subito dopo essere stata lanciata l'app, due esperti di sicurezza informatica (Chris Culnane e Vanessa Teague), hanno trovato non una ma sette pericolose falle sull'app di tracciamento dell'NHS scelta dal Governo inglese attualmente ancora in fase di sperimentazione sull'isola di Wight, che ha una popolazione di circa 140.000 abitanti. Al 15 maggio, oltre 72.000 avevano scaricato l'app, equivalente a più della metà della popolazione dell'isola.
Alla fine, dati i ritardi e i problemi tecnici, il governo inglese, come prima altri paesi, ha deciso di abbandonare il progetto con sistema centralizzato, per abbracciare invece per la sua app NHS il sistema decentralizzato di Google ed Apple (https://www.theguardian.com/world/2020/jun/18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models).
Esiste anche un'altra app inglese che si chiama **"Covid Symptom Study"** *(*https://en.wikipedia.org/wiki/COVID_Symptom_Studyed) ed è stata sviluppata dal *King's College London*, Zoe Global Limited e *Guy's and St Thomas' Hospitals*.

IRLANDA - Anche l'Irlanda sta sviluppando un app di contact tracing col Bluetooth, gestita dall'azienda sanitaria nazionale HSE. Non può essere scaricata da minori di 16 anni. La tecnologia su cui si basa l'app dell'Irlanda è stata ideata per funzionare con i telefoni più recenti e potrebbe non funzionare con i vecchi smartphone. Nel caso di Android, ciò significa Android 6 o versioni successive. Secondo Statcounter, il 10% dei telefoni Android irlandesi utilizza sistemi più vecchi di quello. Allo stesso modo, con un iPhone 6, iPhone 5 (o 5C o 5S) o qualsiasi altra cosa più vecchia di un iPhone 7, potrebbe per fortuna non funzionare (*https://www.independent.ie/business/technology/irelands-contact-tracing-app-may-struggle-and-not-just-on-privacy-39192270.html*).

PAESI BASSI – In **Olanda** l'app "**Covid19 Alert!**" (https://www.covid19-alert.eu/) consente di comprendere se con lo smartphone si è stati vicini a quello di un paziente con il coronavirus, esattamente come accade per altre applicazioni. "Covid19 Alert!", ha già subito quello che in gergo si chiama un "data breach". Stando a quanto scrive il quotidiano *DeStandard*, circa 100-200 nomi, email, password criptate sono state rese pubbliche. *"Un errore umano", ha* detto uno dei creatori dell'app! Il gruppo che ha sviluppato l'app comprende Università di Antwerp in Belgio, Prof Project, Quinto Impacto e e la rete della Digibyte Foundation.
Un altra app di tracciamento in Olanda è **"PrivateTracer"** proposta dalle società **Milvum, YES! Delft, Odyssey ed Hague** (https://www.privatetracer.org/), con un consorzio pubblico-privato che ha una serie di partner tra cui Microsoft. È basata sul protocollo DP-3T.
Nel **Belgio**, invece, una start-up locale ha sviluppato un sistema di tracciamento dei contatti che avvisare i dipendenti sul posto di lavoro di una potenziale infezione da coronavirus. Il sistema, che si chiama **"Savitas"** (che sta per Scoped Anonymous Viral Infection Tracing At Scale), è stato annunciato dalla start-up belga **Esoptra,** dalla società di ispezione&controllo **Vinçotte** e da

Mensura, un servizio di medicina del lavoro esterno che supporta Savitas. Il sistema è inoltre supportato dai consulenti di **Attentia** e **Vias Institute**. L'Università di Anversa fornisce supporto accademico all'iniziativa. Savitas è attualmente in fase di test.
L'app non utilizza segnale GPS o Bluetooth ma tramite la scansione di un codice QR sul proprio smartphone. Chiunque abbia scannerizzato lo stesso codice QR contemporaneamente ad una persona infetta sul luogo di lavoro, viene avvisato alla successiva scansione o quando visita il sito Web (https://www.brusselstimes.com/all-news/belgium-all-news/108517/belgians-develop-anonymous-contact-tracing-system/).
Nel **Liechtenstein**, dove si registrano pochi casi di Covid-19, è in corso una sperimentazione su base volontaria che coinvolge oltre duemila persone, circa il 5% della popolazione, tra i 33 e i 52 anni che usano un braccialetto biometrico per monitorare il loro stato di salute e i loro dati personali. Se verrà giudicato soddisfacente, l'esperimento verrà esteso su tutti i cittadini in autunno, quando secondo le autorità locali sarà altamente probabile una seconda ondata pandemica.

POLONIA - In Polonia si sta invece usando gli smartphone per imporre l'auto-quarantena. L'app "**Home Quarantine"** della Polonia impone di inviare, in seguito a un messaggio, regolari selfie geolocalizzati per vedere se si è in casa oppure no e si hanno solo venti minuti per rispondere a una richiesta di foto, al rischio di vedersi bussare alla porta dalla polizia (https://www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3?IR=T). Il suo uso è volontario, almeno come è volontaria la risposta a 'un'offerta che non si può rifiutare', per citare un celebre film. *"Le persone in quarantena possono scegliere"* - ha infatti detto il portavoce del ministro polacco per il Digitale - *"o ricevono visite inaspettate dalla polizia o scaricano questa app" (*https://www.valigiablu.it/coronavirus-emergenza-tecnologia/).
É comunque attiva anche **"ProteGO"**, l'app di contact tracing supportata dal ministero per gli affari digitali e sviluppata da Jakub Lipinski, Karol Kostrzewa e Dariusz Aniszewski.

NORVEGIA – Si prevede di testare l'efficacia dell'app "**Smittestopp",** sviluppata dal **Simula Research laboratory** (https://en.wikipedia.org/wiki/Simula_Research_Laboratorye) e dall'Istituto pubblico di salute norvegese, con un budget di sviluppo di circa 5 milioni di $, ed inizialmente oltre a tracciare col Bluetooth accedeva alla posizione GPS e richiedeva i numeri di telefono. Ma ha visto un uso considerato limitato dal governo, a causa di un basso numero di nuove infezioni. Il 30% dei norvegesi ha scaricato l'app del proprio governo, secondo il New York Times. Come dichiarato da Gun Peggy Knudsen, vicedirettore dell'Istituto pubblico di salute norvegese in un'intervista, Smittestopp, proverà adesso ad interfacciarsi alle API di Apple-Google: *"Se il tracciamento è molto migliore con lo strumento Apple-Google, allora forse dovremmo cambiare e prendere in considerazione ciò che dobbiamo fare per fare il passaggio"*, ha detto Knudsen (https://venturebeat.com/2020/05/21/23-countries-seek-access-to-apple-and-googles-contact-tracing-technology/). Nel frattempo, l'istituto nazionale di sanità pubblica norvegese ha annunciato a giugno di sospendere i lavori sulla sua app di tracciamento dei contatti e di eliminare tutti i dati raccolti attraverso di essa, a seguito di una decisione dell'autorità di protezione dei dati del paese di vietare il trattamento dei dati personali (posizione e num. di telefono) dell'app (https://inst-search.com/2020/06/16/germany-to-launch-contact-tracing-app-uk-plans-unclear/).

FINLANDIA – l'app di contact tracing **"Ketju"** (www.ketjuapp.com) per Android ed iOS è stata sviluppata da una serie di imprese guidate da 2M-IT. Funziona con Bluetooth.

Al momento è in sperimentazione al Vaasa Central Hospital dove i dipendenti adotteranno l'app durante il progetto pilota e imiteranno le azioni dei cittadini e delle autorità sanitarie dopo aver simulato le diagnosi di coronavirus.
Il processo è tra i primi a utilizzare l'approccio decentralizzato basato su DP-3T in Europa. Finanziata dal fondo finlandese per l'innovazione SITRA, "Ketju" è il risultato della collaborazione avviata su iniziativa di Business Finland. Diverse altre opzioni per lo sviluppo di una soluzione di tracciamento nazionale sono state esplorate per settimane dalle società Fraktal, Futurice e Reaktor (https://www.goodnewsfinland.com/app-for-tracking-coronavirus-contacts-trialled-in-finland/).

MACEDONIA DEL NORD - Il governo ha lanciato **"StopKorona!"** il 13 aprile 2020, diventando il primo paese dei Balcani occidentali a lanciare un'app di tracciamento per il coronavirus.
L'app funziona attraverso il tracciamento di prossimità di dispositivi mobili, utilizzando la tecnologia Bluetooth ed è stata sviluppata e donata al governo dalla società di software **Nextsense** con sede a Skopje. La app richiede i numeri di cellulare degli utenti, memorizzati su server gestiti dal Ministero della Salute.
Il 28 aprile **StopKorona!** di **Nextsense** è stata presentata al festival "Come il mondo risponde a Covid-19", organizzato dalla piattaforma giornalistica internazionale Outriders e a cui hanno partecipato sviluppatori da tutto il mondo (https://nextsense.com/ns-newsarticle-stopkorona-by-nextsense-on-the-festival-on-how-the-world-responds-to-covid-19.nspx).
Nextsense, che opera nel settore da 15 anni, nel paese aiuta governo e parlamento nella digitalizzazione informatica e ha sviluppato il nuovo sistema centralizzato di prenotazione elettronica per l'emissione di farmaci e per le esigenze del Fondo di assicurazione sanitaria della Macedonia settentrionale. È fortemente presente nell'Europa sud-orientale, Nord Macedonia, Repubblica Ceca (attraverso il distributore **Askon**) e Ungheria (atraverso **Biztributor**).

UNGHERIA - "**VírusRadar"**, un'app di contact tracing per Android è stata lanciata il 13 maggio 2020, voluta fortemente dal Ministero dell'Innovazione e della Tecnologia. Presto seguirà una versione iOS. L'app utilizza la tecnologia Bluetooth per tracciare gli ID dei cellulari a meno di 2 metri per più di 20 minuti negli ultimi 14 giorni. Il sistema è stato sviluppato, come nel caso della Macedonia del Nord, da **Nextsense e Kifu**, e basato sulla tecnologia Nextsense Contact Tracing. È gestita dal Ministero dell'innovazione e della tecnologia ungherese, gestito dall'Agenzia governativa per lo sviluppo IT ed è supportato da Biztributor, il distributore di Nextsense per l'Ungheria.
Ha contribuito alla distribuzione dell'applicazione e **Vodafone Ungheria** che offre SMS gratuiti per incoraggiare la registrazione volontaria sull'app.
L'app è volontaria. Ai positivi al virus, lo Stato ungherese chiede di condividere le informazioni con epidemiologi che identificheranno i numeri di telefono degli altri utenti che sono stati in contatto con loro per mandare una notifica via cellulare. I numeri di telefono vengono memorizzati sui server del Ministero dell'innovazione e della tecnologia (https://virusradar.hu e https://apk.tools/details-virusradar-apk/).

REPUBBLICA CECA - Il governo ha lanciato un'app di tracciamento ispirata a Singapore chiamata "**eRouška"** (**eFacemask**). L'app è stata voluta dal ministero della salute e dell'igiene e sviluppata ad inizio aprile dalla comunità IT locale, rilasciata come open source e consegnata al governo. Utilizza Bluetooth LE.

ISLANDA - l'app ufficiale del governo islandese "**Rakning-Covid-19"** è una delle prime ad essere introdotte in Europa ad inizio aprile dal Iceland's Department of Civil Protection and Emergency Management and Directorate of Health, usa il GPS per Android e iOS la cui interfaccia utente di base e la maggior parte dei contenuti è la stessa della pagina Web https://www.covid.is
Una volta scaricata e installata, Rakning C-19 chiede di fornire il proprio numero di cellulare per ricevere un codice da inserire nell'applicazione, per registrarsi. Il numero viene conservato in un database centralizzato di SENSA, società di servizi di proprietà della principale società di

telecomunicazioni islandese. L'app chiede poi di avere accesso alla propria posizione geografica, che viene rilevata dallo smartphone tramite il GPS.
Dopo che l'app è stata configurata, viene eseguita in background e salva la posizione del telefono più volte all'ora. Vengono memorizzati i dati degli ultimi 14 giorni. Se al proprietario del telefono viene diagnosticata la malattia di Covid-19, viene chiesto alla direzione della sanità di condividere i dati sulla posizione al fine di identificare le persone che da mettere in quarantena.
L'Islanda ha subito predisposto anche un piano di test degli infetti a tappeto, lo ha portato avanti per il governo la DeCode genetics, un'azienda islandese che si occupa di biotecnologie (https://www.esquire.com/it/news/attualita/a32472193/coronavirus-islanda).
Secondo uno studio del MIT dell'11 maggio 2020, aveva il più alto tasso di penetrazione di tutti i tracker di contatto al mondo, essendo stato scaricato dal 38% degli islandesi.
Si utilizza volontariamente e memorizza i profili di movimento dell'utente sul proprio smartphone per due settimane. In caso di infezione, le autorità possono utilizzare l'app per monitorare dove si è verificata l'infezione e quali altri contatti si sono verificati (vedi anche https://en.wikipedia.org/wiki/COVID-19_pandemic_in_Iceland).

SVIZZERA - l'app "**SwissCovid**" che si serve del protocollo decentralizzato DP-3T è disponibile pubblicamente su Android e iOS e può essere utilizzata come base per altre app nazionali (https://www.bag.admin.ch/bag/it/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/situation-schweiz-und-international/datenschutzerklaerung-nutzungsbedingungen.html).
È stata patrocinata dalla Federal Office of Public Health FOPH. Dopo un primo test-pilota su larga scala su dipendenti di ospedali, istituzioni ed esercito, DP-3T si prepara a rendere l'app disponibile per tutta la Svizzera a cominciare da metà giugno.
Questo test-pilota è il primo al mondo, su scala così allargata, che si serve degli aggiornamenti API di Google e Apple. Il server statale è gestito dalla Confederazione elvetica.
L'app **Next Step** (https://next-step.io/en) è un'altra app di tracciamento dei contatti sviluppata dalla società di Zurigo **Ubique** (https://www.ubique.ch/). Si basa anch'essa sul protocollo DP-3T.

GEORGIA - Un'app di tracciamento dei contatti sviluppata dal ministero della salute e dall'associazione austriaca **Novid 20** è stata introdotta in **Georgia**. Anche questa si chiama **StopCovid**. Il codice sorgente è stato pubblicato come open source su GitHub. L'app è attualmente in uso nel paese.

GRECIA – In Grecia, infine, nella regione dell'Attica, vi è **DOCANDU Covid Checker**, che però non fa contact tracing ma è un'app con diario clinico self-diagnostic e dottore on-line. DOCANDU è una startup greca con sede nel Regno Unito. Va comunque ricordato che la Grecia è stata uno dei primi paesi a livello mondiale che ha introdotto misure restrittive negli spostamenti per prevenire la diffusione del COVID-19.

CIPRO - Al momento, secondo fonti della Commissione europea, sembra che Cipro stia vagliando soluzioni che sfruttano sia Bluetooth che GPS per lo sviluppo della propria app nazionale.

***

IL CONTACT TRACING FUORI DALL'EUROPA

STATI UNITI D'AMERICA – Il **Nord Dakota**, ha offerto la prima app di tracciamento dei contatti negli Stati Uniti: la sua app "**Care19" (**come strumento di diario clinico) e l'app di contact tracing "**Care19 Exposure"** basata sulla tecnologia Apple-Google.
Fra le varie app di contact tracing, ad aprile il **MIT di Boston (Massachusetts Institute of Tecnology)** ha coordinato il progetto **Safe Paths** (http://news.mit.edu/2020/safe-paths-privacy-first-approach-contact-tracing-0410), un progetto internazionale cui hanno collaborato l'inventore del protocollo di cifratura a chiave simmetrica RSA (**Ramesh Raskar** che ha guidato l'impresa), esperti ed atenei indiani, francesi, canadesi, tedeschi, del Regno Unito, del Vietnam ed anche italiani (https://www.media.mit.edu/projects/safepaths/overview/), con il contributo della Harvard University, la Stanford University e il SUNY Buffalo e col contributo clinico dalla Mayo Clinic e dal Massachusetts General Hospital, supervisionato da membri dell'Organizzazione mondiale della sanità, del Dipartimento americano per la salute e i servizi umani e il Graduate Institute of International and Development Studies. Altre aziende che hanno partecipato al progetto sono TripleBlind, Public Consulting Group e Earned Media Consultants.
Safe Apps è un protocollo che può essere adottato internazionalmente dalle diverse app che si basa sulla geolocalizzazione tramite GPS e il tracciamento dei contatti tramite Bluetooth. Quindi un sistema misto. L'approccio dell'archiviazione dati è decentrato sul server locale del cellulare, inviati a terzi col consenso dell'utente.
"**Healthy Together"**, della **Twenty Holdings Inc**. (https://www.twenty.co/) invece opera principalmente nello stato dello **Utah** e raccoglie dati GPS per le autorità sanitarie. È una app di tracciamento dei contatti sviluppata per IOS di Apple in collaborazione con lo Stato dello Utah (https://apps.apple.com/us/app/healthy-together-covid-19/id1507570835).
Altra app di tracciamento americana è **"Covid Watch"** (https://www.covid-watch.org) realizzata da un team di ricercatori guidati dall'**università di Stanford** e **Waterloo**, e che si basa ancora sul Bluetooth e su un approccio decentralizzato.
Altra app di tracciamento che è stata rilasciata si chiama "**NOVID"** ed invece "**CoEpi"** (del MIT) e "**COVID Control"** raccolgono dati sullo stato di salute: temperatura corporea e altri sintomi associati a Covid-19.
Poi, ovviamente, c'è l'iniziativa congiunta di tracciamento dei contatti di **Google** e **Apple**.
Il 10 aprile 2020, Google e Apple hanno annunciato un progetto per fornire ad una serie di app di contact tracoing nel mondo un'unica piattaforma sviluppata attorno ad API pubbliche che utilizzano il Bluetooth Low Energy. Negli States, la piattaforma funziona sempre come per le altre nazioni, ovvero tracciamento tramite Bluetooth registrando i contatti sul cellulare per 14 giorni, condivisione dei dati relativi ai contatti delle due settimane precedenti e inoltro di un messaggio automatico a questi contatti, ma per chi contrae il virus è previsto che si ricevano notifiche e istruzioni sui passaggi successivi forniti da fonti come l'OMS e il CDC (Centers for Desease Control). Google ed Apple si troveranno così a custodire una mole di dati (di movimento e sanitari) davvero incredibile.
Il progetto di Google ed Apple non è solo utilizzabile negli Stati Uniti, ma rappresenta una proposta che ha trovato purtroppo estimatori in molti paesi.
A metà aprile, perfino il presidente USA, Donald Trump, che di certo non può essere annoverato nel campo dei paladini della libertà, in una conferenza alla Casa Bianca ha detto che le tecnologie di tracing anti Covid-19 messe a punto congiuntamente da Google e Apple pongono *"grandi problemi di costituzionalità"* per *"molte persone"*, anche se alla fine anche gli USA hanno accettato il sistema delle due mulinazionali (https://www.key4biz.it/covid-19-per-trump-il-sistema-di-tracing-di-apple-e-google-pone-grandi-problemi-di-costituzionalita/300240/).
Ma negli Stati Uniti non si usano solo le app di tracking ma anche l'analisi aggregata sugli spostamenti delle persone. Aldilà delle app di tracciamento, gli Usa infatti hanno schierato la Silicon Valley per l'impiego dei dati degli utenti per tracciare la diffusione di Covid-19.

