Stati di tracciamento progressivo

Ma servirà davvero un'app da installare sui nostri *"mobile device"* (si scherza lo sapete) per sbarrare la strada al terribile nemico della nostra salute, il COVID-19? Non siamo certo noi in grado di stabilirlo e non ci passa neanche per l'anticamera del cervello prendere posizione in materia. Se gli esperti ritengono che nel kit delle contromisure ci sia spazio anche per un ausilio digital/elettronico/personale, ben venga. Però, a questo punto, permetteteci di fare il nostro lavoro di studiosi, provare a scoprire, quale sia lo scenario presente nel mondo digitale e analogico, per capire come effettuare al meglio questa scelta. Una sorta di riassunto delle puntate precedenti per non perdere di vista, dentro all'emergenza della pandemia, i nostri diritti, insieme ai doveri (quelli è difficile non averli sotto mano) che ci vengono chiesti, ricordati, e un pochino anche imposti, in questi giorni/settimane/mesi da i nostri amministratori pubblici: locali, regionali e statali. Il concetto su cui ci piacerebbe riflettere assieme a Voi è quello della *"responsabilizzazione"*, un concetto molto caro al sociologo della complessità Piero Dominici, che nel suo ultimo libro: "Dentro la società interconnessa" dice a proposito:

*"...è stata creata quasi una **mitologia dell'individuo autonomo e svincolato da ogni legame**, un individuo che, per le sue azioni, sembra non debba rispondere a niente e nessuno: altro che il riferimento alla ben nota distinzione tra etiche dell'intenzione ed etiche della responsabilità. Siamo andati ben al di là di ogni vincolo giuridico e/o culturale: contano il denaro e il consumo e l'unico (micro)potere dei cittadini sembra essersi ridotto ad essere consumatori. Tali dimensioni, insieme al vuoto di significato lasciato dalla crisi delle ideologie, hanno prodotto, tra le conseguenze, anche una sorta di **disarmo morale**, che nutre **la società dell'irresponsabilità** priva di qualsiasi etica del sacrificio".*

Responsabilizzare, esattamente l'opposto di quello fa/farebbe una app. Che attraverso la tecnologia controlla tutti in modo sistematico (anche se su base volontaria) - e su questo concetto come Vedrete ci sarà da sbizzarrirsi - deresponsabilizzando ciascuno e trasformandoci tutti in *"involontari"* delatori o più *"semplicemente"* consumatori o ancora meglio *"produttori/consumatori"*. Perdonate la chiosa drammatica, e torniamo alla disamina tecnica del percorso che ci ha portato alla scelta di includere un app fra gli ausili medico/sanitari da utilizzare contro il virus.

Una ricerca di LSDI, Libertà di Stampa e Diritto all'Informazione.

Una delle possibili soluzioni per gestire la cosiddetta *"fase due"* evitando di far riesplodere i contagi del COVID-19 sembra essere basata sulla tecnologia. Per meglio orientarsi in uno scenario molto caldo e fluido, vi proponiamo la cronologia dei documenti formali emessi dagli attori che, a vario titolo, sono coinvolti in un ambito che si appresta a modificare integralmente le nostre vite. Ovviamente il contesto è quanto mai in divenire e quindi ci scusiamo anticipatamente se al momento della nostra pubblicazione, alcune delle notizie qui contenute hanno subito ulteriori aggiornamenti e progressi. Come si dice, è un work in progress a cui ci uniamo con deferenza e rispetto. (si scherza). Il documento primo da cui iniziare la nostra disamina, è quello pubblico emanato all'inizio del mese in corso dall'Unione Europea.

8 Aprile 2020
EUROPEAN COMMISSION RECOMMENDATION on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data

EUROPEAN
COMMISSION

Brussels, 8.4.2020
C(2020) 2296 final

COMMISSION RECOMMENDATION

of 8.4.2020

on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data

La Commissione Europea emette per gli Stati membri un documento di "raccomandazioni" per la realizzazione di strumenti tecnologici di contrasto alla diffusione del virus, con particolare attenzione alle applicazioni mobili e all'uso di dati. L'intento è quello di definire un approccio comunitario al problema e di utilizzare uno schema unico per l'utilizzo dei dati. Questi gli obiettivi dichiarati: progettare un modello

predittivo della malattia; monitorare gli effetti delle decisioni dei Governi degli Stati Membri e sostenere una strategia coordinata.

Per gli strumenti che gli Stati utilizzeranno la Commissione:

1. raccomanda il rispetto dei diritti fondamentali e la prevenzione dello stigma sociale, con particolare riferimento alle norme applicabili in materia di protezione dei dati personali e riservatezza delle comunicazioni;
2. esprime preferenza per le misure meno intrusive, che utilizzino dati di prossimità e anonimi e che evitino l'uso dei dati di posizione o di movimento delle persone;
3. richiede la definizione di requisiti tecnici relativi alle tecnologie più appropriate (ad esempio "Bluetooth Low Energy") per stabilire la prossimità tra dispositivi, implementare tecniche di crittografia, garantire la sicurezza e la memorizzazione su dispositivo mobile dei dati, permettere l'eventuale accesso ai dati da parte delle autorità sanitarie e memorizzare i dati;
4. richiede la definizione di efficaci requisiti di sicurezza informatica per salvaguardare la disponibilità, l'integrità, l'autenticità e la riservatezza dei dati;
5. richiede che, quando la pandemia sarà stata dichiarata sotto controllo, ogni misura oggetto della raccomandazione dovrà essere fermata e tutti i dati personali collezionati nell'implementazione di queste misure dovranno essere cancellati;
6. richiede che, per mezzo di questo strumento tecnologico, nel caso di infezione confermata, venga eseguito l'aggiornamento dei dati di prossimità degli utenti e vengano usati metodi appropriati per avvertire le persone entrate in contatto con gli infetti garantendo l'anonimato; e
7. richiede requisiti di trasparenza sulle impostazioni della privacy per garantire la fiducia nelle applicazioni.