Le aziende tecnologiche statunitensi, incluse Google, Facebook e Amazon, l'azienda di estrazione dati Palantir, e Clearview AI, un'azienda molto controversa di riconoscimento facciale, stanno lavorando insieme alla Casa Bianca, al Cdc, e al National Institutes of Health per fare un modello dell'epidemia e sviluppare un modo per monitorare le persone che sono risultate positive al Covid-19. Il governo federale si è confrontato con queste ed altre società tecnologiche per usare i dati sulla geolocalizzazione raccolti dagli smartphone degli americani, in forma aggregata. In questo modo il governo ha controllato se le persone stavano mantenendo le distanze di sicurezza. *"Stiamo valutando i modi in cui le informazioni aggregate e anonime sulla posizione potrebbero aiutare nella lotta contro il Covid-19"*, ha confermato alla Cnn il portavoce di Google Johnny Luu. *"Un esempio potrebbe essere quello di aiutare le autorità sanitarie a determinare l'impatto del distanziamento sociale, in maniera simile al modo in cui mostriamo i tempi di attesa dei ristoranti popolari e i modelli di traffico in Google Maps"* (https://edition.cnn.com/2020/03/18/tech/us-government-location-data-coronavirus/index.html).

In quanto a Facebook si pensa possa fornire dati di localizzazione come già ha fatto per vari scopi, tra cui il monitoraggio dei movimenti dei cittadini durante gli incendi boschivi in California.

L'analisi dei dati aggeragti, però, non è stata fornita solo da Google o Facebook, ma pure da una startup, **Unacast**, che ha usato i dati di localizzazione ricavati da una serie di app per lo shopping, il gaming ecc. Insomma dai dati raccolti normalmente da società di marketing (https://www.unacast.com/covid19/social-distancing-scoreboard).

Tutte le più note aziende tecnologiche stanno dunque aiutando il governo a sviluppare un modello e a tracciare il virus, ma alcune di queste aziende hanno un curriculum pessimo: **Palantir** per esempio, che è stata fondata dalla Cia, e secondo un'intervista di Sam Biddle a *Intercept "ha aiutato a espandere e accelerare il network di spionaggio globale della Nsa"* (https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world).

Alcune indiscrezioni sulle pratiche aziendali di **Clearview AI** – una startup per il riconoscimento facciale che conta centinaia di forze dell'ordine tra i suoi clienti, e che sta collaborando a sua volta col governo a stelle e strisce – hanno causato allarme diffuso tra la popolazione e anche tra alcuni difensori della privacy e portato a chiedere di bandire la pratica del riconoscimento facciale.

I colossi tlc che gestiscono le comunicazioni tramite smartphone di milioni di americani hanno però anche accesso a informazioni dettagliate sulla posizione GPS. Ma non è del tutto chiaro se l'amministrazione Trump abbia chiesto loro di fornire quei dati. Alla domanda della *Cnn* se ha partecipato alle audizioni del governo degli Stati Uniti sull'utilizzo dei dati sulla posizione, il portavoce di AT&T Michael Balmoris ha risposto "No". I portavoce di Verizon, T-Mobile e Sprint non hanno risposto a una richiesta di commento (https://www.startmag.it/innovazione/ecco-cosa-studia-trump-con-google-facebook-per-tracciare-la-diffusione-del-coronavirus/).

Quel che è certo è che la Casa Bianca, in partnership con il **Centers for Desease Control** (Cdc), ha iniziato a tracciare gli smartphone degli americani per vedere dove vanno durante l'epidemia. Quando gli analisti dei dati hanno notato che un gran numero di persone si stava radunando al Prospect Park di Brooklyn, hanno allertato le autorità. Il Center for Disease Control (CDC) è la principale agenzia federale incaricata di salvaguardare la salute pubblica negli Stati Uniti. Il CDC ha anche una vasta gamma di app, tra cui alcune appositamente per gli operatori sanitari. Ma anche app per bambini, oltre ad alcune che offrono strumenti di sicurezza sul posto di lavoro, rilevatori di salute ecc. L'app mobile principale di CDC è disponibile su dispositivi Android e Apple. Contiene informazioni sullo stato attuale della pandemia e consigli utili per gli abitanti degli Stati Uniti su come proteggersi dal contagio. A causa della mancanza di test disponibili negli Stati Uniti, l'app

CDC fornisce anche un autocontrollo dei sintomi in caso di malessere: domande e risposte per aiutare a identificare un possibile positivo.
La **Federal Emergency Management Agency** (FEMA) ha anch'essa sviluppato un'app pubblica per dispositivi Android e Apple che fornisce notifiche relative a emergenze o focolai agli abitanti. Se non si installa l'app FEMA, si può comunque trovare un'enorme quantità di informazioni importanti sul suo sito web.
"**Tracker COVID-19"** del Center for Systems Science and Engineering (CSSE) presso la Johns Hopkins University utilizza **ArcGIS**, un sistema proprietario di "modellizzazione geografica" per analizzare e mappare i dati sullo stato attuale della pandemia.
La **MIT technology rewiew** ha invece avviato un'analisi su ciò che si sta facendo in tutto il mondo sulle app di tracciamento, monitorando la situazione in un unico database chiamato **Covid Tracing Tracker**, per acquisire i dettagli di ogni app di tracciamento dei governi nazionali.
I primi della classe, secondo l'analisi del MIT, sono gli australiani, gli austriaci, gli islandesi, i norvegesi e gli abitanti della Repubblica Ceca, le cui app hanno ottenuto il punteggio massimo. L'analisi ha censito anche la App italiana Immuni, all'inizio assegnando quattro stelle su cinque, con l'unica mancante che riguarda la politica di distruzione dei dati. Alla fine poi gli ha concesso 5 stelle (http://www.quotidianosanita.it/studi-e-analisi/articolo.php?articolo_id=85442).
Da parte sua, l'**Organizzazione mondiale della sanità** (OMS) ha creato una app per combattere la diffusione di notizie false sul coronavirus; la nuova applicazione, annunciata dal direttore dell'Oms Tedros Adhanom Ghebreyesus sul suo account Twitter, si chiama **"WHO MyHealth"** e può essere scaricata per iOS e Android, fornisce notifiche e informazioni sul Covid-19, comunica a chi la usa se si trova in una zona ad alto rischio o se qualcuno nell'area ha dichiarato di aver contratto il virus e fornisce strumenti per l'autodiagnosi nel caso si avessero sintomi simili a quelli del coronavirus; sarà disponibile in inglese, francese, cinese, spagnolo, arabo e russo. Il software è stato sviluppato da ex dipendenti di Google e di Microsoft con la collaborazione di consulenti dell'Oms e volontari del gruppo WHO Covid App Collective (https://www.repubblica.it/tecnologia/mobile/2020/03/30/news/coronavirus_in_arrivo_l_app_dell_oms_su_covid-19-252724526/).
Dobbiamo poi citare, della **Rockefeller Foundation**, il ***"Piano d'azione nazionale per i test COVID-19 - Passaggi strategici per riaprire i nostri luoghi di lavoro e le nostre comunità"***, che popone un quadro strategico che è destinato a diventare parte di una sorveglianza permanente e strutturata di controllo per limitare fortemente la libertà personale e la libertà di scelta. Il piano Rockefeller per gli Stati Uniti prevede l'avvio di test COVID-19 e la tracciabilità di 1 milione di americani alla settimana, aumentando gradualmente fino a 3 milioni e quindi 30 milioni a settimana (il "piano 1-3-30") nei prossimi mesi fino a che l'intera popolazione sia stata coperta. I risultati dei test verrebbero poi raccolti su una piattaforma digitale in modo che la traccia dei contatti possa essere eseguita quando qualcuno risulta positivo. Il Piano addita i dubbi e la salvaguardia della privacy come un ostacolo da eliminare (https://shazidamain.com/2020/05/15/contact-tracing-apps-violate-privacy/).
In piena pandemia gli Usa hanno infine legalizzato il permesso di spiare Internet senza limiti, attraverso la proroga delle norme liberticide post-11 settembre del Patriot Act, poi ribattezzato Freedom Act, che dal 2001 ha permesso agli Stati Uniti di spiare, in segreto, l'attività di chiunque, compresi i leader di altri paesi, giornalisti, attivisti politici, attraverso l'attivazione del paragrafo 215 che consentiva agli inquirenti di raccogliere qualsiasi elemento che fosse *"pertinente a un'indagine di sicurezza nazionale"*. Un emendamento dei Repubblicani di Trump, infatti, estende ora i poteri dell'Fbi su tutti i dati di navigazione on line, senza bisogno di autorizzazione o mandato. Gli investigatori potranno raccogliere tutta la cronologia dei siti, delle chat, dei messaggi e delle chiamate delle persone, chiedendo i dati direttamente dalle grosse società Big Tech. L'hanno sempre

fatto, ma ora l'attività di spionaggio segreto sarà legale, permesso dalla legge e alla luce del sole. Se ci aggiungiamo che, con il pretesto della lotta alla pedofilia, il governo americano sta pensando anche di votare un pacchetto di nuove norme che addirittura vieterebbe l'uso della crittografia, abbiamo detto tutto (https://ilmanifesto.it/in-piena-pandemia-gli-usa-legalizzano-il-permesso-di-spiare-internet-senza-limiti/).

RUSSIA - a metà marzo, il primo ministro Mikhail Mishustin ha ordinato al ministero delle comunicazioni della Russia di sviluppare un sistema basato su GPS in grado di rintracciare le persone che sono venute in contatto con pazienti positivi al coronavirus. Secondo il sito web del governo federale, il sistema dovrebbe analizzare i dati di geolocalizzazione di singoli individui da società di telecomunicazioni. Questi dati saranno inoltre forniti alle task force a livello regionale che si occupano della diffusione del virus (https://meduza.io/en/news/2020/03/23/russian-officials-will-track-coronavirus-patients-geolocation-data-to-design-a-national-warning-system). La Russia intende anche introdurre un'app di geolocalizzazione per i pazienti con diagnosi di COVID-19 che vivono a Mosca, progettata per garantire che non escano di casa.
Le app in uso in Russia sono due: l'app "**Social Monitoring**" delle società Infogodor e Gaskar e "**Contact Tracer**" di SoftTree.

ISRAELE - Alcuni paesi hanno utilizzato il tracciamento della posizione basato sulla rete internet anziché le app, eliminando sia la necessità di scaricare un'app sia la possibilità di evitare il tracciamento. Questo, per esempio, è quanto ha fatto il governo di Israele. Si parla di un software per analizzare dati raccolti dai cellulari e localizzare probabili vettori di coronavirus. Il software è prodotto da **NSO**, società nota per vendere spyware, software spia o trojan ai governi. Il sistema assegnerebbe un punteggio da 1 a 10 in relazione alla probabilità che una persona sia vettore del virus, e tale punteggio verrebbe aggiornato in tempo reale in base agli spostamenti, in aree o locali a rischio. A controllarne l'operato è il ministro della Difesa israeliano (sì il ministro della Difesa, non della Salute). Una bella società NSO: giornalisti e attivisti politici da qualche anno denunciano attacchi informatici da parte sua ma anche contro residenti ed aziende sul suolo americano, e risulta che perfino Whatsapp gli abbia fatto causa accusandola di aver abusato del proprio servizio di chat per veicolare spyware contro alcuni target. In dodici paesi del mondo sono già state introdotte app del gruppo di spyware NSO Group. A metà marzo 2020, è stato infatti annunciato che 12 paesi, *"a scopo di test"*, stavano utilizzando un "tracker corona" del produttore israeliano, venduto ai ministeri della salute.
Ma in Israele, per contenere il contagio, è stato attivato pure lo stato straordinario di guerra. Ricordiamo che Israele è già da oltre 45 anni in guerra contro la popolazione palestinese nella striscia di Gaza, ma ora lo stato di guerra è stato esteso all'interno dei suoi confini e contro gli stessi israeliani. Il primo ministro Benjamin Netanyahu ha fatto sapere di aver aumentato *"la capacità di localizzare e mettere in quarantena coloro che sono stati infettati"* attraverso la tecnologia digitale. *"Informeremo queste persone che devono andare in quarantena per 14 giorni. Si prevede che saranno numeri grandi, anche molto grandi. Entrare in quarantena non sarà una raccomandazione ma un requisito e lo applicheremo senza compromessi"*. La quarantena è imposta utilizzando la tecnologia cellulare di geolocalizzazione con GPS attraverso la **App Waze** di fabbricazione israeliana. Il meccanismo dell'app è coperto da segreto
Israele ha intensificato il monitoraggio informatico e le tecnologie militari già presenti, bypassando la necessaria approvazione da parte del parlamento. Il monitoraggio avviene direttamente da parte del servizio segreto di sicurezza Shin Bet mentre la polizia pedina le persone che circolano per strada sulla base di campioni randomizzati (https://www.agendadigitale.eu/sicurezza/privacy/coronavirus-i-sistemi-per-tracciare-i-positivi-come-funzionano/). In sostanza il primo ministro Benjamin Netanyahu ha autorizzato l'agenzia di sicurezza interna del paese ad attingere a una vasta serie di dati dei cellulari, tra cui la

localizzazione, per rintracciare gli spostamenti delle persone contagiate e identificare altri che dovrebbero essere messi in quarantena poiché hanno avuto contatti con loro. Si tratta di misure tecnologiche antiterrorismo, reimpiegate dal governo israeliano perché considerate *"necessarie per salvare vite umane"*. Il governo ha anche autorizzato la pena detentiva fino a 6 mesi per chi viola gli ordini di isolamento, vietato le visite di parenti e avvocati nelle carceri e dato l'autorizzazione alla polizia di interrompere le riunioni e gli assembramenti di più di 10 persone, anche con l'uso della forza (https://www.money.it/Coronavirus-servizi-segreti-007-per-spiare-malati-tracciare-virus).
Il Ministero della Salute israeliano ha comunque lanciato il 22 marzo anche un'app di contact tracing chiamata **"HaMagen"** per cellulari iOS e Android che tiene traccia della posizione di una persona e fa un confronto con i movimenti di casi confermati di COVID-19, per verificare se i loro percorsi si sono sovrapposti nelle due settimane precedenti (https://www.gov.il/en/departments/news/hamagenapp).
"Da noi le app e i questionari online sono obbligatori quando si è positivi, ma stiamo pensando di renderli tali anche per tutti gli altri", ha spiegato Kira Radinsky, della **Diagnostic Robotics** e capo ricercatrice sul fronte big data di eBay. A Tel Aviv, grazie ai dati, l'azienda elabora mappe in tempo reale del contagio e ha messo a punto una serie di questionari sanitari.

GIAPPONE – L'app del sol levante "**COVID-19 Contact App**" (anche se in Giappone si riferisce all'app come **COCOA**, che sta per COVID-19 Contact-Confirming Application) il 22 giugno è stata fermata dalle autorità giapponesi, dopo soli pochi giorni dal lancio, perché produceva numeri di codice fantasma e "dava i numeri" per una serie di errori e bug tecnici. Era stata scaricata 3,71 milioni di volte fino ad allora. Il ministro della sanità ha detto di voler risolvere gli errori del sistema (http://www.askanews.it/esteri/2020/06/23/covid-19-app-tracciamento-giappone-fermata-per-numeri-fantasma-pn_20200623_00089/). Il funzionamento della app messa in campo in Giappone da venerdì è più o meno simile a quello dell'app "Immuni" in funzione in Italia, si basa sulla piattaforma di Apple e Google solo che la tecnologia è stata sviluppata da ingegneri **Microsoft** assieme a **Nikkei**: nel momento in cui un individuo che l'ha installata entra in contatto per un tempo superiore ai 15 minuti a una distanza di un metro o meno con un "positivo", viene avvertito. La comunicazione tra gli smartphone degli utenti avviene via Bluetooth. I dati restano sul dispositivo per 14 giorni prima di essere automaticamente invalidati. Se un utente viene testato positivo e segnala alla app la sua situazione inserendo un numero di codice, gli altri utenti che hanno l'app installata e sono nelle vicinanze ricevono un allarme (https://www.theverge.com/2020/6/19/21296603/japan-covid-19-contact-tracking-app-cocoa-released).

NUOVA ZELANDA - Il Ministero della Salute ha lanciato il **NZ COVID Tracer** il 20 maggio (https://en.wikipedia.org/wiki/NZ_COVID_Tracer). L'app è disponibile su App Store e Google Play. Oltre ad usare il Bluetooth, consente di scansionare i codici QR presso aziende, edifici pubblici e altre organizzazioni per rintracciare dove sono state le persone ai fini della traccia dei contratti e delle aree infette. Si basa sul modello ***BlueTrace*** di Singapore.
In più, **Vodafone New Zealand**, da marzo, ha introdotto nei suoi uffici un'applicazione telefonica per tenere traccia dello stato di salute e dei contatti dei suoi dipendenti, monitorando le aree in cui il dipendente trascorre il tempo e le persone con cui viene in contatto. L'app usa anche i codici QR.
"Dalla fine di marzo, la nostra app per lo staff obbligatoria pone ai dipendenti Vodafone quattro domande su salute e sicurezza ogni mattina nei giorni feriali, in modo da poter dare seguito a

qualsiasi bandiera rossa sullo stato di salute che si presenti", ha affermato il responsabile neozelandese dell'azienda. In base alle linee guida per la "Fase2", anche i punti vendita Vodafone in tutto il paese hanno aperto con misure di sicurezza e tracciabilità dei contatti. Un sistema di "accodamento virtuale" invita i clienti ad inserire i propri dati tramite un codice QR all'esterno del negozio, con notifiche inviate al cliente quando è il suo turno di entrare. I dati raccolti e archiviati da Vodafone vengono condivisi con il Ministero della salute (https://www.scoop.co.nz/stories/BU2005/S00282/vodafone-prepares-for-level-two.htm).

INDIA - L'app "**Aarogya Setu"** (https://www.aarogyasetu.gov.in e https://en.wikipedia.org/wiki/Aarogya_Setu) sviluppata dal National Informatics Center che appartiene al Ministero dell'elettronica e della tecnologia dell'informazione e dal programma Niti Aayog, è l'app del governo indiano disponibile su Google Play Store e Apple App Store per il download. L'app dell'India, lanciata a fine marzo 2020, è diventata l'applicazione in più rapida crescita al mondo battendo PokemonGo con 50 milioni di utenti nei primi 13 giorni della sua uscita. All'inizio di maggio, l'app era già stata installata oltre 90 milioni di volte.
L'app utilizza Bluetooth LE e il sistema di "global position" per determinare la posizione e traccia i contatti negli ultimi 14 giorni. Il data-base è in un laboratorio del Consiglio indiano di ricerca medica.
Il governo indiano collabora inoltre con le grandi compagnie telefoniche Airtel, Jio e Vodafone per la tracciabilità dei contatti. Gli utenti di Vodafone, Airtel e Reliance Jio in tutto il paese ricevono chiamate vocali dal governo per verificare se presentano o meno sintomi correlati a COVID-19. Le persone che hanno scaricato l'app Aarogya Setu e gli utenti di telefonia mobile possono essere direttamente contattati dal governo (stiamo parlando di oltre 900 milioni di utenti). Esiste un IVRS (Interactive Voice Response System (IVRS) che interagisce con gli utenti e verifica se presentano sintomi o meno. Avvisa quindi le autorità locali se viene riscontrato che qualcuno sta mostrando i sintomi di COVID-19. Tutti gli utenti di smartphone che non hanno ancora scaricato l'applicazione Aarogya Setu riceveranno in più notifiche dai loro fornitori di servizi per scaricarla. Il team medico di Ayushhman Bharat sta contattando le persone che hanno condiviso il loro stato di salute o dichiarato i loro sintomi, utilizzando i dati forniti dall'app Aarogya Setu. Il governo sta inoltre pianificando di portare l'app sui telefoni Jio dato che vi sono attualmente oltre 150 milioni di utenti Jiophone nel paese. Dal 4 maggio l'uso dell'app è stato reso obbligatorio per tutti i dipendenti di aziende pubbliche e private, nonché per tutte le persone nelle zone di quarantena. Il ministero degli interni ha ordinato alle autorità locali di garantire una copertura del 100% attraverso Arogya Setu nelle zone rosse ed è stata recentemente resa obbligatoria anche per tutti i dipendenti del governo centrale, a cui viene imposto di andare in ufficio solo se il loro stato sull'app mostra un rischio basso. L'app Aarogya Setu è stata resa inoltre obbligatoria per i lavoratori migranti. Il governo ha affermato che i lavoratori devono *"essere incoraggiati a scaricare l'app attraverso la quale è possibile monitorare il loro stato di salute"* (https://www.msn.com/en-in/money/news/govt-teams-up-with-airtel-jio-and-vodafone-for-covid-19-contact-tracing/ar-BB13yEIh).
La app del governo indiano si è però anche dimostrata molto fragile dal punto di vista della sicurezza informatica. Un esperto di sicurezza informatica francese, Robert Baptiste, installando l'app sul suo telefono, ha dichiarato di aver trovato un modo per accedere ai dati che avrebbero dovuto essere protetti. Baptiste ha scoperto che modificando le coordinate della posizione di un utente, l'app potrebbe dirti chi è infetto ovunque in India. *"È in gioco la privacy di 90 milioni di indiani"*, ha scritto (https://www.financialexpress.com/industry/technology/aarogya-setu-govt-mulls-open-source-architecture-for-app/1951651/).

Altre app per il contact tracing in India sono “COVA Punjab” introdotta dal governo del Punjab; “COVID-19 Quarantine Monitor” del governo del Tamil Nadu; “Mahakavach” del governo dello stato del Maharashtra; “Quarantine Watch” del governo del Karnataka; “Trackcovid-19.org” e molte altre app su base regionale che invece forniscono servizi di auto-diagnosi e monitoraggio dei sintomi (diario clinico).

AUSTRALIA - “COVIDSafe” è un'app di tracciamento dei contatti annunciata dal governo australiano e dal Dipartimento della Salute e si basa sul protocollo ***BlueTrace*** sviluppato dal governo di Singapore. È stata rilasciata per la prima volta il 26 aprile 2020. All’app di tracciamento se ne accompagna un’altra, “**Coronavirus Australia”**, facente funzioni di diario clinico contenente informazioni sanitarie personali. Oltre un milione di australiani hanno scaricato l'app COVIDSafe nelle prime 24 ore da quando è stata lanciata, a fine aprile, dal primo ministro Scott Morrison.
Le due app australiane sono sostenute da organizzazioni di medici, infermieri, imprenditori e bancari e registra le connessioni Bluetooth tra cellulari. Sono collegate a un server gestito da **Amazon** (https://www.ansa.it/canale_saluteebenessere/notizie/sanita/2020/04/27/coronavirus-australia-un-successo-lancio-app-tracciamento_ad24e78a-fbdf-49ec-ad70-f54e8e4f0934.html). **Amazon Web Services (AWS)** ha ricevuto infatti il contratto di archiviazione dei dati per le app di tracciamento dei contatti COVID-19 in Australia. Il contratto fa parte di un accordo che AWS ha firmato con il governo australiano e che prevede che tutte le agenzie e dipartimenti federali, statali e territoriali, nonché le università pubbliche e le società controllate dal governo, facciano riferimento ai server di Amazon. L’app australiana identifica gli smartphone che si trovano entro due metri l'uno dall'altro per più di 30 minuti. I dati vengono quindi acquisiti, crittografati e archiviati localmente sul telefono dell'utente per 21 giorni, e sul server di Amazon (https://www.zdnet.com/article/canberra-has-confidence-in-aws-ability-to-securely-store-covid-19-tracing-app-data/). Se i telefoni rimangono in contatto per oltre 15 minuti, l'app registra dati quali data, ora, distanza e durata della connessione, nonché il codice di identificazione crittografato dell'altro utente. Queste informazioni sono memorizzate sullo smartphone e mantenute per 21 giorni. È facoltà dell’utente decidere se inviare o meno questi dati a un server centrale. Nel caso questo avvenisse, quando un utente che utilizza CovidSafe risulta positivo al coronavirus, le autorità sanitarie possono utilizzare i dati dell'app del paziente per informare rapidamente le persone con cui è stato in contatto. CovidSafe chiede di fornire nome (può essere anche uno pseudonimo), fascia di età, numero di telefono e codice postale (http://www.ictbusiness.it/cont/news/in-australia-l-app-per-il-tracciamento-dei-contatti-e-gia-realta/44328/1.html). L'Australia, come altri paesi che stanno cercando di sviluppare la propria tecnologia senza le API di Apple e Google, sta registrando varie anomalie, esaurendo per esempio le batterie dei dispositivi. Il governo australiano ha quindi dichiarato di aver discusso con Apple e Google per migliorare la sua app COVIDSafe.
Lo Stato dell’Australia Occidentale ha invece preso ispirazione da strumenti di controllo applicati solitamente a chi è condannato agli arresti domiciliari, come i braccialetti elettronici. Una nuova legge passata con la scusa dell’emergenza permette di obbligare una persona in quarantena a essere monitorata attraverso un dispositivo che deve indossare o installare in casa. Tentativi di rimuoverlo o interferire con le operazioni dell’apparecchio può portare a un anno di prigione e a una multa di alcune migliaia di euro (https://www.theregister.com/2020/04/01/west_australia_isolation). C’è di più: I funzionari possono, *“in ogni momento”*, entrare nel luogo dove è stato installato l’apparecchio, cioè in casa delle persone, per recuperarlo (vedi https://www.parliament.wa.gov.au/Parliament/Bills.nsf/5924018EEA598B994825853B001C0B08/$File/Bill179-1.pdf).

COREA DEL SUD - Il governo della Corea del Sud ha optato per blocchi localizzati, concentrandosi sul test di un gran numero di persone (circa 15.000 test al giorno, gratuitamente) oltre a incoraggiare il distanziamento sociale. L'app **"Corona 100m"** è stata rilasciata l'11 febbraio 2020. Incrocia i dati di geolocalizzazione con quelli forniti dal governo. Sulla base di questi ultimi, l'app avvisa l'utente quando si sta avvicinando a una posizione a meno di 100 metri dal sospetto contagiato, sia sul territorio nazionale che internazionale, o come per altre app che usano il sistema collaborativo è la stessa persona a segnalare qualcuno. La persona che utilizza l'app può vedere quanto siano vicini ai pazienti con coronavirus. L'app mostra il sesso, l'età approssimativa e un identificativo della persona infetta. È stata installata un milione di volte nei primi 10 giorni, portando al collasso il server a causa del numero elevato di download e portando **TinaThree** (**Tina3D**), lo sviluppatore insieme a **Bae Won-Seoka**, a dover implementare la potenza e la stabilizzazione dello stesso.
Dalla versione 3 (1 aprile) l'app consente il riconoscimento automatico del numero della carta d'identità. Il tracciamento è esteso al controllo del rispetto della quarantena. L'app di autodiagnosi è obbligatoria per tutte le persone che entrano in Corea del Sud. L'app registra lo stato di salute giornaliero per 14 giorni dopo l'arrivo in Corea del Sud e si viene contattati se non si effettua la segnalazione giornaliera. Esiste anche un sistema di "sicurezza auto-quarantena" che utilizza il GPS, controllata da dei supervisori, dato che è punibile lasciare la quarantena senza permesso. In questo caso è stato utilizzato un sistema non basato su app di contact tracing ma che raccoglie e combina tra loro informazioni da una varietà di fonti, come i dati di posizione dei dispositivi mobili, i dati sulle transazioni delle carte di credito digitali e i dati dalle videocamere di sicurezza, con notifiche che arrivano ai cittadini quando un nuovo caso viene scoperto nella loro area. Soluzioni messe in campo già a partire dall'epidemia Mers del 2015.
Oltre a utilizzare queste informazioni, il governo ha anche reso pubblicamente disponibili le informazioni sulla posizione dei cellulari, cosa consentita a causa di profonde modifiche alle leggi sulla privacy delle informazioni dopo lo scoppio del virus MERS in quel paese. *"Compiamo le nostre indagini come fossimo ufficiali di polizia"*, ha spiegato al *New York Times* Ki Mo-ran, epidemiologo che lavora per conto del governo di Seoul. *"E con il tempo abbiamo rivisto le nostre leggi per dare priorità alla sicurezza invece che alla privacy in caso di crisi sanitarie"*.
Queste informazioni sono rese disponibili al pubblico tramite una serie di app popolari e siti Web. Le autorità hanno attivato una serie di messaggi che descrivono dettagliatamente i movimenti di persone infettate da Covid-19, suscitando vergogna pubblica e "chiacchiericcio". Questo ha comportato non solo umiliazioni pubbliche, minacce e stigma sociale verso le persone indicate come positive e le scene di caccia all'"untore" ma ha anche finito per alimentare in alcuni casi il chiacchiericcio sulle relazioni extraconiugali. Perché i dati di ogni paziente, con i relativi spostamenti negli ultimi 14 giorni – tracciati da cellulari, carte di credito, circuiti di videocamere ecc. – sono stati pubblicati su appositi siti, in modo da consentire di ricostruire la rete di contatti avuti, e quindi di possibili contagi (https://www.corriere.it/esteri/20_marzo_11/perche-corea-sud-ci-sono-relativamente-cosi-pochi-morti-coronavirus-31214682-63b3-11ea-9cf4-1c175ff3bb7c.shtml?refresh_ce-cp). Chi infrange il confinamento viene infatti messo nelle condizioni di vergogna davanti alle proprie famiglie e ai datori di lavoro molto severi sull'onorabilità dei propri dipendenti. Non vengono diffusi nomi o altro, ma brevi messaggi di testo dove viene descritto una scappatella o un comportamento anomalo in dettagli così minuziosi che le persone si riconoscono, o vedendosi nella stessa situazione per la paura ddi essere scoperti si autolimitano sentendosi "osservati". Il tracciamento ha così generato una gigantesca telenovela che sta appassionando a tal punto una parte

del popolo coreano che non può più fare a meno di questi messaggi sul comportamento dei loro concittadini.
Ma nel paese, oltre a Corona100m" vi sono molte altre app messe a disposizione che lavorano con Google Maps ma anche interagendo con la stessa "Corona 100m", come "Corona Map" e "Shincheonji Location Notification", che risultano le più scaricate da GooglePay. Quindi non solo app ufficiali di Governo ma anche rilasciate direttamente da società private (https://www.corriere.it/economia/consumi/20_marzo_18/coronavirus-compagnie-telefoniche-pronte-tracciare-catena-contagi-5dc8df48-68ee-11ea-913c-55c2df06d574.shtml?refresh_ce-cp).

BAHRAIN - "**BeAware Bahrain"** è l'app mobile ufficiale per Android e iOS, sviluppata da The Information & eGovernment Authority (**iGA**), in collaborazione con la Task force nazionale per la lotta contro il coronavirus. Utilizza i dati di localizzazione per avvisare le persone nel caso in cui si avvicinino a un caso positivo o in un luogo visitato dallo stesso, nonché per tenere traccia del movimento dei casi di quarantena per una durata di 14 giorni. Mohammed Ali Al Qaed, amministratore delegato di iGA, ha dichiarato: *"L'applicazione utilizza un braccialetto di localizzazione GPS a prova di manomissione per condividere informazioni di tracciamento in tempo reale con gli operatori sanitari. Gli operatori sanitari vengono informati quando i casi di quarantena escono dalla loro area prestabilita di 15 metri"*.

IRAQ - Gli ufficiali iraniani hanno rilasciato un'app per monitorare il contagio da coronavirus che prometteva agli utenti di sapere se era probabile che avessero contratto il virus, ma ha cominciato invece a tracciare i dettagli della geolocalizzazione in tempo reale degli utenti.

CINA - La risposta della Cina è stato un rigoroso distanziamento corporeo, blocchi in tutta la città di Wuhan e delle aree circostanti, un ampio monitoraggio pubblico dei cittadini attraverso app già diffuse tra la popolazione, nonché vari metodi di punizione e premi per incoraggiare l'adesione a tali misure.
Il governo cinese, in collaborazione con Alipay, ha rilasciato un mini-programma di close contact detector il 9 febbraio, chiamato **Alipay Health Code**, che avverte se si ha avuto contatti con una persona potenzialmente infetta. Il mini programma funziona con app estremamente diffuse in Cina come **Alipay**, **WeChat** e **QQ**. Il programma assegna automaticamente alle persone uno dei tre codici colore, che può essere aggiornato tramite un codice QR ed è valido solo per un breve periodo, in base alla loro cronologia di viaggio, cioè il tempo trascorso nei focolai dell'epidemia e l'esposizione a potenziali portatori del virus. Questo per determinare se devono mettersi in quarantena: verde – nessun giorno, giallo - 7 giorni, rosso - 14 giorni di isolamento. Le persone possono controllare i colori degli altri residenti quando vengono immessi i loro numeri ID. Le informazioni vengono direttamente integrate nelle App di uso comune ad esempio per il web mapping Gaode Maps (il nostro Google Maps). I dati sono aggiornati costantemente tramite REST API anche con dati ufficiali forniti dal governo. All'inizio di marzo, oltre 200 città cinesi hanno utilizzato questo "servizio". Lo status di coronavirus-free deve essere mostrato ai controlli all'ingresso e all'uscita di stazioni della metropolitana, negozi e uffici. Per accedere a negozi e uffici si accede sempre indossando la mascherina chirurgica, viene effettuato il controllo della temperatura all'ingresso e si può fare su Alipay e WeChat una sorta di autodichiarazione che non si è infetti. Si ottiene in questo modo un qr-code che viene scannerizzato all'ingresso di locali pubblici e ti consente di entrare. Nella pratica di tutti i giorni, in alcune città, è diventato quasi impossibile andare in giro senza mostrare sullo smartphine il codice Alipay alla polizia, una sorta di