Le scadenze fissate dalla Commissione Europea sono:

1. **15 Aprile 2020** - gli Stati Membri devono sviluppare un pan-European approach for COVID-19 mobile applications (mandatory)
2. **31 Maggio 2020** - gli Stati Membri dovrebbero riportare le azioni prese per seguire le raccomandazioni di questo documento (should)
3. **Giugno 2020** - la Commissione deve fare un assessment dei progressi fatti riguardo l'implementazione di queste raccomandazioni

10 Aprile 2020
Apple and Google partner on COVID-19 contact tracing technology

Apple a Google, dai rispettivi "house organ", hanno trasmesso un comunicato a dir poco "storico", un documento che sancisce una sorta di Santa Alleanza fra i due colossi hi-tech contro il virus, qualcosa di inaudito e impossibile da prevedere anche solo pochi giorni prima, e che rimarrà negli annali. Ne riportiamo due passi essenziali:

"Gli sviluppatori stanno creando strumenti tecnici per aiutare a combattere il virus e salvare vite umane. In questo spirito di collaborazione, Google e Apple annunciano lo sforzo congiunto per consentire l'uso della tecnologia Bluetooth per aiutare i governi e le agenzie sanitarie a ridurre la diffusione del virus, con la privacy e la sicurezza degli utenti al centro della progettazione.

Poiché il COVID-19 può essere trasmesso grazie alla prossimità tra soggetti infetti, le autorità sanitarie hanno definito il tracciamento dei contatti uno strumento prezioso per contribuire a contenerne la diffusione. Numerose autorità sanitarie pubbliche, università e ONG in tutto il mondo hanno svolto un lavoro importante per sviluppare tecnologie di tracciamento dei contatti di tipo opt-in. Per favorire questa causa, Apple e Google lanceranno una soluzione completa che include le API e agisca a livello di sistema operativo per aiutare il tracciamento dei contatti."

Oltre al comunicato i due colossi hanno poi diffuso tre documenti:

1. **Contact Tracing Bluetooth Specification**

Tale documento - si legge in Overview - definisce un protocollo per il Contact Tracing basato su Bluetooth e in grado di preservare la privacy. Un protocollo che, dichiarano Apple e Google, consente di combattere la diffusione del COVID-19 avvisando della possibile esposizione a persone alle quali è stato diagnosticato

il virus. Questo servizio "poggia" sul Bluetooth Low Energy utilizzato per il rilevamento di prossimità dei telefonini e per lo scambio dati.

Sulla questione della Privacy, viene specificato che:

- il rilevamento della prossimità non fa uso di dati di geolocalizzazione (quelli del GPS dei dispositivi, per intendersi)
- il rischio per la privacy viene mitigato dall'utilizzo di un meccanismo protetto (con una "chiave giornaliera di tracciamento") di rotazione/modifica ciclica del cosiddetto "identificatore di prossimità";
- gli identificatori di prossimità vengono elaborati soltanto sui dispositivi (telefonini) interessati
- gli utenti scelgono se contribuire al contact tracing oppure no;
- in caso di diagnosi di COVID-19, gli utenti condividono la "chiave di diagnosi" su un server;
- gli utenti hanno garantita la trasparenza

2. **Contact Tracing Cryptography Specification**

In questo secondo documento, invece, sono dati i dettagli di come vengono programmate le chiavi crittografiche utilizzate dal protocollo. Anche qui sono fatte delle puntualizzazioni sulla privacy. Ne segnaliamo un paio:

- chi gestisce il server utilizzato per il funzionamento di questo protocollo non è in grado di apprendere gli utenti che sono stati in prossimità tra loro
- il server non deve mantenere i metadati degli utenti che hanno notificato il loro stato di positività al COVID-19 (condivisione della "chiave di diagnosi", passaggio spiegato nel primo documento)

3. **Contact Tracing Framework Documentation (API)**

In quest'ultimo documento viene definito il "ContactTracing Framework" con il dichiarato intento di aiutare gli sviluppatori a realizzare il protocollo per garantirne l'interoperabilità. Nel documento sono descritti due ruoli:

- Affected User: un utente che dichiara il suo stato di diagnosi positiva al COVID-19
- Exposed User: un utente che dichiara di essere potenzialmente esposto ad un utente positivo

Il contact tracing, per cui questo documento definisce il flusso e le funzioni in gioco, è l'insieme delle interazioni tra queste due tipologie di utenza: la "chiave di tracciamento giornaliero" di un utente positivo viene condivisa ed elaborata perché per ciascun altro utente si possa stabilire l'esposizione.