autocertificazione digitale che alcuni controllori sociali avrebbero voluto introdurre anche in Italia.
C'è poi la questione della censura. In Cina **YY**, una piattaforma di live streaming, ha iniziato a censurare parole chiave connesse al coronavirus fin dal 31 dicembre; WeChat, l'app di comunicazione/social multifunzione fondamentale in Cina (l'equivalente di WhatsApp) ha censurato ampiamente contenuti legati al coronavirus. Tra le cose più censurate, ovviamente: le critiche al governo e i riferimenti al dottore Li Wenliang (che per primo avvisò dell'epidemia).
Il virus è divenuto catalizzatore per un'ulteriore espansione del regime di sorveglianza, che si perfeziona ad ogni evento particolare alzando ancor più l'asticella: a partire dalle Olimpiadi del 2008 tenutesi a Pechino o all'Expo di Shanghai nel 2010. La Cina, insomma, ha sfruttato e al tempo stesso perfezionato il suo già collaudato sistema di sorveglianza di massa basato su big data, app e intelligenza artificiale.
Tanto per capirci, per esempio, In Cina esiste un progetto pilota di un'applicazione che funziona attraverso la piattaforma WeChat, per identificare la presenza di debitori in un raggio di 500m dall'utente-creditore e per segnalare a quest'ultimo i comportamenti sospetti dei suoi debitori, come acquisti impropri, sino ad impedire che il debitore possa spendere in viaggi od oggetti il suo denaro: è la sperimentazione del cosiddetto "punteggio sociale", un credito che va ad assottigliarsi fino a ridurre la possibilità di fare acquisti.
Inoltre ormai larga parte della popolazione cinese è abituata ad usare le app per ogni aspetto della loro vita. WeChat in Cina è utilizzata per fare qualunque cosa offrendo innumerevoli funzioni adatte all'uso quotidiano: telefonare, inviare messaggi (vocali), pubblicare foto, noleggiare una bicicletta, prenotare viaggi, acquistare un biglietto del cinema, prenotare un tavolo nel tuo ristorante preferito, cercare le ultime offerte, organizzare un appuntamento dal medico e molto altro ancora, il tutto in un'unica app. AliPay è invece il sistema di pagamenti di **Alibaba**: una piattaforma di pagamento online usato dalla popolazione ormai più del denaro contante.
Ogni App viene incorporata all'interno di WeChat in cui è possibile aggiungere e incorporare funzioni di fornitori di servizi esterni. La strategia del governo è stata quindi quella di non creare un'ulteriore App, con il rischio che non venisse scaricata, ma di usare App ampiamente utilizzate dalla popolazione come WeChat (sistema di messaggistica e di pagamento con Wechat Pay) o Alipay (sistema di pagamento) e 高德地图 (Gaode ditu o gaode maps) nelle attività di vita quotidiana: come muoversi, pagare/comprare, chattare. Tutti i dati così ottenuti, da quelli sugli spostamenti a quelli sugli acquisti eseguiti con le app di pagamento, confluiscono in data base governativi. I dati vengono implementati e sovrapporti a quelli ottenuti con la videosorveglianza, il riconoscimento facciale ed altri apparati della smart city.
WeChat e Weibo hanno anche "hotline" che permette a chiunque di segnalare altre persone che potrebbero essere malati o che hanno commesso eventuali infrazioni. Le città offrono ricompense alle persone per queste informazioni.
Nell'app WeChat c'è una sezione dove si può cliccare per inserire il numero del treno o del bus, analogamente su Alipay, per verificare se si è viaggiato insieme a casi confermati di covid-19.
Oltretutto, i pagamenti in Cina sono quasi al 90% elettronici (ad aprile la Cina ha lanciato la moneta interamente digitale di Stato, "De/Ep", con test pilota in quattro città: Shenzhen, Suzhou, Xiongan e Chengdu, attraverso le banche di Stato e una apposita app; vedi https://www.ansa.it/sito/notizie/tecnologia/tlc/2020/04/20/cina-testa-in-4-citta-app-su-moneta-digitale-di-stato_3200f82b-2f51-43b2-9e1c-2328586fa0c8.html) e quando si prende il pullman, la metro o il taxi spesso si paga facendo "tap" con una tessera magnetica o scannerizzando un QR-code con Alipay o WeChat pay che hanno dunque tutti i dati personali della ID card. Il governo può sapere in tempo reale con chi hai viaggiato, quando e dove. Se invece si paga in contanti si deve

compilare un foglio che ha l'autista nel quale si registra nome, cognome e numero ID della carta d'identità.
In farmacia se si comprano antibiotici o altri farmaci per sindromi influenzali si viene registrati automaticamente, e l'applicazione può accendere un allerta mandata alle autorità per cui si potrebbe venire chiamati o visitati a casa per verifiche. Il controllo è così invasivo che i datori di lavoro potrebbero richiedere l'esibizione della cronologia degli spostamenti per verificare un eventuale profilo di rischio, ottenibile inviando un Sms al proprio operatore telefonico (ad esempio 10086 per China Mobile) e ricevendone uno con la lista delle città e dei paesi nelle quali si è stati durante gli ultimi 14 giorni. Per uscire di casa esiste una tessera che serve per uscire ogni 2/3 giorni per andare al supermercato, ma una una sola persona per famiglia, e sopra la scheda, diversa per ogni comunità, ogni volta viene apposto un timbro sulla data nella quale si è stati al supermercato. Non solo: per entrare nel proprio appartamento o sul posto di lavoro è necessario scansionare un codice QR, scrivere il proprio nome e numero ID, temperatura e cronologia di viaggio recente.
Per la "Fase2", le aziende cinesi stanno nel frattempo implementando la tecnologia di riconoscimento facciale in grado di rilevare temperature elevate in una folla o verificare se i cittadini non indossano la mascherina.
I problemi e le criticità delle tecnologie di sorveglianza ci sono stati anche in Cina. É accaduto, per esempio, che chi transitava in auto senza fermarti attraverso Hubei, una zona rossa, con Weibo attivo (l'equivalente cinese di Instagram) ha visto il suo codice-colore diventare da verde a giallo e quindi messo in quarantena. Oppure, in un paese dove la domotica (la digitalizzazione delle cose all'interno dell'abitazione) negli appartamenti e nei megacondomini è ormai molto diffusa, è successo che fosse efficiente al punto da non consentire di aprire la porta di casa se il codice sul telefonino diventava improvvisamente giallo o rosso.
il governo cinese è disposto a spendere denaro pubblico illimitatamente per realizzare l'infrastruttura di sorveglianza ad alta tecnologia, pur consentendo a società tecnologiche cinesi come Alibaba, Baidu e Huawei di intascare i profitti dalle applicazioni commerciali.
Non è nemmeno un segreto che in Cina, dove la galassia Facebook è bloccata dal partito, **Tencent** (l'impresa che ha sviluppato WeChat, che ha circa 980 milioni di utenti mensili) collabora con il governo cinese e condivide le informazioni personali dei propri utenti ed è anche la società che ha fornito i dati per alimentare il sistema di apprendimento automatico del riconoscimento facciale.
Inoltre vi è stata l'imposizione ai cittadini di muoversi con il cellulare acceso.
"Quando usciamo o restiamo in un hotel, possiamo sentire un paio di occhi che ci guardano in qualsiasi momento. Siamo completamente esposti al monitoraggio del governo" è stato il commento di Maya Wang di China for Human Rights Watch.

HONG KONG - Ad Hong Kong, a tutti gli individui che entrano nel paese viene consegnato un braccialetto "Stay Home Safe" che ne monitora i movimenti per la durata della loro presenza in loco. Braccialetti per il tracciamento anche a chi deve stare in quarantena.

COLOMBIA - "**CoronApp"** è l'app mobile per Android e iOS - e disponibile per Huawei AppGallery - sviluppata dal governo colombiano. L'app, scaricata oltre 1,2 milioni di utenti, è un'applicazione gratuita che rileva le aree colpite e le persone vicine con diagnosi positiva per COVID-19. Attiva il monitoraggio in tempo reale dei dati raccolti presso il Centro operativo di emergenza dell'Instituto Nacional de Salud (National Health Institute, INS). Incorpora tecnologie come quelle sviluppate dai governi di Singapore e della Corea del Sud, nonché da Apple. La Fundación Karisma ha evidenziato alcune vulnerabilità di CoronApp, comuni a molte app simili.

Come vantaggio per chi scarica l'app, il governo colombiano finanzia 1 gigabyte al mese e 100 minuti gratis per gli utenti delle linee prepagate che lo installano.

GHANA - Il governo ha lanciato **"GH Covid-19 Tracker App"**, un'app per Android e IOS dotata di tecnologia di geolocalizzazione per fornire informazioni dettagliate sulle persone che si sono trovate nello stesso evento, posizione, paese o altre posizioni definite al fine di fornire informazioni accurate alle autorità. L'app è stata sviluppata dal Ministero della Comunicazione e della Tecnologia e dal Ministero della Salute.

MALAYSIA - il governo ha lanciato "**MyTrace"** il 3 maggio 2020, una delle tre app di tracciamento rilasciate insieme a "**Gerak Malaysia"** e "**MySejahtera"**. "Gerak Malaysia" della Royal Malaysia Police in collaborazione col ministero della salute, è un'app di tracciamento che consente alla polizia di tracciare e analizzare i movimenti degli utenti e registrarsi per ottenere l'autorizzazione a consentire l'attraversamento delle frontiere statali. MySejahtera è un'app sviluppata dal Consiglio di sicurezza nazionale e dal Ministero della salute per recuperare informazioni riguardanti le informazioni aggiornate e le statistiche della pandemia. MyTrace è invece un'app di tracciamento che utilizza il Bluetooth per rilevare per quanto tempo uno smartphone dell'utente è in prossimità di altri utenti di smartphone con un'app simile installata.

ARABIA SAUDITA - "**Corona Map Arabia Saudita"** è l'app mobile ufficiale per Web, Android e iOS, sviluppata dal National Health Information Center (NHIC).

SINGAPORE – L'esperienza delle precedenti epidemie di Aviaria e di H1N1, che hanno colpito Singapore, città-stato ed isola di 23 milioni di abitanti, ha dato luogo da tempo alla creazione del National Centre for Infectious Diseases NCID: un'istituzione che utilizza le più avanzate tecnologie per il controllo dei contagi. I contatti vengono rintracciati dalle forze di polizia di Singapore, che usano le telecamere di videosorveglianza, interviste con i pazienti per redigere elenchi di persone che potrebbero essere state esposte ed anche l'app di tracciamento. Nel paese preso a modello da molti stati europei, dal 20 marzo 2020 è infatti in uso un'app chiamata **TraceTogether** (https://www.tracetogether.gov.sg/), sviluppata da un'agenzia governativa con protocollo di tracciamento dei contatti digitali ***BlueTrace***, e con un'implementazione di riferimento open source, *OpenTrace* (https://en.wikipedia.org/wiki/TraceTogether).
È stata la prima applicazione Bluetooth Low Energy (BLE) nazionale al mondo per il rilevamento dei contatti. Disponibile per Android e iOS, TraceTogether, sviluppata dal Government Tecnhology Agency of Singapore, rileva automaticamente gli smartphone che usano questa app. Si deve abilitare le notifiche, mantenere il Bluetooth attivo e lasciare "TraceTogether" in esecuzione. I dati (ID-Identificativi) vengono memorizzati nel telefono per 21 giorni e quindi eliminati (però si è saputo che ogni installazione di app è collegata al numero di telefono dell'utente e quindi identificabile). Ma il sistema cifra i dati dell'utente anche su server governativi e gli assegna un ID temporaneo, che viene trasmesso da un dispositivo all'altro quando questi si trovano a "portata" del segnale Bluetooth. Se si viene identificati come una persona che ha avuto un contatto con un caso positivo al Covid-19 confermato tramite l'app, si verrà contattati direttamente dal ministero della Salute. Chiunque sia tenuto alla quarantena, attraverso questa app può essere chiamato più volte al giorno dalle autorità e fare clic su un collegamento online che condivide la posizione del proprio telefono. Coloro che non restano a casa possono aspettarsi una multa fino a 10mila dollari o fino a sei mesi di reclusione e la perdita della cittadinanza. Le misure dopo il tracciamento dei positivi

(veri o falsi) prevedono l'isolamento totale per tutti i soggetti "a contatto" per come risulta dalla app. Spesso il paese è stato indicato come esempio da seguire per la capacità di gestire l'emergenza da coronavirus, indicando proprio nell'uso dell'app di tracciamento con Bluetooth il mezzo con il quale ha raggiunto l'obiettivo di contenere il contagio. Eppure, a Singapore, solo una persona su sei aveva scaricato l'app TraceTogether ad aprile 2020. L'app è stata anche sottoutilizzata a causa del fatto che richiedeva agli utenti di tenerla sempre aperta. Oltre a ciò, l'introduzione dell'app di contact tracing non è comunque riuscita a far risalire a molti dei contagiati, per stessa ammissione del primo ministro Lee Hsien Loong, che anzi parlando di una crescita di nuovi casi nella città Stato ha poi dovuto annunciare il piano B, ovvero...il lockdown per un mese intero, iniziato l'8 aprile (https://www.key4biz.it/contact-tracing-lockdown-anche-a-singapore-dove-si-usa-lapp-miracolosa/298769/). Il primo ministro ha dichiarato testualmente che *"malgrado il nostro buon contact tracing, per quasi metà di questi casi non sappiamo da dove o da chi le persone abbiano contratto il virus"*. Si è così scoperto che l'applicazione "miracolosa", molto simile a quella introdotta in Italia, non è servita a frenare il virus. Per altro l' "esempio" del tracciamento contatti di Singapore non è nemmeno a "prova di privacy": come segnalato in un post di un programmatore del luogo (https://splira.com/2020-03-28/) nella app c'è una "libreria" che salva i dati, inclusi quelli per individuare gli utenti, in una piattaforma governativa che salva il numero del telefono e il codice Imei che identifica in modo univoco un dispositivo mobile cellulare. Quindi anche se il *contact tracing* è ufficialmente anonimizzato, poi la libreria di tracking che sta nell'app ti deanonimizza all'istante.
L'esempio tanto celebrato è quindi naufragato nel fallimento: l'app è stata scaricata da meno del 20% della popolazione e ha fatto dichiarare al direttore dell'Agenzia dei servizi digitali che il suo utilizzo debba ritenersi pericoloso per i troppi falsi positivi e negativi registrati, cosa che discende dalla natura stessa della tecnologia Bluetooth che, a seconda del modello di smartphone posseduto, può captare soggetti a distanza diversa (anche a distanza superiore ai cento metri) con i quali non necessariamente si è entrati in contatto.
Per informazione, per sorvegliare le persone a Sigapore oltre all'app di tracciamento (e a varie decine di droni) vi è anche **Robot Spot**, cane robot a quattro zampe realizzato da **Boston Dynamics**, che si sposta su vari tipi di terreno ed equipaggiato con telecamere che consentono di fare una stima delle persone presenti in un parco e invita a sciogliere assembramenti attraverso un messaggio preregistrato (https://www.money.it/Coronavirus-scenario-distopico-a-Singapore-cane-robot).

Altri stati che hanno introdotto proprie app di contact tracing sono:
- **Angola** con l'app "Covid-19 AO" con diario clinico, sviluppata da Ravelino De Castro;
- **South Africa** in uso l'app "Cov-ID" dell'Università di Cape Town e della società The Delta Studio;
- **Sri Lanka** con "COVID Shield" del Commonwealth Centre for Digital Health, disponibile solo per Android;
- **Vietnam** con l'app clinica "NCOVI" del ministero della salute;

Per una panoramica vedi anche https://en.wikipedia.org/wiki/COVID-19_apps

***

CRITICITÀ E (in)SICUREZZA

Il cosiddetto tema della privacy è stato più volte messo al centro del dibattito attorno alle misure che i governi di mezzo mondo hanno introdotto o si stanno apprestando ad introdurre per la cosiddetta *fase 2* della pandemia da coronavirus, a cominciare dalle app per il contact tracing.
C'è chi, come i politici, ha affermato che non si potesse introdurre l'utilizzo di un'app di tracciamento semplicemente per decreto o attraverso una semplice ordinanza del commissario per l'emergenza Covid, Domenico Arcuri, proponendo la conversione in legge in parlamento (https://www.repubblica.it/politica/2020/04/20/news/fase_2_sull_app_immuni_pd_e_forza_italia_in_sintonia_serve_una_legge_va_votata_in_parlamento_-254515000/).
Persino Salvini si è stracciato le vesti ed ipocritamente ha parlato di "libertà non in vendita", proprio lui che vorrebbe toglierla a tutti quanti se potesse.
È entrato in campo perfino il Copasir (il Comitato parlamentare per la sicurezza della Repubblica, che si occupa anche del coordinamento dei servizi segreti) per approfondire alcuni aspetti ritenendo quella dell'app è una *"questione di sicurezza nazionale"*.
Altri si sono appellati al Garante dell'Authority per la Privacy, Antonello Soro, per dare almeno una parvenza di costituzionalità al tracciamento dei dati personali. Per intenderci, è quel Antonello Soro che in sostanza ha dato il suo avvallo all'intera operazione di Immuni, seppur da posizione defilata, giocando l'antico ruolo del piede in due scarpe, da un lato raccomandando la salvaguardia dell'anonimato e della volontarietà dell'applicazione, dall'altro sostenendo l'impiego di massa per l'"interesse collettivo" chiedendo la collaborazione dei cittadini e rassicurandoli sui *"pochi rischi per la privacy"*. Il garante che in un'intervista a Radio Radicale affermava che "s*ono possibili tutte le deroghe, ma ci deve essere una base giuridica che consenta attraverso i poteri alla Protezione civile di tenere questa fase emergenziale dentro un contesto di garanzie accettabile*".
Ma accettabile da chi, per chi? Non ci rincuora affatto sapere che l'uso di questa tecnologia di sorveglianza sia normato da una legge, anzi. Una volta introdotta la legge, l'uso delle app di tracciamento diverrà un precedente legale, una cosa normale e normalizzata, con buona pace dei giuristi democratici e dei politici preoccupati per la privacy. Anzi, sentire parlare questi ipocriti di "diritto fondamentale alla privacy" e proporre i loro inutili palliativi non può che disgustare.
Ma, al di là delle preoccupazioni morali di costituzionalisti, tecnici, esperti, politici e giuristi democratici (vedi anche https://www.ansa.it/sito/notizie/tecnologia/software_app/2020/04/21/esperti-dati-app-siano-su-smartphone_867a4ce8-511c-412f-af91-8e1076a6295e.html), quando si parla di applicazioni per smartphone, il problema non sono solo i dati che la persona immette volontariamente, ma anche la richiesta iniziale di una lunga serie di permessi di accesso allo smartphone quando si scarica l'app. Le autorizzazioni richieste per funzionare sono davvero tante e una volta installata un'app, a seconda del caso, questa può: accedere alla cronologia del dispositivo e conoscere quali altre app sono installate; accedere ai dati personali del titolare dello smartphone e aggiungere o rimuovere account; accedere a tutte le foto, gli elementi multimediali e i file sul dispositivo; registrare audio; conoscere le informazioni relative alla rete Wi-Fi; registrare video e fare foto; leggere la lista dei contatti; leggere, modificare e cancellare il contenuto di una memoria USB collegata al dispositivo; leggere le impostazioni Home e le scorciatoie; ricevere dati da Internet; impedire al dispositivo di andare in risparmio energetico; espandere/comprimere la barra di stato; disinstallare le scorciatoie; controllare il flash; eseguire codice all'avvio del dispositivo; controllare la vibrazione del dispositivo; installare scorciatoie; visualizzare le connessioni di rete; riordinare le app in esecuzione; creare account e impostare password; attivare e disattivare la sincronizzazione; avere accesso completo alla rete; cambiare le impostazioni audio; utilizzare gli account sul dispositivo. Insomma, un'app può davvero prendere il controllo di parte del meccanismo e delle informazioni del proprio cellulare. Per esempio, potendo accedere a microfono e videocamera un'app può essere usata a distanza nel caso si voglia spiare l'utente e, ovviamente, inviare i file registrati allo spione di turno (ad aprile di quest'anno si è avuta notizia della denuncia

di due persone a Napoli che, rubato un cellulare, sono stati individuati dalla Polizia sfruttando un'app installata sul telefonino in grado di scattare foto e attivare la telecamera da remoto; vedi *https://napoli.fanpage.it/rubano-il-telefonino-la-proprietaria-li-fotografa-con-lapp-da-casa-presi/*). Le possibilità sono infinite.

Intanto partiamo da un fattore importante che ci permette di inquadrare bene il discorso: i dati "sufficentemente" anonimi non esistono. L'anonimizzazione dei dati personali o c'è o non c'è, e dovrebbe essere totale, per cui se un dato è davvero anonimo nessuno dovrebbe essere in grado di identificare una persona reale. Cosa che invece non succede con le app di tracciamento, ovviamente (e con la quasi totalità di strumenti tecnologici per cellulari). Queste lavoreranno su dati cosiddetti 'pseudonimizzati', suscettibili di subire un processo di reidentificazione in caso di rilevata positività da chi è autorizzato a prenderne visione.

Chiariamo ulteriormente il concetto. I dati anonimizzati sono quei dati che sono stati privati degli elementi identificativi. Non sono quindi ritenuti dati personali e non sono nemmeno soggetti alle norme a tutela dei dati personali. Ovviamente può accadere che i dati, una volta esaurito lo scopo del trattamento, possano essere conservati a fini statistici, storici o scientifici.

I dati pseudonimi sono invece quei dati personali nei quali gli elementi identificativi sono stati sostituiti da elementi diversi, quali stringhe di caratteri o numeri (codici), oppure sostituendo al nome un nickname, tali da rendere più difficoltosa ma non impossibile l'identificazione dell'interessato. Ovviamente da qualche parte esiste però un soggetto che detiene la chiave per decifrare i dati, cioè collegare l'elemento pseudonimo al dato personale.

Sull'anonimato, se si vuol approfondire, vale la pena di leggere lo scritto di Edward Snowden, *Mémoires vives*, Parigi, Seuil, 2019. In questo testo, Snowden insiste sull'impossibilità di cancellare definitivamente i dati registrati attraverso l'uso di strumenti tecnologici. Per quanto riguarda l'impossibilità di anonimizzare i dati in maniera totale e sicura, possiamo fare riferimento alle analisi di Luc Rocher nel suo articolo "Dati anonimi, fin troppo facili da identificare", pubblicato in francese il 17 settembre 2019 sul sito web www.theconversation.com

Secondo Snowden, ex tecnico della CIA che ha dato la stura al "datagate" che ha coinvolto i governi americano e britannico, permettere alle autorità di usare misure di sorveglianza individuali basate sulla tecnologia per contrastare il contagio del coronavirus potrebbe creare un precedente a totale danno delle libertà personali.

Sull'argomento contact tracing si registra già un deciso incremento di attacchi informatici. Ad inizio aprile, per esempio, attraverso una ricerca che ha interessato Iran, Colombia e Italia erano state individuate alcune app Android per il tracciamento del Covid-19 contraffatte ad arte per carpire dati e controllare da remoto i dispositivi su cui vengono installate (vedi la ricerca di Zerofox Alpha Team su https://www.zerofox.com/blog/covid-19-mobile-apps/). In Colombia questo ha provocato l'esposizione dei dati sanitari di circa 100.000 persone. In particolare, per l'Italia è stata riscontrata l'esistenza di una campagna mirata a diffondere un'app contraffatta a regola d'arte, ovvero una vera app per il contact tracing rilasciata in versione beta, ma poi riprogrammata e rimessa in circolo con finalità diverse. L'app clonata, in molti dei casi esaminati da questa ricerca, è risultata essere l'app "Sm_Covid19", sviluppata dall'azienda Soft Mining di Avellino e dall'Università di Salerno, ma con la peculiarità di avere un certificato di firma a nome "Raven" con sede a Baltimora. L'app clonata è stata rilasciata col package "*it.softmining.]projects.covid19.]savelifestyle.]apzcp*" (https://www.cybersecurity360.it/nuove-minacce/app-android-per-il-tracciamento-del-covid-19-allarme-malware-tutti-i-dettagli/).

In Italia, dopo il lancio di Immuni il 1 giugno 2020, una persona se risultata positiva al virus può caricare sul server gestito da Sogei i dati raccolti dalla sua app, comprese le informazioni sulla sua

salute e la lista con i codici numerici degli smartphone delle persone a cui è stato vicino. Questa tipologia di dati è altamente appetibile dai “cyber criminali” che lavorano per le aziende private nazionali ed internazionali e per i Governi di altri Paesi (anche quelli sulla carta “alleati”, in primis gli Stati Uniti). Un'operazione di intelligence straniera potrebbe per esempio bloccare un'intera città segnalando falsamente infezioni COVID-19 in ogni quartiere, attraverso l’hakeraggio delle app. Utilizzare server dislocati sul territorio italiano, di per sé è una garanzia? Ogni stoccaggio di informazioni sensibili ha una sua “fragilità” intrinseca, al di là del mero strumento tecnico, ed è il personale che deve gestire server e dati, che come dimostrato in altre occasioni può essere ricattato o addirittura comprato per ottenere delle informazioni così rilevanti sul piano economico e commerciale. C’è l’aspetto, niente affatto secondario, dei fini commerciali: ti dicono che i servizi che forniscono le App sono gratuiti, al pari dei social, ma il costo di entrambi sono i tuoi dati. É quello il denaro che paghi, che per loro diventa merce da vendere. Per pubblicizzare un prodotto, per fare un sondaggio, per sondare i tuoi gusti e le tue opinioni… e anche il tuo voto, come nel caso di Cambridge Analytica (https://www.wired.it/topic/cambridge-analytica/) che sfruttando i dati personali di oltre 50 milioni di utenti di Facebook ha potuto ottimizzare la portata della propaganda politica di diverse campagne elettorali, compresa quella per l'elezione di Donald Trump. Una gigantesca mole di informazioni sulle preferenze di miliardi di persone viene usata per ottenere una posizione di potere nel mercato della pubblicità online. Come è possibile essere così ingenui da credere che le informazioni archiviate dalle app di tracciamento non saranno anch’esse usate allo stesso modo?

Secondo il rapporto Clusit 2020, l’anno trascorso (il 2019), è stato un *annus horribilis* evidenziando un *trend* persistente di crescita degli attacchi informatici, della loro gravità e dei danni conseguenti. E gli attacchi informatici che utilizzano come vettore i cellulari e le mobile-app sono destinati a salire. La crescita più forte di attacchi malware la si registra tra l’altro verso i server gestiti dalle amministrazioni pubbliche statali, col settore sanitario tra i settori più colpiti e più fragili (https://www.key4biz.it/rapporto-clusit-2020-cresce-la-cyber-insicurezza-piu-malware-contro-pa-e-gaming/295521/).

È sufficiente ricordare cosa è accaduto con il furto delle informazioni personali dal sito Inps per chi ha richiesto il bonus da 600 euro per capire qual è il rischio. Nel caso di Immuni, le informazioni sanitarie di milioni di italiani saranno gestiti attraverso il server di Sogei, la piattaforma del ministero dell’Economia, che tra l’altro gestisce centinaia di altri dati personali forniti alle pubbliche amministrazioni da ogni singolo individuo. E ricordiamo che Sogei è nota per essere la responsabile delle cartelle pazze di Equitalia, dei tilt ciclici dei suoi server per le “rottamazioni delle cartelle”, oltre che di ben note clientele e corruttele.

Ma anche le società private non sono certo esenti dal rischio del furto dei dati e delle informazioni sensibili. **“Zoom”**, l'app per le videochiamate fondata da Eric S. Yuan, prima del coronavirus aveva 10 milioni di utenti al giorno nel mondo, ora più di 200 milioni, gareggiando con la più conosciuta Skype. Ad inizio aprile sono emersi molti problemi di sicurezza sui dati. Il 27 marzo Facebook, sfruttando una falla dell’app, ha carpito alcuni dati degli utenti, anche di chi non è iscritto al social e senza esprimerlo nell’informativa sulla privacy di Zoom. Facebook lo ha potuto fare sfruttando la possibilità di accedere a Zoom con il login di Facebook. È anche successo che dopo una videochiamata su Zoom uno degli interlocutori sia venuto in possesso dei dati del profilo LinkedIn degli altri partecipanti. Il tutto in totale segreto. Perché? L’app inviava automaticamente nomi ed indirizzi email dei partecipanti alla videoconferenza a un sistema per abbinarli ai loro profili LinkedIn. Questa funzione era disponibile per gli utenti di Zoom abbonati a LinkedIn Sales Navigator. Una volta che un utente Zoom aveva abilitato la funzione poteva accedere rapidamente e

segretamente ai dati del profilo LinkedIn – come posizioni, nomi dei datori di lavoro e titoli di lavoro, facendo clic sull'icona LinkedIn visibile sullo schermo durante le videocall su Zoom 8https://www.key4biz.it/zoom-tutte-le-falle-di-privacy-dellapp-da-200-milioni-di-utenti-al-giorno-nel-mondo-come-usarla-in-modo-piu-sicuro/298613/). Questa funzione, che consentiva una fuga di dati senza il consenso degli utenti, è stata disabilitata da Zoom. Ma quanti altri sistemi per carpire dati e informazioni, quante "falle" esistono in queste tecnologie che ancora non conosciamo? Di sicuro tante!

Un altro esempio è quello di **TikTok**, finita perfino sotto la lente d'ingrandimento dei servizi segreti italiani, dopo le indagini della National Security Agency americana, che ha portato al divieto per i soldati americani di usare l'app sviluppata dalla società cinese **ByteDance**. L'Aise, l'Agenzia per le informazioni e la sicurezza esterna, e il Dis, il Dipartimento delle informazioni per la sicurezza, dietro consiglio del Comitato parlamentare per la sicurezza della Repubblica (Copasir) hanno aperto un'istruttoria sull'uso dei dati degli utenti da parte di Tik Tok, per capire dove finiscono e come vengono usati i dati personali e i contenuti caricati sul social dai 6,4 milioni di utenti italiani. Verrebbe da dire che non uguale solerzia è stata usata nei confronti delle multinazionali statunitensi come Fecebook, Apple e Google, ma comunque il problema principale, di TikTok come di altre aziende cinesi che lavorano sul Web, è che sono tenute a rendere disponibili i dati raccolti alle autorità governative. I server di TikTok sono infatti in Cina e così i dati degli utenti italiani possono essere controllati dalle autorità cinesi senza limitazioni e il Governo potrebbe visionare file, documenti, fotografie, video, vocali, messaggi e farne ciò che vuole (https://tecnologia.libero.it/dopo-gli-usa-anche-servizi-segreti-italiani-puntano-il-dito-su-tiktok-33453).

É risaputo che già solo con i dati anonimi delle telecomunicazioni si possono ottenere molte informazioni: analisi di big data sul traffico, individuazione di assembramenti, messaggi a specifici utenti e *geofencing* (tracciare delle aree e, se vengono superate, far scattare un avvertimento). In più, con le app di tracciamento dei contatti è richiesto di portare addosso con sè il cellulare per tutto il giorno, indipendentemente da ciò che si sta facendo. A prescindere dalle preoccupazioni sull'esposizione al campo elettromagnetico del cellulare, c'è da dire che quest'ultimo, per sua natura intrinseca, già traccia e condivide innumerevoli altri dati. Uno studio del Washington Post del 2019, per esempio, ha scoperto circa 5.400 tracker di dati (principalmente basati su app) su un iPhone, inviati a terze parti. E incoraggiare le persone a portare sempre con sé il proprio smartphone, a farlo rimanere sempre attivo, vuol dire proprio sottoporsi al costante pericolo di fornire i propri dati a qualcun altro. Gli hardware e i software che rendono i nostri telefoni così indispensabili ci stanno già tracciando ventiquattrore al giorno ogni giorno. Per esempio, le app sul Coronavirus che usano la geolocalizzazione per capire se un individuo sta rispettando il distanziamento sociale o sta all'interno della zona di quarantena sono possibili solo perché i nostri telefoni sono pensati per fornire precisi dati di geolocalizzazione, che compagnie come Google raccolgono e immagazzinano da sempre. Se ti porti in giro il telefono con il GPS acceso, Google sa sempre dove ti trovi in qualunque momento. Ti basterà aprire la app Maps, e Google prenderà nota di dove ti trovavi quando l'hai aperta. Tutte le volte che fai una ricerca non vengono solo immagazzinati i contenuti della tua ricerca ma anche dove ti trovavi quando l'hai fatta. I ricercatori di Princeton hanno confermato che, addirittura, anche se hai impostato gli strumenti sulla privacy di Google sia su Android che sull'iPhone chiedendogli di non tracciare la tua posizione, Google lo fa lo stesso (https://apnews.com/828aefab64d4411bac257a07c1af0ecb/AP-Exclusive:-Google-tracks-your-movements,-like-it-or-not).

Oltre a ciò, la costellazione di comportamenti che facilitano la pronta volontà di farsi un selfie per il

riconoscimento facciale o di usare una app per tracciare e segnalare potenziali sintomi di malattia sono state sviluppate molto prima del Coronavirus. Usiamo FaceID per sbloccare i telefonini, postiamo selfie su Instagram e veniamo taggati su Facebook usando le capacità del riconoscimento facciale. Ci auto-monitoriamo con applicazioni che tracciano il ciclo o il sonno, che ci aiutano a meditare o a calcolare il nostro bioritmo. Governi e multinazionali fanno affidamento proprio su questi sconsiderati e diffusi comportamenti individuali (https://jacobinitalia.it/a-che-prezzo-la-sorveglianza-digitale-ci-salva-dal-virus/).

In più, l'anonimato può essere sempre aggirato anche con altri sistemi. Per dire, molti grandi negozi nel mondo, anche in Italia, si stanno già attrezzando con dei beacon bluetooth ai loro ingressi collegati ad un cellulare. Questi negozi scaricano sul cellulare un'app di contact tracing e si comportano come fossero un altro utente. Quando ricevono i codici e le allerte, possono sapere in maniera sicura chi è positivo e cioè chi in quel momento sta varcando la soglia del loro negozio. Ma anche senza cellulare, ci sono molti altri strumenti per fare monitoraggio, dai consumi energetici ai biglietti dei mezzi pubblici, dai pedaggi alla lettura delle targhe. L'anonimato, insomma, è già oggi una illusione nel mondo in cui viviamo, anche senza l'uso delle app di tracciamento, prodotte tra l'altro in questo caso dichiaratamente per il controllo. Il che non vuol dire assolutamente, però, che allora non ci dobbiamo curare di come i nostri dati vengono carpiti, di quale uso se ne faccia oppure non adottare accortezze per evitare che cadano nelle mani sbagliate e quindi ridurre i rischi al minimo. Al contrario, saremmo veramente delle e degli irresponsabili!

Si è fatto strada – principalmente da parte dei sostenitori del contact tracing – un frame narrativo per il quale i cittadini sarebbero ben disposti a cedere i loro dati personali per ragioni frivole – spesso si parla di quiz online sui social media, cose del tipo "*Che verdura sei?*" – ma sarebbero, al contrario, restii a cedere le medesime informazioni allo Stato e per fini sanitari. Scemi i cittadini, quindi, accusati di essere attenti alla riservatezza per i motivi sbagliati. Questa argomentazione sembra dire: la privacy è già abolita, che differenza fa ormai? Però il fatto che molta privacy sia già stata ceduta attraverso la commercializzazione e privatizzazione delle piattaforme web non autorizza oggi a non porsi domande sulle innumerevoli problematicità del contact tracing, dato che nessuna tecnologia è un destino ineluttabile dell'umanità!

Sul fatto che i quiz online che raccolgono in modo subdolo molti più dati di quelli che danno a vedere siano rischiosi non c'è dubbio alcuno, come non c'è dubbio che in tantissimi cadano in questo tranello. Questo non significa, però, che si debba concedere allora di essere inseriti in un progetto di tracciamento voluto dal proprio governo.

Si tratta di due piani completamente diversi. Anche se il mondo del tracciamento per fini commerciali e quello politico/governativo sono spesso intrecciati e complementari, specialmente quando si tratta di ambito sanitario non si possono confondere completamente i due piani, riducendo il contact tracing a una mera necessità burocratica. E il fatto di criticare la dimensione commerciale della sorveglianza, non significa automaticamente che quella statale sia invece da accettare acriticamente come benigna. Anzi!