Questa la Roadmap di Apple e Google:

4. **Maggio 2020**: Apple e Google rilasceranno le API per garantire l'interoperabilità tra i dispositivi Android e quelli iOS che usino applicazioni delle autorità sanitarie. Queste applicazioni saranno disponibili nei rispettivi store
5. **Mesi successivi**: Apple e Google lavoreranno per implementare la capability di contact tracing direttamente su piattaforma, cioè a livello HW dei telefonini con una soluzione sicuramente più robusta

NOTA: già il giorno 9 Aprile Techcrunch riferiva di esperimenti in corso al MIT su sistemi di tracciamento ispirati alla funzione "Find My" utilizzata proprio da Apple per la ricerca di dispositivi Mac e iOS smarriti.

15 Aprile 2020
Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States

eHealth Network

Mobile applications to support contact tracing in the EU's fight against COVID-19

Common EU Toolbox for Member States

Si tratta del primo passo del lavoro promosso dalla Commissione Europea sette giorni prima, l'8 di Aprile.

Oltre a riportare lo stato di avanzamento delle iniziative del consorzio PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) e dei singoli Stati membri, il documento è una guida pratica che definisce i capisaldi che qualsiasi applicazione selezionata deve avere. Si tratta in effetti di una declinazione delle raccomandazioni emesse l'8 Aprile. Questi i quattro punti evidenziati nell'Executive Summary:

- deve essere utilizzata su base volontaria
- deve essere approvata dalle autorità sanitarie nazionale
- deve preservare la privacy dei cittadini
- deve essere disattivata quando diventa non più necessaria

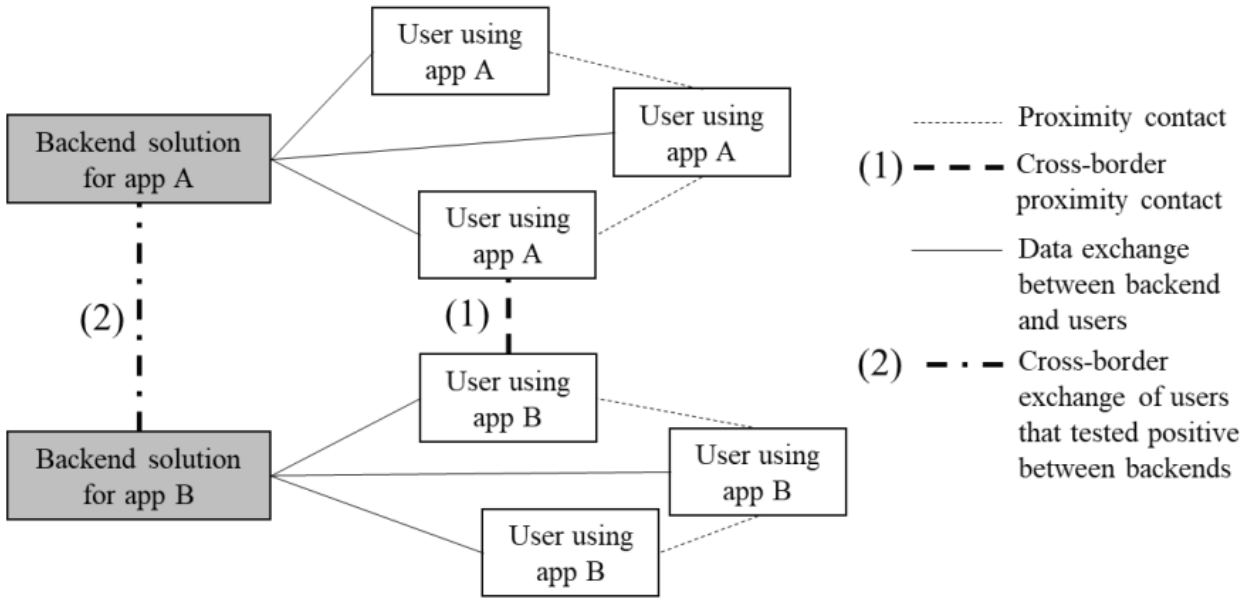
Il valore aggiunto di queste app - continuiamo a leggere dall'Executive Summary - è che possono registrare contatti che una persona non può notare o ricordare. I requisiti stabiliti nel documento riguardano i criteri di registrazione dei contatti e di informazione alle persone; si basano su linee guida epidemiologiche condivise e riflettono le migliori pratiche in materia di sicurezza informatica e accessibilità.
Questa guida ha l'obiettivo di:

- prevenire la comparsa di applicazioni non approvate e potenzialmente dannose
- stabilire criteri di successo e di monitoraggio dell'efficacia delle applicazioni
- definire una strategia di comunicazione per interagire con le parti interessate

Il lavoro - si legge in conclusione dell'Executive Summary - è solo un primo passo e proseguirà come stabilito nelle raccomandazioni emesse l'8 Aprile.
Detto che i principi sono espressi già nelle raccomandazioni dell'8 Aprile, questo documento - che riporta fissa in modo più netto alcuni paletti dettando quindi i requisiti tecnici degli strumenti che gli Stati membri dovranno adottare:

1. Interoperabilità transfrontaliera

Si tratta della traduzione di cross-border interoperability. Con l'ovvia premessa che "la catena di trasmissione delle infezioni non si ferma ai confini nazionali o regionali", le linee guida hanno l'obiettivo di garantire alle autorità sanitarie degli stati membri di scambiarsi le informazioni sulle persone infette. Le applicazioni dovranno favorire questo scambio seguendo un protocollo comune in modo che esso avvenga senza problemi, salvaguardando la privacy e la protezione dei dati, indipendentemente da dove i dispositivi sono dislocati su territorio europeo.



2. Privacy

Le soluzioni che dovranno essere messe in campo possono essere divise in due macro categorie: (a) decentralizzate e (b) soluzioni basate sull'uso di server. Le soluzioni decentralizzate lasciano sui telefonini i dati di prossimità dei contatti avuti generati dalle app. Alla seconda categoria, invece, appartengono le app che fanno uso di un server tenuto dalle autorità sanitarie degli stati membri. Nessuna delle due opzioni, viene specificato, prevede l'immagazzinamento di informazioni personali non necessarie.

3. Crittografia

Le comunicazioni tra dispositivi mobili e server e dovranno essere criptati secondo degli standard esistenti e testati.

4. App temporanea/Cancellazione dei dati

Le applicazioni dovranno essere disattivate e tutti i dati personali di prossimità dovranno essere cancellati, non appena la crisi sarà finita

5. Volontarietà

Le applicazioni dovranno avere un meccanismo di richiesta di consenso informato su tutti i dati utilizzati dalle applicazioni stesse.
App should be consent-based with full information of intended processing of data

6. No allo stigma

Bisognerà assicurare che nessun utente verrà a conoscenza dell'identità delle persone infette o di contatti di persone infette.

7. Open Source e Trasparenza

Agli sviluppatori, cioè alle case produttrici delle applicazioni, viene richiesto di rilasciare in modo aperto sia le specifiche tecniche sia i codici sorgenti delle app, per massimizzare il riuso, garantire interoperabilità e sicurezza e facilitare i processi di verifica.
Le autorità nazionali dovranno garantire che l'architettura e il codice delle applicazioni e del backend server siano resi disponibili per la revisione da parte di esperti indipendenti.

8. Dispositivi

La funzione di contact tracing dovrà essere supportata da tutti i dispositivi che hanno il Bluetooth e dovrà essere disponibile in tutti i possibili sistemi operativi con la precauzione di non consumare eccessivamente energia.

9. Accessibilità e inclusività

L'inclusività è un principio fondamentale non soltanto da un punto di vista dei diritti ma anche da un punto di vista di efficacia del sistema. La questione riguarda gli individui, come bambini e anziani, che non hanno smartphone o dispositivi connessi o non sono sufficientemente esperti per installare ed utilizzare appropriatamente delle applicazioni. Riguarda anche il personale sanitario che non ha sempre con sé il dispositivo mobile durante il lavoro. Il punto, quindi, è che non tutti i cittadini potranno avere l'applicazione mobile; da Singapore si hanno però evidenze che l'efficacia di un sistema di tracciamento dei contatti basato su app si raggiunge se il 60-75% della popolazione utilizza in modo attivo l'applicazione stessa. Un altro aspetto evidenziato nel documento è che non tutti i dispositivi hanno la capacità Bluetooth.
Per questi casi potrebbero essere necessari dei dispositivi ad hoc.

10. Ruolo delle autorità sanitarie

In diversi punti del documento viene richiamato il ruolo attivo che devono avere le autorità sanitarie degli Stati membri:

a. le autorità sanitarie saranno responsabili dell'emissione di un codice per i pazienti risultati infetti. Tali codici dovranno avere delle caratteristiche di pseudo-randomicità e dovranno essere facilmente gestite dagli utenti (per esempio QR code)

b. quando una persona risulta positiva, l'autorità sanitaria dovrà sbloccare la notifica per mezzo dell'applicazione e dovrà gestire i differenti livelli di rischio connessi all'intensità e alla prossimità dei contatti avuti dal soggetto

c. in alcuni casi le autorità sanitarie hanno comunque un protocollo che impone loro di telefonare ai contatti più che basarsi esclusivamente su una notifica automatica. In questi casi sarà richiesto agli utenti di fornire i numeri telefonici delle persone con cui sono venute in contatto
d. potrebbe essere richiesto alle autorità sanitarie di farsi garanti della processazione dei dati personali dei pazienti

11. Azioni di supporto

Queste alcune delle azioni che gli Stati Membri dovranno intraprendere:
a. scambio di dati epidemiologici tra Stati
b. prevenire la proliferazione di applicazioni dannose
c. monitoraggio dei benefici dell'app attraverso la definizione di KPI (Key Performance Indicator)

17 Aprile

ORDINANZA n. 10/2020 del commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica COVID-19

Presidenza del Consiglio dei Ministri

COMMISSARIO STRAORDINARIO PER L'ATTUAZIONE E IL COORDINAMENTO DELLE MISURE DI CONTENIMENTO E CONTRASTO DELL'EMERGENZA EPIDEMIOLOGICA COVID-19

ORDINANZA n. 10/2020

IL COMMISSARIO STRAORDINARIO
PER L'ATTUAZIONE E IL COORDINAMENTO DELLE MISURE DI CONTENIMENTO
E CONTRASTO DELL'EMERGENZA EPIDEMIOLOGICA COVID-19

Questo è l'ultimo documento di cui diamo conto, si tratta dell'ordinanza che dispone la stipula del "contratto di concessione gratuita della licenza d'uso sul software di contact tracing e di appalto di servizio gratuito con la società Bending Spoons S.p.a."

Bending Spoons, si legge dall'ordinanza, è la società che ha proposto la soluzione di contact tracing "Immuni", ritenuta 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."

L'ordinanza prende in considerazione 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.