Allo stesso tempo, è veramente stupido continuare a prendersela solo con i singoli individui per la loro mancanza di attenzione nella gestione in sicurezza dei propri dati, perché questo è l'alibi perfetto per cercare di nascondere le responsabilità di chi, in maniera invece del tutto consapevole, predispone piani e tecnologie per impadronirsi delle informazioni personali. Non ci si può dimenticare come gli individui siano più che altro *vittime* di piattaforme e applicazioni per loro natura poco trasparenti, dove il "*consenso informato*" è una beffa.

Comunque sia, le app di tracciamento non sono problematiche e rischiose solo per la riservatezza dei dati personali ma anche per la nostra libertà, in senso più generale. Perfino Human Rights Watch

ha suggerito che le applicazioni mobili per la tranciabilità dei contatti potrebbero potenzialmente costituire una grave minaccia per i diritti umani.
È possibile che la combinazione di queste app, insieme a telecamere a circuito chiuso o altri strumenti di sicurezza, possa portare ad identificare sempre con più accuratezza le persone. Inoltre il tracciamento dei contatti va ad aggiungersi alle altre tipologie di controllo possibili attraverso il cellulare (geolocalizzazione con GPS attivo; possibilità di prendere possesso di alcune parti del telefono attraverso l'hakeraggio con trojan del microfono e della telecamera; intercettazione di messaggi e telefonate; monitoraggio tramite il traffico dati on-line).
Un altro aspetto tutt'altro che confortante, è che queste app spesso si presentano in un modo salvo successivamente integrare funzioni aggiuntive e trasformarsi in qualcosa di diverso. Questa mutevolezza è confermata da Luca Foresti – a.d. della rete di poliambulatori privati del Centro Medico Santagostino che con Bending Spoons ha ideato Immuni – che al Corriere della Serra, in una intervista, alla domanda se Immuni può usare anche il Gps, ha risposto testualmente che *"il governo deve decidere se usare anche questo"*. Ammettendo in questo modo che il problema non è puramente tecnico ma anche politico e che, se ritenuto opportuno, in futuro l'app potrebbe ricomprendere anche la geo-localizzazione. Ma Luca Foresti dice anche di più, ovvero che "*Siamo già in grado di rilevare su base statistica assembramenti a rischio o di dire quali comuni hanno comportamenti sbagliati e quindi devono rivedere le politiche di contenimento. Non solo, questi dati possono essere incrociati con quelli dell'Istat per tracciare ulteriori mappe di rischio*".
Quali dati Istat? "*L'Istat divide tutto il territorio nazionale in "cellette" di 65 famiglie. Per ognuna di esse abbiamo la distribuzione della popolazione in base all'età: se sappiamo che in un determinato territorio c'è una maggiore concentrazione di anziani, sappiamo che c'è una più alta probabilità di avere vittime e che quindi dobbiamo pensare a interventi mirati per quella zona"* (https://www.corriere.it/tecnologia/20_marzo_18/coronavirus-pronta-app-italiana-tracciare-contagi-cosi-possiamo-fermare-l-epidemia-c6c31218-6919-11ea-913c-55c2df06d574.shtml?refresh_ce-cp).
Un altro modo per valutare l'impatto delle misure di contenimento di un governo sulla mobilità pubblica può consistere nel misurare il traffico lungo le strade. Ci sono molte app che possono farlo e i dati così forniti potrebbero essere integrati da quelli appresi dalle app di contact tracing. **Waze**, che è un navigatore-app scaricabile sul cellulare, ha per esempio messo a disposizione del sito Wired i dati relativi ai chilometri percorsi e alle ore di utilizzo dell'app in alcune province lombarde (Lodi soprattutto) tra il 15 ed il 21 febbraio, giorno in cui veniva istituita la zona rossa a Codogno e i sette giorni successivi. Quindi, lo diciamo ancora una volta, uno dei rischi più grandi è che le informazioni del contact tracing si vadano a integrare con l'insieme di dati disponibili che sono già in possesso dei controllori sociali, attraverso le sue tante appendici burocratiche-amministrative. Dati personali, per individuare persone reali tra la folla anonima di cittadini e consumatori, e che sono destinati, purtroppo, ad ampliarsi nei prossimi anni, se è vero che nei prossimi tempi l'impatto maggiore lo avranno le misure di sicurezza biometriche, come il riconoscimento vocale e facciale per accedere ad alcuni servizi (e già c'è chi evoca la prossima forma di violazione dei dati attraverso il *deepfake*, ossia attacchi portati avanti attraverso false identità, in cui sarà sempre più difficile distinguere ciò che è vero e ciò che non lo è perché la riproduzione audio/video potrà sfiorare la perfezione ...ecco un altro buon motivo per astenersi dal pubblicare *on line* contenuti multimediali con le nostre voci o i nostri volti che potrebbero essere utilizzati nei prossimi anni per costruire falsi profili, o anche false accuse nei nostri riguardi).
Ma soprattutto, le app di contact tracing trasformano la prossimità, il contatto sociale in allarme, una cosa mostruosa a dirsi mentre non è affatto scontato che la vicinanza ad un malato comporti automaticamente l'ammalarsi a propria volta. Un'app, qualsiasi sia, non potrà mai sostituirsi ad

un’analisi medica. È la diagnosi a dare un responso di positività (anche questo sempre con dei margini di errore, tra l’altro!). Ma visto che i test non vengono eseguiti, ma centellinati per risparmiare, si è voluta trovare la soluzione in queste tecnologie di controllo di massa che sotto il profilo sanitario sono inutili e danno solo un finto senso di sicurezza, anzi di “immunità” di fronte al virus. Un modo per mostrare che il governo sta facendo qualcosa, mentre con una mano continua a tagliare la salute pubblica e con l’altra a finanziare quella privata, le spese militari e il controllo sociale e poliziesco. Anche volendo credere nella bontà delle intenzioni – cosa che non abbiamo intenzione di fare - un’app di tracciamento è chiaramente del tutto inutile se i dati raccolti non vengono accompagnati ad azioni pratiche come sottoporre a tampone i soggetti che hanno avuto contatti con positivi. E abbiamo visto come sotto questo aspetto, in Italia, la disponibilità di test diagnostici sia mancata del tutto, persone anziane siano state lasciate morire in casa senza alcun test e non sia stato sottoposto a tampone nemmeno il personale sanitario o quello di cura nelle RSA, cioè le categorie di persone più a contatto con potenziali malati. L’unica opzione dopo aver ricevuto un allerta sull’app resterà la quarantena autoimposta!
Il rischio è quello di rendere disponibili informazioni sanitarie di qualsiasi tipo al di fuori del circuito sanitario, illudendosi che un'applicazione possa fare il lavoro di un medico, che almeno sulla carta dovrebbe essere quello di prendersi cura. Ma queste app non ci salveranno! Una persona malata ma senza sintomi, anche con l’app installata, non saprà mai che in realtà e proprio lui a diffondere il contagio, mentre l’app gli darà una falsa sensazione di sicurezza percepita. L’app non potrà mai distinguere una persona asintomatica, ma contagiosa, che non ha mai sviluppato sintomi, proprio perché non è mai stata sottoposta ad un test.
Ancora una volta, la vicinanza non è poi di per sé “contaminazione” automatica: potrei essere stato in coda a un negozio accanto a una persona risultata positiva o aver parlato con un amico malato attraverso un plexiglass senza essermi infettato a mia volta! Magari vicino a me è passata un’auto, o magari la persona contagiata è dall’altra parte di un muro, in un’altra abitazione. In questo modo, per esempio, tutti i residenti di un palazzo potrebbero essere messi in quarantena forzata, dato che il Bluetooth funziona anche al chiuso con un raggio di 40 metri. A preoccupare è anche l'inaffidabilità del funzionamento del tracciamento, che nelle zone affollate potrebbe captare una "falsa" prossimità, ad esempio tra due soggetti separati da una parete, oppure non considerare la durata della vicinanza che invece può essere un indice importante nella trasmissione del contagio. Il sistema bluetooth non può tenere conto nemmeno del fatto che una persona abbia o no la mascherina, se uno è di spalle, se uno ha starnutito, ecc. Si creeranno inevitabilmente molti falsi allarmi sui cellulari, che si tradurranno in una valanga di "falsi positivi". Un problema che non solo esiste ma è anche molto alto. Poiché la maggior parte delle notifiche di esposizione non porterà a vere infezioni, molti utenti verranno istruiti all'auto-quarantena anche quando non sono stati infettati. Una persona può tollerarlo una o due volte, ma dopo alcuni falsi allarmi e il conseguente inconveniente di un autoisolamento prolungato, è prevedibile che in molti inizieranno a ignorare gli avvertimenti (e speriamo anche ad arrabbiarsi sul serio). È inevitabile, poi, che questi allarmi, che aumenteranno al ritmo di quanti scaricheranno l’app sul proprio cellulare, genereranno apprensione diffusa, senso di vergogna, ansia e rabbia quando lo schermo si colorerà di rosso per l’arrivo dell’alert e quando ci si dovrà auto-recludere nel limbo del “probabilmente ammalato”.
Che le app di tracciamento non siano efficaci sul piano del contenimento sanitario di un virus, d’altronde, ce lo dimostra proprio l’esempio di Singapore, preso ad esempio per lo sviluppo di “Immuni”, un paese che queste tecnologie le ha usate estensivamente perché le aveva già a disposizione e dove la popolazione è ormai abituata a farlo. Risultato, Singapore ha dovuto mettere comunque tutto il paese in quarantena, nonostante l’uso di app che si sono rivelate incapaci di

prevenire il contagio.
Di più! Gli standard di contact tracing forniti dall'European Center for Disease Prevention and Control (ECDC) nel marzo 2020 relativamente all'epidemia di COVID-19 indicano in 12 ore – con l'utilizzo di 3 risorse di personale specializzato – il tempo medio per ogni operazione manuale di contact tracing, con un tasso di successo peraltro insufficiente a identificare tutti i contatti o comunque a ridurre il numero di contatti secondari potenzialmente infetti.
Ma uno degli aspetti fondamentali è un altro: le persone anziane, proprio quelle più esposte e colpite dal virus, sono quelle che meno possiedono uno smartphone. Per cui per loro continuerà ad essere praticato il tracciamento manuale da parte del le strutture e del personale medico e le app non serviranno.
Ma allora, se queste app non sono efficaci per contenere il contagio, a cosa serviranno realmente?

****

RIFLESSIONI CONCLUSIVE

«Le misure temporanee hanno la fastidiosa abitudine di sopravvivere alle emergenze, specialmente se c'è sempre una nuova emergenza all'orizzonte. Qualsiasi cosa entri a far parte della quotidianità presto comincia a passare inosservata».

"Forse è arrivato il momento di prendere d'assedio i palazzi del governo. Non lasciare le piazze a chi chiede la riapertura dei negozi".
Tom Morello, chitarrista dei Rage Against The Machine.

Le misure del distanziamento interpersonale e la paura del contatto con gli altri, generati dall'epidemia e dai decreti dei governi, hanno esasperato le tendenze già in atto della società contemporanea. All'orizzonte si delinea un nuovo regime sociale, senza contatto umano, o con il minimo contatto possibile e regolato dalla burocrazia statale e dai diktat dell'OMS, e soprattutto dalla tecnologia.
La crisi sanitaria ha enormemente peggiorato l'influenza delle tecnologie sulla nostra vita, non solo per quanto riguarda la dipendenza dall'informazione ufficiale attraverso i media, ma anche perché mesi di confinamento domestico hanno avuto come conseguenza immediata la radicalizzazione della dipendenza dai computer e dagli schermi degli smartphone. Con il confinamento a casa, l'uso di computer e schermi sembra l'unica modalità di connessione col mondo. Come a dire: "Resta a casa" … ma su Internet!
L'emergenza Covid19 è stato un enorme vantaggio per i governi, che hanno potuto accelerare la sostituzione dei costosi servizi pubblici con portali online. Stessa cosa per le imprese, che guardano al futuro sognando fabbriche gestite interamente da robot, assistiti magari da pochi dipendenti

qualificati attraverso il monitoraggio da remoto e il tele-lavoro, e anche qui i paesi asiatici come la Cina sono spesso presi come esempio e percepiti come all'avanguardia.
Per ciò che concerne le app di contact tracing, nel tempo, le persone potrebbero essere portate ad abituarsi all'idea di svolgere le proprie attività quotidiane o di frequentare determinati luoghi o non frequentarli sulla base di ciò che un'app dice loro di fare. Gli strumenti tecnologici hanno in sé questo potere di assuefazione che è la conseguenza del delegare il proprio giudizio personale e di discernimento ad un'applicazione o a un'intelligenza artificiale.
L'emergere del virus che provoca il Covid19, come quello di altri virus almeno dall'anno 2000, è collegato da molti ricercatori, sia indipendenti ma anche degli stessi legati agli enti istituzionali, alla deforestazione, che costringe molte specie animali selvatiche a entrare in contatto inaspettato con l'uomo. Altri hanno messo in discussione gli allevamenti a concentrazione intensiva, che usano antibiotici mutageni. Se queste sono le cause, le app di tracciamento e le altre risposte tecnologiche forniscono una falsa soluzione, mentre l'attuale pandemia dovrebbe spingerci, al contrario, a trasformare radicalmente una società in cui la crisi ecologica, l'urbanizzazione dilagante, la deforestazione, gli allevamenti intensivi, l'inquinamento dell'aria, l'eccessiva mobilità delle merci e dei capitali possono avere conseguenze così incontrollabili. Dire che la risposta deve essere tecnologica – illudendoci di poter controllare la natura (e questa pandemia è il fallimento conclamato di questa illusione) - è voler continuare sulla stessa strada che ci ha portato a questa pandemia e ci porterà alle prossime catastrofi.
L'emergenza di questo coronavirus, viceversa, sta servendo da ponte sia per dare alle aziende un nuovo accesso ai dati privati delle persone tramite le app di tracciamento e le altre tecnologie di sorveglianza, sia ai governi di molti paesi permettendogli di paralizzare, per un periodo indefinito, le proteste sociali, gli scioperi e le manifestazioni.
Per quanto riguarda le aziende private, nel provvedimento del 16 aprile con cui il governo italiano ha stipulato il contratto per l'app "Immuni" con Bending Spoons, si legge che "*la società Bending Spoons S.p.a., esclusivamente per spirito di solidarietà e, quindi, al solo scopo di fornire un proprio contributo, volontario e personale, utile per fronteggiare l'emergenza da COVID-19 in atto, ha manifestato la volontà di concedere in licenza d'uso aperta, gratuita e perpetua, al Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica COVID-19 e alla Presidenza del Consiglio dei ministri, il codice sorgente e tutte le componenti applicative facenti parte del sistema di contact tracing già sviluppate, nonché, per le medesime ragioni e motivazioni e sempre a titolo gratuito, ha manifestato la propria disponibilità a completare gli sviluppi informatici che si renderanno necessari per consentire la messa in esercizio del sistema nazionale di contact tracing digitale*".
Lo slancio "filantropico" di Bending Spoons SpA si era già palesato 15 giorni prima della "*fast call for contribution"* con una donazione di un milione di euro alla Protezione Civile.
Ma davvero la società privata Bending Spoons non ci guadagna niente? Davvero le aziende private fanno tutto questo solamente per *"spirito di solidarietà"*, come ci tengono a far sapere dal governo italiano? Per quanti hanno un minimo di dimestichezza di marketing, la pubblicizzazione dell'adozione da parte di un governo di un app sviluppata da una società privata, comportano per quest'ultima vantaggi economici in termini di ritorno di visibilità, notorietà del brand e richieste di partnership. Tutte cose che generano profitto. Non solo, tra le dinamiche del *Marketing* aziendale vi è sempre più quello del monitoraggio dei dati, utile a rilevare le opinioni e i comportamenti degli utenti*;* si tratta di un business mastodontico per le aziende, da cui trarre le informazioni strategiche per l'impostazione delle proprie scelte commerciali. Ciò che sfugge ad un pubblico di non addetti ai lavori è l'enorme valore del dato stesso, in possesso delle società che gestiscono i sistemi di