***

Fin qui i documenti che delineano uno scenario complesso e con più fronti aperti; uno scenario che impone un'ampia riflessione. Un primo tema è quello dell'utilizzo dei sistemi automatici di decisione, in inglese "Automated Decision-Making Systems (ADMS)". Algorithm Watch ha prodotto un "endecalogo": un insieme di principi e considerazioni - così si legge nella nota introduttiva - per una discussione informata, democratica e utile sulle ADMS ai tempi della pandemia.

Questi sono i punti di indagine che prendiamo dalle raccomandazioni di Algorithm Watch per fare le nostre riflessioni (abbiamo chiamato in causa anche qualche amico di LSDI e li ringraziamo):

1. **Tecnologia** - Il COVID-19 non è un problema tecnologico
2. **Benefici effettivi delle soluzioni adottate** - prima di considerare le implicazioni sulla protezione dei dati delle applicazioni digitali per il contact tracing dovremmo chiederci se tali applicazioni servono oppure no. Il sacrificio dei diritti dovrebbe essere richiesto se ci sono dei reali benefici
3. **Privacy** - le protazione dal COVID-19 e la protezione della privacy non sono cose che si escludono a vicenda
4. **Trasparenza** - Solo la trasparenza può permettere alla società civile e ai parlamentari di chiedere poi conto ai Governi
5. **Stato di emergenza** - Lo stato di emergenza non deve giustificare l'adozione di soluzioni ADMS che hanno evidenziato delle problematicità, come il riconoscimento facciale
6. **Risposte globali** - Una pandemia è globale per definizione. È necessario che vi sia una serie di risposte globali, diverse e coordinate ad esso
7. **Necessità del dibattito** - Bisogna assicurarsi che ogni dibattito su questa materia non cada nel vuoto.

Percorriamo quindi questi sette punti.

1. **Tecnologia**

Che non si tratti di una soluzione meramente tecnologica è fatto ben descritto nelle raccomandazioni e nelle linee guida dettate dalla Commissione Europea. Le autorità sanitarie degli Stati membri, infatti, hanno un ruolo centrale.
Se pensiamo al caso italiano, quindi, bisogna - nella migliore delle ipotesi - sospendere il giudizio per capire se e quanto il nostro sistema sanitario sarà in grado di essere parte attiva di un meccanismo che individua nell'applicazione solo una delle sue parti.
Non si può però evitare di osservare quanto la soluzione tecnologica - benché non autosufficiente - sia una delega ai singoli cittadini ed uno scarico sui cittadini del peso di una situazione oggettivamente insostenibile.

Disobbedienze

***Nicola Zamperini**, giornalista e scrittore, così si è espresso sul primo punto dell'endecalogo di Algorithm Watch: dire che l'epidemia non è un problema tecnologico è una semplificazione colossale. In una società iper connessa, ahimè, ogni problema è anche un problema tecnologico. Qualunque presa di posizione che parta dalla pretesa di una rimozione della tecnologia dal campo di applicazione della clinica e dell'epidemiologia è ridicola. In che modo, senza tecnologia, sarebbe possibile arrivare a determinare se una persona è morta di Covid19, pressoché in tempo reale? Non dopo un'autopsia, voglio dire.*

Ciò di cui discutiamo oggi non dovrebbe essere soltanto della privacy dei cittadini, ricordiamoci sempre dei buoi fuori della stalla, ma di un utilizzo da parte delle istituzioni dei dati dei cittadini con fini di sanità pubblica. Avete minimamente idea della scarsa (scarsissima) capacità di correlazione dei tanti dati che possiedono le amministrazioni pubbliche e della - invece - facilità con cui Google, per dirne una, può aggregare e correlare tutto quello che sa di noi? Le pubbliche amministrazioni italiane non sono Penelope Garcia di Criminal Minds.

I dati aggregati di miliardi di persone dovrebbero essere un bene comune; eppure li possiedono per lo più meta-nazioni digitali dalle quali nessuno è andato per reclamarli e pretenderne l'utilizzo con fini di sanità pubblica. Nessuno è andato da loro esercitando un potere legittimo, esercitando quel monopolio dell'esercizio della forza che sta in capo agli Stati in uno stato d'eccezione come quello che stiamo vivendo e che - in quanto stato d'eccezione - ha tenuto a casa milioni (miliardi nel mondo) di persone.
Tanto suona assurda questa pretesa, anche in chi la formula, che è sembrato naturale che ciò non sia accaduto. E che quindi il governo italiano e così altri governi abbiano dovuto sviluppare da soli un software che raccoglie e correla dati, quando sarebbe stato più facile obbligare Google e Facebook a fornire quei dati in maniera imperativa.

Ricordiamo poi che per il singolo i dati rappresentano esattamente l'individuo, la persona, il singolo essere umano. Essi sono l'individuo, costituiscono una parte di noi che concorre a definire chi siamo. I dati non sono di nostra proprietà, i dati siamo noi, i dati sono noi. Dovremmo rammentarcene. E ricordarlo ai promotori

dei dibattiti sulla privacy, e a chi evoca un presunto protagonismo della società civile (!) chiamata a controllare ciò che i decisori pubblici fanno dei nostri dati.

Per continuare a seguire gli aspetti tecnologici e le varie implicazioni consigliamo di seguire **Matteo G.P. Flora**, che già qualche giorno fa ha fatto delle interessanti puntualizzazioni, e la newsletter di **Carola Frediani**, Guerre di Rete.