tracciamento o gli accessi ai server o che fanno manutenzione tecnologica sugli stessi.
L'aggregazione di dati clinici e movimenti delle persone genera valore. Non importa il grado di anonimato, quello che importa è il controllo di una vasta quantità di dati digitali anche aggregati.
L'amministratore delegato del gruppo milanese, Luca Ferrari, ha ricordato che Bending Spoons finanzierà autonomamente i propri costi. Ma davvero queste brave persone fanno tutto questo senza volere nulla in cambio? O quello con cui verranno ripagati di questo strano altruismo sono proprio i nostri dati? Tracciare i contatti di milioni di abitanti e le informazioni sanitarie di questi ultimi significa disporre gratuitamente, senza neanche bisogno di pubblicità mirate, di milioni di dati leggibili, interpretabili e vendibili ai futuri clienti. Milioni di dati e di numeri sui quali disegnare persuasive politiche commerciali. La stessa cosa a cui ambiscono società multinazionali come Google o Apple. Da qualche parte è stata scritta una frase più che opportuna: *"allo Stato non costa nulla ma noi pagheremo tutto!"*.
Lo Stato, già! Dicevamo che l'emergenza coronavirus sta servendo ai governi dei vari paesi per mettere in atto tipologie di intervento impensabili in tempi "normali".
In Spagna, dall'inizio della crisi sanitaria, la stampa mainstream si è chiesta apertamente se la "democrazia" non sia un peso che condanna i governi all'inefficacia, mentre in quasi tutti i paesi europei i politici "liberali" hanno espresso la loro ammirazione per l'autoritarismo cinese ad alta tecnologia: geolocalizzazione dei telefoni cellulari, sistemi di classificazione sociale alimentati da dati costantemente raccolti con Internet, riconoscimento facciale, uso di droni per monitorare, colpevolizzare e punire la popolazione. Da molte parti la sola volontarietà di queste tecnologie è stata criticata ed è stato richiesto a gran voce, per esempio, di rendere anche le app di contact tracing obbligatorie per legge. In Italia, il presidente della regione Veneto, il leghista Luca Zaia, ha fatto intendere che sarebbe stato pronto a rendere obbligatoria un'app per gli abitanti veneti, ma anche insospettabili come Shoshana Zuboff, della Harvard Business School, autrice del libro cult *"Il capitalismo della sorveglianza"*, liquidando il dibattito sulla difesa della privacy, ha sposato la causa dell'obbligatorietà, sostenendo che*"le app per controllare la diffusione del virus dovrebbero esser gestite da istituzioni pubbliche e diventare obbligatorie come i vaccini"* (*https://rep.repubblica.it/pwa/intervista/2020/04/09/news/shoshana_zuboff_altro_che_privacy_le_app_per_il_controllo_della_pandemia_devono_essere_obbligatorie_come_i_vaccini_-253587046/*).
Società che sviluppano software ad uso militare e d'intelligence hanno saputo presentare, sfruttando questa fase, a molti paesi soluzioni tecnologiche all'avanguardia: si parla di aziende come la **Palantir Technologies** (specializzata nell'analisi di Big Data e che offre i suoi servizi al ministero della difesa statunitense oltre che a CIA, NSA e FBI), **NSO Group** (azienda che vende a governi di tutto il mondo sistemi di spionaggio e Trojan) o l'italiana **CY4GATE** (azienda romana che opera nella Cyber Electronic Warfare, Cyber Intelligence e Cyber Security e che avrebbe proposto al governo l'utilizzo, a titolo gratuito di una sua *"piattaforma software capace di raccogliere, elaborare e aggregare dati di geolocalizzaizone provenienti da molteplici dispositivi mobili";* vedi https://roundrobin.info/2020/05/considerazioni-sulle-applicazioni-di-tracciamento-dei-contatti/).
Per i governi con derive autoritarie, la situazione che stiamo vivendo è un'opportunità d'oro per poter promuovere decreti e leggi speciali che accentrino ancor più il potere nelle mani del governo e introdurre tecnologie di sorveglianza. L'uso costante del linguaggio militare, il paragone continuo alla "guerra", la revoca di diritti essenziali e l'approvazione di misure eccezionali in "tempi di pace" impensabili fino a poco tempo fa, creano un ambiente favorevole al consolidarsi di un potere sempre più autoritario, in cui si giustifica pressoché qualsiasi decisione. Chi si oppone, come abbiamo visto anche in Italia, viene multato, denunciato, se non arrestato o comunque visto come un pericoloso "traditore della patria" dai suoi stessi concittadini, ammaestrati ad arte dalla

propaganda di Stato.
Come è stato detto da più parti, in tempi difficili è molto più facile approvare misure estreme, ma in tempi *normali* è molto difficile revocarle.
In Ungheria, col pretesto dell'emergenza sanitaria, il parlamento ha approvato una legge che dà "pieni poteri" al primo ministro, Viktor Orbán (che si è contraddistinto in questi 10 anni al governo per la sua linea reazionaria, xenofoba, omofoba e ostile alla libertà d'informazione) che gli permette di legiferare per decreto senza bisogno del parlamento durante tutta la durata dello stato d'emergenza nazionale, per il quale non è previsto alcun limite temporale. La legge, che prevede la sospensione di nuove elezioni e referendum, la revoca e la promulgazione di qualsiasi legge e che permette di perseguire penalmente chi diffonde "false notizie" (pene fino a 5 anni di carcere per chi diffonde *"disinformazione che ostacoli la risposta del governo alla crisi sanitaria"*, cioè gli oppositori del governo), è stata approvata dal parlamento ungherese con 137 voti a favore e 53 contrari.
Ricordiamo che l'Ungheria fa parte da 16 anni dell'Unione Europea, non è un lontano regime asiatico. Ma Orbán è in buona compagnia: tralasciando l'esempio noto della Cina, molti altri governi nel mondo stanno usando questa crisi sanitaria come pretesto per schiacciare il dissenso interno.
In Slovenia, dopo aver elogiato la gestione di Orbán in più di un'occasione, l'esecutivo del conservatore Janez Jansa, al governo del paese dal 13 marzo, sta utilizzando la lotta al coronavirus come una scusa per restringere la libertà d'informazione e attaccare giornalisti scomodi.
In Thailandia e nelle Filippine sono state approvate leggi bavaglio per permettono di incarcerare chiunque pubblichi "informazioni false".
In Giordania, Oman, Marocco, Yemen e Iran le autorità hanno sospeso la pubblicazione e distribuzione dei giornali.
In Brasile, il presidente Jair Bolsonaro ha revocato la legge di trasparenza: la norma che permette agli abitanti del paese di conoscere l'operato del governo mediante l'accesso a informazioni e documenti governativi.
In India il governo voleva legalizzare la censura, in quanto "informazioni false o imprecise potrebbero causare reazioni di panico tra la popolazione", per cui i media dovrebbero limitarsi a pubblicare solo le informazioni ufficiali rilasciate dal governo. La Corte Suprema ha negato al governo la possibilità ma nel suo verdetto ha invitato i media a pubblicare solo le informazioni ufficiali sulla pandemia.
Il Turkmenistan ha addirittura deciso di proibire l'uso della parola "coronavirus" (per le misure introdotte da questi paesi vedi https://www.valigiablu.it/leader-autoritari-coronavirus/).
Negli Usa a seguito dell'ennesimo omicidio di un uomo dalla pelle nera, George Floyd, da parte della polizia americana, la popolazione nera, esasperata anche dai mesi di lockdown con continue prevaricazioni da parte della polizia, ha fatto scoppiare delle rivolte in tutti gli stati federali con attacchi e incendi a caserme e scontri, fino a lambire con le proteste la Casa Bianca dove il presidente Donal Trump ha dovuto essere nascosto in un bunker sotterraneo.
Intanto anche in Italia sono stati stanziati dal governo Pd-5Stelle-ItaliaViva-LeU fondi per oltre 100 milioni di euro per il pagamento degli straordinari per i controlli connessi all'emergenza per le Forze di polizia, le Forze armate, il Corpo di polizia penitenziaria, il Corpo nazionale dei Vigili del Fuoco, il personale della carriera prefettizia e delle le polizie locali (http://www.mef.gov.it/focus/Decreto-Cura-Italia-cosa-prevede-per-le-famiglie/). Un regalo che serve anche per assicurarsi la riconoscenza delle forze della repressione quando ce ne fosse bisogno, se in futuro scoppiassero proteste sociali e rivolte, sull'esempio degli Usa, a seguito della probabile

crisi economica che seguirà dopo i mesi di lockdown.
Questo è il quadro mondiale in cui si inserisce l'introduzione di tecnologie di sorveglianza quali le app di contact tracing. Perché sapere di essere costantemente tracciati (e rintracciati) può essere fonte di conformismo e sottomissione alle autorità anche quando non si vive sotto una dittatura; esattamente come già succede con le telecamere, i comportamenti si adattano e si adeguano al controllo che subiscono. Come è già stato detto da altre parti in maniera perfetta: *"la diffusione di queste App e la convivenza con il tracciamento costante dei propri spostamenti – sotto il costante inganno del "tanto non ho niente da nascondere", anzi "lo fanno per il nostro bene" – apre la strada all'accettazione sociale di altre tecnologie del controllo che fino ad ora erano state malviste dalla maggior parte delle persone dotate di buon senso, come le telecamere capaci di riconoscimento facciale negli spazi pubblici (dando un bel colpo di spugna a tutte le problematiche relative al possibile abuso dei dati biometrici) o l'utilizzo dei droni per la sorveglianza"* (https://malamente.info/2020/05/23/immuni-e-diary-perche-le-app-per-il-tracciamento-non-sono-la-soluzione-ma-un-ulteriore-problema/#more-2550).
In tutta Europa i governi, assecondando le richieste delle categorie imprenditoriali che chiedevano il ritorno al lavoro (preferibilmente con più capacità di sfruttamento della manodopera), l'apertura totale delle aziende e il rilancio dell'economia, hanno affrettato le riaperture delle attività economiche, o almeno quelle che avevano chiuso, dato che per la maggior parte le fabbriche più grandi, come quelle del nord-Italia, erano rimaste aperte anche durante il lockdown per fare un piacere alla Confindustria e alle associazioni padronali. Per questo diventa urgente per i governi dimostrare di avere la situazione in mano, lanciando le app di tracciamento, che non garantiscono nulla ma che servono a dare un'illusoria sensazione di sicurezza, dal momento che come si è visto gli Stati non hanno nient'altro a disposizione per proteggere le popolazioni della vuota retorica del "se restate a casa andrà tutto bene". Le app di tracciamento servono a dare l'impressione che il governo stia facendo "qualcosa", non importa se del tutto inutile quando non addirittura controproducente. Il messaggio che si vuole far passare è quello dell'esistenza di una tecnologia salvifica al nostro servizio; in realtà la promozione di queste app risponde solamente all'affannosa ricerca di una malinterpretata "sicurezza". Mai che ci si ponga il problema: ma la sicurezza di chi? I tecnocrati e i governi di tutto il mondo affermano di salvarci dal coronavirus accelerando quello stesso sistema di produzione e di sviluppo tecnologico che ci ha portato alla situazione attuale. Dobbiamo riconoscere in questa posizione assurda, una scelta votata al fallimento e quindi assassina. Del resto è certo che la tecnologia non ci salverà, come scritto in un comunicato durante il lockdown (vedi http://www.ecn.org/xm24/2020/05/09/di-tecno-assoluzionismo):*"Oggi la soluzione tecnica viene sbandierata come panacea, semplice, accessibile, ma è pura propaganda. La tecnica asservita al potere economico e politico sembra avere il diritto di parlare di tutto, proponendo soluzioni che vanno dalla sanità, alla formazione, alla gestione dei flussi di persone, ma parla sempre da una posizione disincarnata, senza l'esperienza diretta delle problematiche e delle risorse fondamentali da preservare. (…) La pre-condizione per questa fantomatica fase due dovrebbe essere il ripristino di una sanità pubblica di prossimità, smantellata da scelte di governo bipartisan. (…) Eppure non se ne sente parlare. Se non ci sono abbastanza laboratori d'analisi per fare un tampone a una persona con la polmonite, se non c'è nessuna persona in grado di andarglielo a fare a casa, se non ci si prende cura delle persone capillarmente, a poco serviranno uno smartphone e una app"*. E non potrebbe essere altrimenti, dato che smartphone ed app non possiedono proprietà curative! Tra l'altro, a che serve una app di contact tracing se, come ci hanno continuato a ripetere per mesi, persone asintomatiche possono trasmettere il contagio, che avviene dunque anche attraverso persone che ancora non sanno di essere infette e che quindi non possono

avvertire altre persone di esserlo attraverso la lista dei contatti dell'app? Ed infatti, se le cose stanno così, le app di contact tracing non avrebbero proprio senso. É un caso se, con un tempismo davvero eccezionale, appena le app di tracciamento sono state lanciate sul mercato, gli stessi "esperti" che avevano seminato il terrore per primi sulla trasmissione del virus da parte degli asintomatici hanno fatto marcia indietro ed hanno detto che no, contrariamente a quanto affermato fino a pochi istanti prima, le persone asintomatiche non sono contagiose? E se lo sono, lo sono molto poco? Scusate se a questo punto, degli "esperti" che ci vengono a dire tutto e il suo contrario, non ci fidiamo granché e ne facciamo volentieri a meno, come a meno vogliamo continuare a fare delle app che ci consigliano "per il nostro bene"!

Quello che abbiamo imparato è che ancora una volta si cerca di sacrificare la libertà in nome di un bene considerato più grande, in questo caso la salute pubblica. Ma è uno scambio che conviene? Alcuni rispondono con un netto "sì", per la semplice ragione che, viene detto, la sorveglianza digitale è stata un fattore strategico per quelle nazioni che sembrano essere riuscite a gestire meglio la diffusione del virus. Ma abbiamo già visto che anche questa è stata una menzogna fatta girare ad arte, dato che quei paesi che per primi hanno introdotto il contact tracing hanno poi dovuto ammettere che questo in realtà non è servito a nulla e sono stati costretti a ricorrere comunque a chiusure mirate e al lockdown. La vera differenza tra quei paesi che hanno saputo contenere il numero dei contagi e, per esempio, l'Italia, l'ha fatta semmai un sistema sanitario efficiente, al contrario del martoriato sistema sanitario italiano che si è dimostrato a dir poco carente sotto tantissimi punti di vista.

E' difficile pensare che le persone scaricheranno in massa sul proprio smartphone un'applicazione che potrebbe cambiargli la vita in peggio, costringendole a due settimane di quarantena, col rischio di denunce penali in caso di violazione del confinamento domestico (si parla addirittura di "attentato alla salute pubblica"). Il governo per "invogliare" le persone a scaricarla volontariamente potrà sempre ricorrere ad incentivi, premi, bonus e punti voucher. Ma poi, come farà a controllare che chi ha scaricato l'app stia andando in giro col cellulare acceso? Certo l'installazione e l'uso delle app di contact tracing nelle società occidentali, ancora formalmente democratiche come in Italia, non è obbligatoria, per ora. Ma una volta sdoganata questa tecnologia ed accettata dalla maggioranza della popolazione potrebbe diventarlo presto, se non per forza di legge per lo meno in maniera subdola: averla sul proprio telefonino potrebbe essere la discriminante per accedere a certi luoghi, farsi assumere in certi lavori o per salire sui mezzi pubblici. Un certificato di immunità fittizio, che non prova certo davvero che si è "immuni" ad un virus oppure no, ma che ha delle implicazioni reali sul proprio vissuto quotidiano. Ovviamente, chi rifiutasse di installare un'app di tracciamento, quando divenisse obbligatoria di fatto o per convenzione, verrebbe guardato con sospetto e messo ai margini della società in cui vive. Chi non vorrà scaricare l'app potrebbe subire pregiudizi da parte delle altre persone, un po' come abbiamo visto accadere con l'accanimento contro chi faceva jogging, chi portava a spasso il cane, chi andava al parco col bambino, chi usciva senza la mascherina, ecc. La risposta negativa alla domanda *"tu l'hai scaricata l'app?"* potrebbe diventare fonte di guai, esattamente come è successo alle persone aggredite da passanti-sceriffi perché non indossavano la mascherina.

Uno sguardo alla storia delle tecnologie mostra che non si è quasi mai tornati indietro con i dispositivi liberticidi introdotti in tempi di "crisi": se accettati su larga scala sotto l'egida dello Stato, la domanda di controllo farà sì che sarà molto difficile impedirne prima o dopo l'estensione a tutta la popolazione, alla fine in maniera obbligatoria. Imporre a tutta la società l'utilizzo di app di contact tracing è comunque ad oggi forse ancora impossibile, perché permangono delle fasce della popolazione il cui uso quotidiano degli smartphone può dirsi tutt'altro che scontato. Per questo si

sono fatte avanti voci che hanno proposto, per gli anziani che non possiedono smartphone, perfino l'imposizione di appositi braccialetti elettronici di tracciamento indossabili. Fonti del governo hanno smentito che una tale proposta fosse stata presa davvero in considerazione, ma già l'averla formulata suona alquanto preoccupante. Con le debite proporzioni, stiamo parlando del corrispettivo del codice a barre per le merci o del numero identificativo IBM tatuato agli ebrei nei campi di concentramento nazisti. Dunque, la cosa più probabile è che, procedendo per tappe, in un primo momento l'installazione di queste app potrebbe diventare "obbligatoria ma non obbligatoria". Mentre apparentemente ed ufficialmente il download potrebbe rimanere sulla carta volontario, potrebbe man mano diventare effettivamente obbligatorio nei luoghi di lavoro e nelle scuole, o per entrare in qualche luogo o per accedere ad alcuni servizi. C'è un grande spazio interpretativo tra qualcosa che è legalmente richiesto e 'ufficiosamente' obbligatorio.
Con appositi decreti o successive modifiche del codice, queste applicazioni potrebbero sempre, in un secondo tempo, mutare i loro scopi dichiarati e, a seguito di aggiornamenti tecnici ciclici e avvicendamenti normativi, diventare strumenti diversi da quelli che erano in origine, magari con impostazioni per poter accedere a determinati luoghi o per fornire i dati alle polizie, per finire magari per mostrare pubblicamente chi ha contaminato chi e quando, con l'immaginabile caccia all'untore che si scatenerebbe (un capro espiatorio perfetto in tempo di crisi economica, per alleggerire il peso delle responsabilità dello Stato).
Un altro rischio, ovviamente, è quello che, in caso di nuovi aumenti dei contagiati dopo le riaperture, nell'imporre un nuovo lockdown si possa passare dal controllo tramite auto-certificazioni cartacee alle certificazioni digitali sull'applicazione da mostrare ai controlli quando un poliziotto ti ferma, anche se per ora quella di abbinare "Immuni" all'autocertificazione o ad una patente di immunità rimane appunto solo un'ipotesi. Ipotesi che però è stata anch'essa fatta. In seguito a nuovi contagi, magari dopo le vacanze estive (che si devono fare per far girare l'economia, ecco allora il "bonus vacanze" elargito dal governo!) scaricare l'app "Immuni" continuerà forse ad essere un atto volontario ma bisognerà fare i conti con le eventuali fresche limitazioni che il governo potrebbe disporre. A quel punto potrebbe non essere così scontato che chi non ha l'app scaricata sul proprio cellulare possa continuare a godere delle stesse libertà di chi l'ha. Il rischio è che l'aver sacricato l'app possa diventare una sorta di nulla-osta alla circolazione, un'autocertificazione digitale, un "passaporto immunitario" da esibire ai controlli della polizia. Si potrebbe creare una situazione in cui chi ha l'app può uscire di casa, mentre chi non l'ha no. Cittadini di serie A, e (non)cittadini di serie B. Sarebbe un ampliamento della pratica del controllo da parte della polizia che tende ad allargare sempre più i suoi campi di intervento per mezzo della tecnologia. E per fortuna che qualcuno dava per morto lo Stato e le sue appendici.
Proprio come già avviene in Cina e in altri paesi asiatici, l'app di contact tracing potrebbe essere "abbinata" all'accesso a determinati servizi e beni: pagamenti tramite smartphone, prenotazioni, accesso al welfare, bonifici degli stipendi, il che determinerebbe una coercizione indiretta all'utilizzo. Sebbene non obbligatoria, il tuo datore di lavoro ti potrebbe dire comunque che non puoi andare a lavorare senza l'app attiva. Di questo passo, di certo si arriverebbe a una legge per disciplinare non solo l'installazione ma anche l'uso e l'obbligo di queste app, specie in ambienti di lavoro o in luoghi pubblici, con il risultato di portare la discriminazione basata su questa tecnologia alla luce del sole e renderla perfettamente legale. Per lo sviluppo di queste tecnologie, è infatti stato fatto esplicito riferimento che in un prossimo futuro, se solo lo si volesse, potrebbe essere possibile adottare soluzioni che utilizzano non dati anonimi ma i dati personali delle persone (numero di telefono, nome, cognome, ubicazione). Con l'unica "raccomandazione" che per farlo debba essere necessaria una legge approvata dai rispettivi parlamenti nazionali.

Non vi è alcuna reale garanzia contro questi "cambiamenti" di registro delle app di tracciamento, tanto più se la rabbia e la paura generate dalla prossima crisi economica farà gettare definitivamente la maschera democratica ai governi. Sia rendendole obbligatorie, sia a causa di un'eccessiva pressione sociale, le persone che non usano queste applicazioni rischierebbero di non trovare lavoro o di non poter accedere a determinati luoghi liberamente. E il libero consenso? Potrebbe finire sacrificato sull'altare di un finto interesse collettivo perché è scontato che queste app apriranno delle brecce nel muro della cosiddetta privacy, ovvero il diritto alla riservatezza. Con l'estensione dell'uso di queste app, immancabilmente anche le normative sulla privacy verranno prima o poi opportunamente "ritoccate" (e non certo in meglio!). Molti esperti di tecnologia lo ritengono ormai un passaggio inevitabile, e lo giustificano con la necessità di tutelare la salute pubblica. Dovrebbero spiegarci perché mai un diritto dovrebbe essere più tutelato di un altro e perché il diritto alla salute lo dovrebbe essere più di quello alla riservatezza e alla libertà individulae. Mettere l'accento sul tema della salute per "consigliare" e alla fine imporre strumenti di sorveglianza, significa consapevolmente farsi scudo con un argomento che nelle intenzioni non deve ammettere la possibilità di replica. Il dissenso viene stroncato sul nascere con dissertazioni scientifiche da parte di "esperti" dalla pretesa neutralità e, si sa, la scienza come la matematica non è un'opinione. Certo, a prima vista sembra un discorso razionale che fila: il diritto alla riservatezza interessa la sfera individuale mentre quello alla salute è un diritto collettivo ed è quindi più importante. Ma in realtà non è così: ci si dimentica che la società è fatta di individui. Il modo in cui viene tutelata od erosa la libertà individuale non può essere disgiunta dall'interesse collettivo: la mia libertà è la libertà di tutte e tutti. E non crediamo che la salute, e il modo di tutelarla, sia solo una mera questione medica, soprattutto oggi quando questa ricade, come abbiamo potuto constatare, sotto l'amministrazione del controllo sociale e dell'ordine pubblico.

Lo "slittamento" più insidioso è che queste app lascino che la salute di tutti, proprio perché considerata bene di interesse collettivo, sia presto vista da tutti: datori di lavoro, vicini, polizia! Tutti potrebbero conoscere che malattia ha una persona, dove l'ha contratta e se ha contagiato qualcun altro. È stato anche fatto presente il rischio che con le app di tracciamento gli assistenti sanitari possano diventare assistenti di polizia.

Le domande che si impongono riguardano anche lo stoccaggio dei dati sanitari e la loro gestione futura. Un simile strumento potrebbe divenire addirittura discriminante per l'accesso al mondo del lavoro e alle scuole, alle strutture assistenziali e di cura. Perché? Oggi l'app traccia i contagiati da coronavirus ma chi ci dice che domani non potrebbe farlo per ogni altro genere di malattia o patologia? Immaginiamo che le compagnie di assicurazione saranno assai golose di mettere le mani su informazioni che riguardano la salute dei loro clienti. Associare un singolo individuo a portatore di una malattia apre scenari davvero inquietanti.

Per i datori di lavoro, il vantaggio di un'app di tracciamento dei contatti è fin troppo chiaro: possono proteggere meglio la loro produzione licenziando la forza lavoro malata oppure sospetta tale.

Mentre le autorità che gestiscono la banca-dati del sistema di tracciamento potrebbero utilizzare le informazioni raccolte per altri scopi, e non solo per fini "statistici". C'è chi si fida ciecamente del governo e dei suoi ministeri… eh, noi saremo anche inguaribili diffidenti ma invece non ci fidiamo neanche un po'!

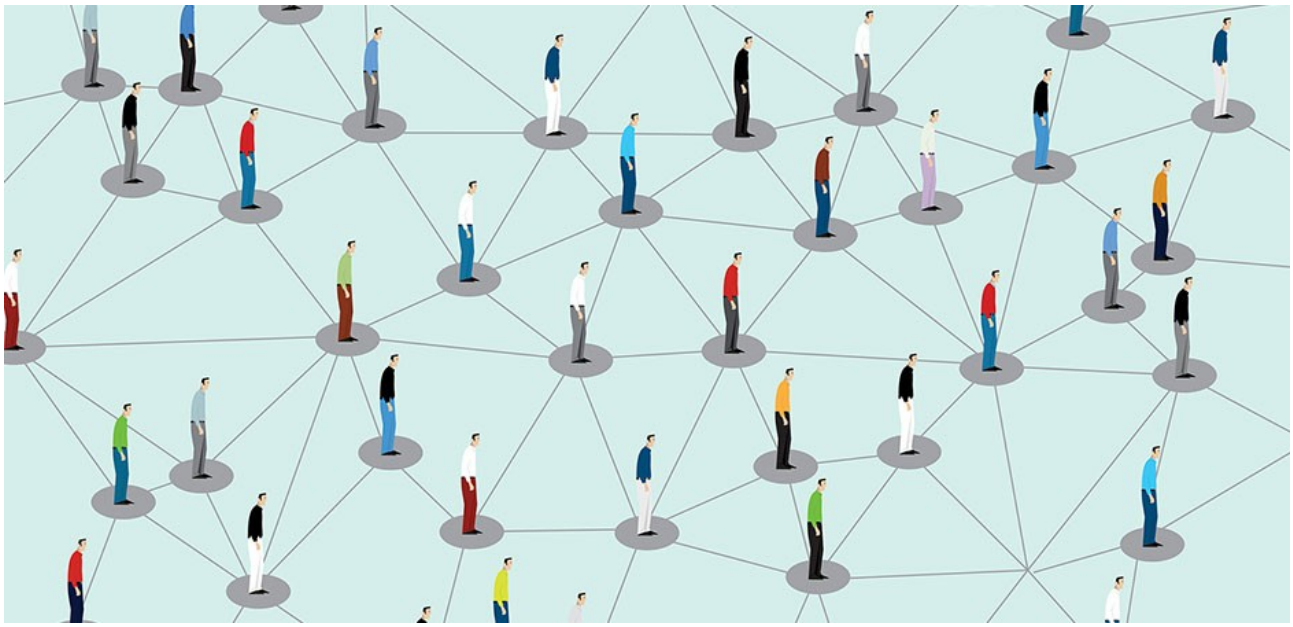
E perché l'app di contact tracing non dovrebbe diventare obbligatoria anche tra i tifosi per accedere allo stadio? Una volta sdoganato l'uso di queste app, sarà facile per i singoli ministeri decidere autonomamente di renderne obbligatorio l'uso per chi, ad esempio, vorrà seguire una partita allo stadio o un concerto. Citiamo lo stadio non a caso poiché, nella ricerca di nuovi strumenti di controllo sociale, sappiamo benissimo che è da sempre il laboratorio di sperimentazione preferito in

cui testare le soluzioni repressive: un caso esemplare è il Daspo, introdotto per le manifestazioni sportive e poi allargato al resto della società con il famigerato Daspo Urbano.
Allo stesso modo, dato che uno dei principali sintomi del SARS-CoV-2 (il virus che provoca il Covid19) è la febbre, le tecnologie per monitorare la temperatura corporea e la frequenza cardiaca che oggi appaiono magari normali, un domani potrebbero servire per riuscire a leggere le emozioni delle persone in relazione a determinati stimoli o in determinate situazioni, sulla base di dati come pressione sanguigna, temperatura e battito del cuore. Si potrbebe così valutare la risposta alle situazioni di stress e di tensione di una persona, magari nel corso di un colloquio di lavoro per un futuro dipendente, ma anche negli interrogatori di polizia o per valutare attraverso le telecamere il comportamento di una persona che si venga a trovare nei pressi di "obiettivi sensibili" (caserme di polizia, sedi politiche, palazzi istituzionali, banche, ecc).
Ma senza addentrarci in scenari che se sono senz'altro probabili sono ancora futuribili, già con il solo affacciarsi oggi della possibilità di tracciare i nostri contatti viene modificata tutta una serie di comportamenti con i quali "stare al mondo". Nessuna tecnologia, infatti, è di per sé neutra ma tutte hanno delle conseguenze quando vengono usate. Questo "rilevatore di contatti" sempre acceso nelle nostre tasche potrebbe portarci ancor di più a modificare i nostri comportamenti: distanziandoci dalle altre persone, perfino a una distanza superiore a quella "di sicurezza" per evitare che anche brevi contatti ininfluenti (pensiamo ad un passante incrociato su un marciapiede o all'affiancamento di una vettura in un parcheggio) possano "marcarci" come falsi positivi. Così il distanziamento corporeo si tradurrà fatalmente e propriamente in distanziamento sociale.
Controllare il comportamento delle singole persone, ed abituarle ad autocontrollarsi, per controllare l'intera società. Ecco l'obiettivo dei dispositivi di tracciamento. Ecco l'uso che se ne farà.
È difficile in poco tempo abituarsi alle ordinanze costrittive, al distanziamento corporeo, alle nuove regole di convivenza, alla quarantena domestica, alla perdita di libertà considerate fino a poco prima come intoccabili. Al continuo stato di emergenza o, meglio, allo stato di emergenza imposto di continuo. Eppure è stato fatto! E col tempo ci si abitua a tutto o quasi. È nella natura umana adattarsi. In questi mesi abbiamo potuto vedere come il presidente del governo, Giuseppe Conte, da zero assoluto che era, ha avuto il massimo di gradimento da parte delle persone quando ha iniziato – supportato da una copertura mediatica di primo piano - ad imporre limitazioni alla libertà delle persone. Con decreti draconiani, imponendo zone rosse e la reclusione nei propri domicili, ha dato la sensazione di avere la situazione in mano, quando invece si è visto come è stata gestita l'intera faccenda da parte dello Stato e delle istituzioni: con gli ospedali in allarme per la mancanze di posti letto causati da anni di privatizzazioni nel settore della sanità e con persone lasciate morire da sole nelle case senza essere mai state sottoposte al tampone, oppure morte a cetninaia nelle residenze per anziani dopo il trasferimento dagli ospedali alle RSA dei contagiati dal virus. Per non parlare delle fabbriche rimaste aperte con mirabile cinismo, anche nelle zone rosse, per piaggeria nei confronti di Confindustria.
Qualcuno ha detto che c'è il rischio che le persone ci prendano gusto a farsi comandare. La cosa è persino più banale: a molte persone non interessa tanto la forma con cui il potere governa, se attraverso una democrazia dichiarata o con lo stato d'eccezione. Interessa più che altro che questo potere dia risposte dirette, immediate, percepite come risolutive. In questo, lo stato d'eccezione sembra dare più sicurezze. Che poi queste risposte siano realmente efficaci poco importa, l'importante è che lo sembrino. Mal che vada, ci sarà sempre un gruppo di sedicenti "esperti" a dare l'avvallo alle decisioni prese. Lo svilimento della discussione e del ragionamento politico a favore delle disposizioni avvallate dai cosiddetti competenti, esperti, tecnici o scienziati, è sotto gli occhi di tutti. Quello che è stato messo in luce dall'emergenza coronavirus, infatti, non è tanto il ricorso

allo stato d'emergenza – cosa già vista con la fantomatica lotta al terrorismo internazionale e in Italia con la gestione dei post-terremoti da parte della Protezione Civile – quanto lo spostamento del discorso da un ambito politico ad uno prettamente scientifico. A dettare le linee guida in questa occasione sono stati a livello internazionale l'OMS e a livello italiano, ancora una volta, la Protezione Civile con l'appoggio dei diversi "comitati di esperti". Il ruolo politico vero lo hanno avuto queste istituzioni, a cui il governo, i ministeri e il Presidente del Consiglio hanno solo fornito l'appoggio amministrativo. Ma la risposta della "Scienza" ufficiale di fronte a un'emergenza è sempre tecnologica, come abbiamo visto. Alphabet, Google, Apple, Facebook, Microsoft, Amazon, i colossi cinesi e americani, fino agli sviluppatori di app...in questo contesto saranno sempre più i partner della comunità scientifica, che tra l'altro riceve ingenti finanziamenti, magari sottoforma di "aiuti" filantropici, dalle fondazioni che controllano questi gruppi di potere economico a livello mondiale. L'approccio istituzionale e "scientifico" all'emergenza sanitaria si è concentrato, come al solito, sugli effetti invece che sulle molteplici cause (da quelle più immediate come i tagli alla sanità fino a quelle più profonde come le modifiche che l'insostenibile sistema di sviluppo capitalista arreca all'ecosistema), nella direzione di un maggiore controllo tecnologico e poliziesco, trattando l'essere umano come un "untore" dai comportamenti "irresponsabili" che ha bisogno per correggerli di trovare strumenti al di fuori di sé. Siamo sicuri che anche in futuro, superata l'emergenza sanitaria (se mai ci diranno che è finita e non si inventeranno qualche motivo per protrarla ancora) non ci libereremo tanto facilmente di tecnologie ed applicazioni come "Immuni" e roba simile. Ogni qual volta il governo, la protezione civile o le istituzioni sanitarie decreteranno nuove emergenze queste tecnologie rispunteranno fuori dal cilindro. Nessuno ci dice che non verranno rese fruibili anche per altre ragioni, e magari fortemente richieste come oggi già sono richiesti un conto corrente bancario, una carta di credito, un cellulare o una mail per un numero altissimo di prestazioni basilari per la vita sociale (o, meglio, asociale), dall'ambito della salute pubblica al pagamento del salario per il lavoro svolto o della pensione, fino alle misure di sostegno pubblico come il reddito di cittadinanza che viene versato non in contanti ma su una carta elettronica. Queste tecnologie che oggi tracciano la prossimità fra le persone, inviando un'allerta nel caso si sia stati vicini a qualcuno ritenuto "appestato", oggi funzionano nel caso di positivi al Covid-19, ma domani chissà, la stressa cosa la si potrebbe fare per i sospettati di terrorismo o per gli schedati come sovversivi dalle questure, oppure per gli immigrati clandestini. Un allarme ti potrebbe avvisare che vicino a te c'è un qualche tipo di persona irregolare, magari ricercata dalla polizia. Piano piano la volontarietà lascerà spazio alla mancanza di scelta quando tutte queste applicazioni diverranno "di serie" sui sistemi operativi dei nuovi modelli di smartphone, che tra l'altro saranno sempre più connessi alla tecnologia 5G, che di per sé rende interconnessa una vastità di "cose" che prima non lo erano (non a caso lo chiamano "internet delle cose"). I nostri dati finiranno in mano ai datori di lavoro, ai vicini, alla polizia, al governo, a società private. Ci continueranno a dire che è per il nostro bene, che ci sono "pochi rischi per la privacy" e che dobbiamo rinunciare ad un po' della nostra libertà per il bene, la salute e la sicurezza collettivi. A questo punto nasce una domanda spontanea: a forza di rinunciare poco a poco ad un po' di libertà, non si finisce prima o poi con il perderla tutta? Domanda retorica, dalla risposta scontata. É proprio così, a meno di cominciare da subito a rifiutare il controllo tecnologico sulle nostre vite. Cominciando da un piccolo passo, ma indispensabile: rifiutarsi di installare queste app di tracciamento sul proprio cellulare. Personalmente, non concedere mai in maniera volontaria i dati sui propri spostamenti, sui propri contatti e sulla propria salute a un governo di qualsiasi colore o a delle società private quali che sia il loro nome.

Per finire, una parola occorre spenderla anche nei confronti di quelle utopie che dipingevano il

mondo dell’open source e del software libero come portatore di speranze rivoluzionarie nel campo digitale, sbandierato da sempre come sinonimo di libertà contro la proprietà privata della conoscenza. Qualcosina occorrerà dire sul fatto che molte app di contact tracing nel mondo sono state distribuite proprio attraverso diritti liberi open-source, liberamente replicabili da altri sviluppatori e utilizzabili da altri governi nelle varie nazioni. Proprio attraverso questo modello di software libero si stanno distribuendo i codici sorgenti di molte di queste app di tracciamento. Il più noto è il codice sorgente dell’app sviluppata a Singapore, pubblicato sul web con il nome di progetto *OpenTrace* e che ha fatto da base per le applicazioni sviluppate dagli altri paesi. Anche “Immuni” in Italia è stata distribuita in maniera open source. Quindi una modalità di distribuzione pensata come libera sta contribuendo a diffondere applicazioni che restringono la stessa libertà. Ironico, vero?! Le utopie cyber-punk sono state usate come trampolino da coloro che hanno creato sistemi oppressivi (con MacOSX, basato su un sistema BSD, e Android, basato su Linux, come i due esempi più eclatanti). Che cosa ci dice tutto questo? Che è ora di abbandonare un poco le tecnologie e le realtà digitali per riprendersi le strade e le vite reali.



DÌ DI NO ALLE APP DI CONTACT TRACING!