2. Benefici effettivi delle soluzioni adottate

Al netto della non secondaria questione della "delega alla cittadinanza" e assodato che la soluzione non è puramente tecnologica, se la commissione europea chiede agli stati di definire dei KPI, bisogna pensare che dovremo aspettare del tempo prima di capire se le soluzioni tecnologiche messe in campo avranno avuto successo.

Se il dato di Singapore è vero, e cioè se soluzioni di questo tipo sono efficaci se almeno il 60-75% della popolazione le utilizza,dovremmo aspettarci che 40 milioni di italiani installino l'app oppure - a garanzia di accessibilità e inclusività - si dotino di dispositivi Bluetooh che supportino "Immuni". In questo secondo caso, chi dovrebbe garantire i dispositivi per le categorie potenzialmente escluse (bambini, anziani, personale sanitario)?

Oltretutto che senso avrebbe attivare questa applicazione, se poi i sistemi sanitari non riuscissero a completare il servizio (si pensi alla semplice capacità di diagnosi)?

***Maurizio Codogno**, di Wikimedia Italia, che abbiamo coinvolto su questo tema, ci dice: "Una funzionalità su base volontaria funziona allo stesso modo di una vaccinazione. In quest'ultimo caso occorre raggiungere l'immunità di gregge: una percentuale piuttosto alta della popolazione, che dipende dalla contagiosità della malattia ma che varia tra l'80 e il 95%. Nel caso dell'app avremmo qualcosa di simile: una certa percentuale di persone deve usarla per avere un tracciamento globale. Le stime che leggo variano dal 60 al 75%, probabilmente tenendo conto del fattore R_0 più basso che per altre malattie; ma ho dei dubbi sulla validità di questa banale trasposizione, che non tiene conto della diversa logica dei due sistemi. Chi usa l'app non è infatti immunizzato, ma solo controllato; quindi può contagiare ed essere contagiato. Bene: chi ci assicura che l'app parta in pompa magna, si vede che i risultati sono deludenti, si dà la colpa alla bassa percentuale d'uso e la si renda obbligatoria? E una volta che l'app è obbligatoria, chi ci assicura che nessuno penserà di usarla per altri tipi di controllo?"*

3. Privacy

In questo spazio abbiamo più volte posto l'accento sul fatto che, nello scenario della cosiddetta, ma mai avvenuta, rivoluzione digitale, il problema non è tanto la privacy, quanto quello dell'utilizzo che viene fatto dei dati condivisi. Una ambiguità che la stessa commissione europea ha generato parlando, nell'ormai famoso regolamento GDPR, indistintamente di dati e informazioni personali. A questo aspetto se ne aggiunge un altro: siamo davvero sicuri che chi svilupperà le applicazioni, garantirà la "compliance" ai requisiti dettati dalla Commissione Europea in materia di privacy? Di qui nasce l'esigenza della trasparenza delle architetture e dei codici sorgenti delle applicazioni stesse. Per quanto riguarda "Immuni", finché non ne avremo conosciuto le specifiche, non saremo in grado di trarre alcuna conclusione.

Sulla questione della Privacy, Maurizio Codogno, esprime dei dubbi: "La prima cosa che viene in mente leggendo la proposta è naturalmente chiedersi se la privacy è davvero rispettata. Io non ho le competenze necessarie per dare una risposta definitiva. Comprendo la logica alla base di scegliere Bluetooth e non GPS come modo per ottenere i dati di vicinanza: in questo modo, anche se qualcuno riuscisse ad accedere ai nostri dati, non potrebbe scoprire dove siamo stati ma solo quanti sono stati i nostri contatti; non quali sono, perché il server non conosce i nostri dati visto che è il nostro telefono a collegarsi per sapere se siamo stati in contatto con un contagiato, e uno dei principi fondamentali della sicurezza è "meno sai, meno danni può fare un baco di sicurezza". È anche positivo il fatto che Apple e Google abbiano rese pubbliche le specifiche tecniche della loro soluzione: sicuramente saranno scrutinate con molta attenzione dagli esperti di privacy e di crittografia."

4. **Trasparenza**

Come si può/potrà chiedere conto alle autorità pubbliche competenti se non si conoscono i requisiti delle applicazioni e il relativo codice sorgente? A parte il procedimento che ha portato alla selezione di "Immuni", partito da una "fast call for contribution", raccogliamo in toto l'osservazione di **Luca Corsato**:

"Che la società Bending Spoons mantenga la proprietà intellettuale mi pare giusto, perché in sostanza si dirà sempre che l'hanno fatta loro. La titolarità è un po' più delicata, perché potrebbe limitare le possibilità di modifica dei codici sorgenti. Soprattutto la pubblicazione del codice.
Si dirà che il codice non può essere pubblicato perché degli hacker potrebbero violare la app e rubare tutti i dati. Questo non sarebbe un rischio nel codice ma nei server in cui verrà installata la app e i criteri di trasmissione e condivisione dati. Se il sito stesso del Governo non usa connessioni criptate in https, non so se queste protezioni verranno naturali applicarle per la app di contact tracing.
La pubblicazione del codice è invece utile proprio per segnalare eventuali bug o migliorie e tranquillizzare i cittadini nell'uso. Più un codice è usato e analizzato meglio è. Però se Bending Spoons, con il proprio business model, valutasse come un danno la pubblicazione del codice, stando a quanto scritto nell'ordinanza si può opporre. E tutti gli elementi di trasparenza sarebbero persi."

Dobbiamo pensare che Apple e Google sono riuscite a fare meglio e che in nome della trasparenza che hanno offerto pubblicando le loro specifiche potranno vantare crediti nell'opinione pubblica? Bisogna cioè lasciare che a queste compagnie private, proprio perché sembrano "saper far meglio", sia delegata anche l'implementazione di soluzioni di gestione di salute pubblica? E' un po' questo il senso da ricercare in un'altra interessante considerazione di **Luca Corsato**:

"Gli amministratori dovrebbero cominciare a chiedersi quanto è giunto a destinazione il ciclo di obsolescenza della democrazia rappresentativa. Un voto oggi vale meno di un'azione Google o Apple: le due

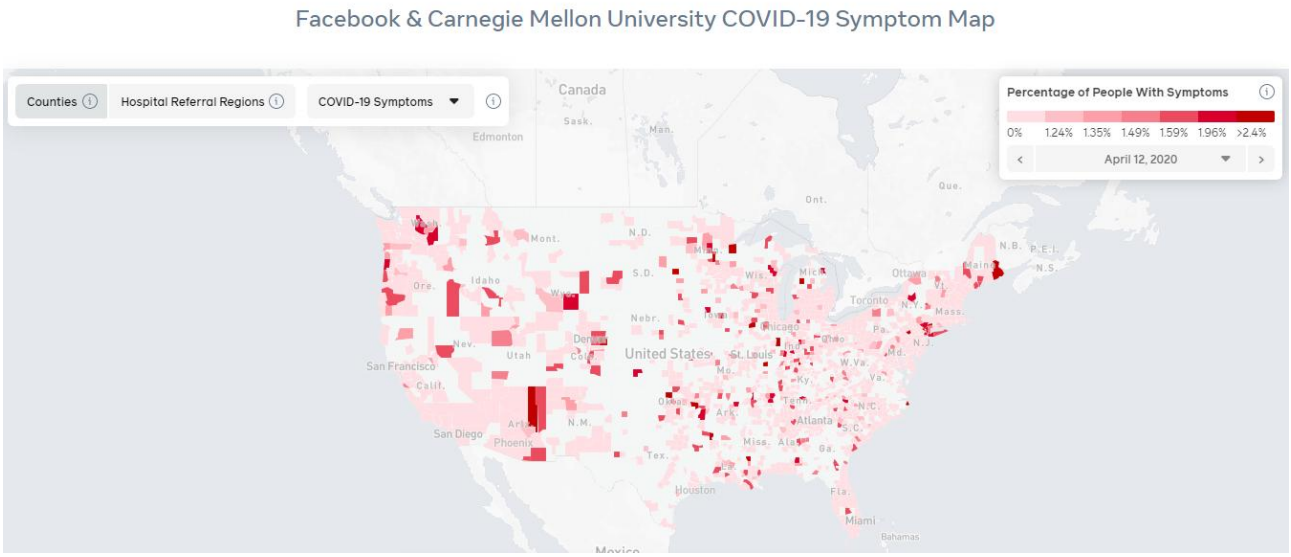
megacorp possono garantire il ritorno alla circolazione, servizi e redditività, mentre i governi subiscono il tracollo dei sistemi sanitari e delle catene di comando.
Si dirà però che è lo Stato Imprenditore a formare i cittadini e le loro competenze che poi alimentano i cicli produttivi delle megacorp. Che solo lo Stato imprenditore finanzia la ricerca pura e può essere un investitore paziente. In alcuni casi lo è ancora. Ma se i suoi rappresentanti non nutrono di alcuna fiducia da parte degli stessi elettori, quando manca affinché ci si senta più rappresentati e tutelati da Jeff Bezos, rispetto a Giuseppe Conte?
Forse ci siamo già arrivati. Alla democrazia dell'azionariato."

Uno scenario che si complicherebbe con l'entrata in campo di altre megacorp. Facebook non si è fatta attendere e, per voce di Mark Zuckerberg, ha annunciato di aver rilasciato una mappa che rileva chi ha i sintomi di Covid19.

Facebook – si legge su NBC News - ha pubblicato le sue prime mappe contea per contea degli Stati Uniti che mostrano i sintomi COVID-19 "auto-riportati". Le mappe, che verranno aggiornate quotidianamente, hanno lo scopo di aiutare i funzionari sanitari a allocare le risorse e decidere dove riaprire.

L'immagine in basso è uno schreenshot della mappa al momento della pubblicazione di questo approfondimento. Queste le avvertenze pubblicate:

La mappa mostra una percentuale stimata di persone con sintomi non confermati COVID-19.
Facebook utilizza dati pubblici aggregati da un sondaggio condotto dal Centro di ricerca Delphi della Carnegie Mellon University.
Facebook non riceve, raccoglie o archivia le risposte individuali.
Questa mappa non è intesa per scopi diagnostici o terapeutici o come guida di viaggio.



Ma è davvero questo lo scenario che vogliamo?

Ancora Maurizio Codogno sul problema che definisce di oligopolio. "Un problema – quello dei produttori di software per telefonini – che, dice, si sta rafforzando sempre più. Al momento c'è già qualcuno che sa perfettamente cosa facciamo e dove ci muoviamo, e sono gli operatori di telefonia mobile. È vero che i loro dati sono tipicamente meno precisi: come scrissi in occasione della grande mossa del governatore lombardo Fontana che chiese i dati aggregati per scoprire come i milanesi si stavano muovendo troppo, a me non serve neppure uscire di casa per passare da una cella a un'altra. Ma quello che probabilmente conta di più è che giustamente questi dati hanno dei vincoli d'uso molto stretti, e quindi non possono essere usati all'atto pratico. (Immagino anche ci sia poca inventiva da parte delle Telco per trovare degli usi interessanti ma rispettosi della privacy; non che io abbia tutta questa inventiva, intendiamoci, altrimenti avrei già proposto dei servizi). Una delle cose peggiori dei dati anonimizzati è però che possono diventare ben poco anonimi se incrociati con altri dati. Per esempio, se qualcuno sapesse più o meno dove abito e in che azienda lavoro potrebbe scoprire qual è il telefono che posseggo, guardando semplicemente gli spostamenti di tutti e filtrando i dati. Google e Apple al momento hanno dati più precisi ma meno facili da incrociare con altri dati pubblici; un insieme di coppie di vicinanza potrebbe essere incrociato in molti casi con la geolocalizzazione telefonica storica per recuperare i numeri corrispondenti alle connessioni anonime. Per evitare una cosa del genere, come minimo il server centralizzato dovrebbe essere gestito da una terza parte, e così d'acchito non saprei dire se è meglio che questa terza parte sia governativa – meglio, paneuropea – o privata.
Sicuramente lo European Data Protection Board si sta preoccupando dei temi della privacy, ma non so fino a che punto."

Noi osserviamo che la soluzione Apple e Google è comunque in campo. Si tratta di capire quanto questa rispetti le raccomandazioni e i requisiti tecnici dettati dalla Commissione Europea. Una interessante analisi viene proposta da dday.it:
"Il sistema PEPP-PT inizialmente era stato pensato per funzionare in entrambi i modi (come riportato sia in modo decentralizzato, sia basato su server. Nota LSDI), mentre oggi si cerca di andare verso un approccio centralizzato. Il sistema di Apple e Google invece nasce per essere usato solo in modo decentralizzato, perché si ritiene che quest'ultimo sia più privacy oriented.
Pure il parlamento Europeo, in una risoluzione, ha spinto per una soluzione decentralizzata, ed è bene ricordare che il PEPP-PT non ha nulla a che fare con l'Europa, è solo un consorzio.
Siamo quindi ad una situazione di stallo: da una parte Apple e Google (ma non solo, vedremo poi) e dall'altra il PEPP-PT, lo stesso che l'Italia ha scelto per la sua app."

Su questo aspetto specifico la domanda è: ma "Immuni" a quale delle due categorie appartiene? E' una soluzione decentralizzata oppure no?

"Il problema - continuano su Dday - è che tutte le applicazioni di contact tracing che non useranno il sistema di Apple e Google vanno incontro ad una serie di problematiche di implementazione: l'integrazione di una

applicazione che usa perennemente il bluetooth LE e codifica i dati deve essere integrata al meglio con i sistemi operativi. Dalla gestione delle app in background, al modo in cui viene gestito il bluetooth LE, un'applicazione sviluppata con le librerie di Apple e Google risulta sicuramente più efficiente anche sotto il profilo del risparmio energetico, soprattutto in una seconda fase dove le api saranno integrate direttamente in iOS e Android."

La questione comunque non è puramente tecnologica. La partita della soluzione è anche di carattere politico: molto banalmente: un conto è decentrare, un altro conto è accentrare.

Questo il punto di vista di Maurizio Codogno su - la definizione è sua - "l'italica app, scelta dopo regolare bando di concorso. In Italia siamo sempre pronti ad avere soluzioni autarchiche, dalla PEC a SPID, che di per sé funzionicchiano anche ma non sono assolutamente interoperabili, oltre ad essere rigorosamente gestite da privati o pseudoprivati. In questo caso, a oggi sappiamo ben poco di Immuni, se non che è stata fatta da una software house milanese in collaborazione con una nota catena lombarda di poliambulatori privati (che pure il mese scorso pare lavorassero a un'app di tipo ben diverso e da una società di marketing che evidentemente avrà collaborato per rendere la proposta più appetibile. Sicuramente l'ordinanza – che chissà come mai non sono riuscito ad aprire dal sito del Corriere che pure indicava il link da cliccare – non dice assolutamente nulla di tecnico, né contiene allegati tecnici sulla soluzione. Per quanto io possa parlare male di Apple e Google, la security by oscurity mi pare ancora più preoccupante: al governo e al commissario straordinario evidentemente no, o forse magari hanno avuto tutte le spiegazioni del caso con un obbligo di non divulgazione."

Prima di passare al punto successivo ci sembra interessante riportare la questione posta da **Mario Tedeschini-Lalli**:
"Nella discussione sulle app di tracciamento - si legge su un post Facebook - mi sembra sia rimasto non indicato un problema potenziale: l'uso per indagini penali - anche se si trattasse di un sistema meno centralizzato. I dati accumulati localmente della app potranno essere utilizzati ai fini dell'indagine oppure no? O anche per altre indagini? E i dati di quelli con cui sono entrato in contatto?"

5. Stato di emergenza

Qui bisogna fidarsi. Certamente del fatto che, una volta passata l'emergenza, l'applicazione verrà disattivata. Bisogna, invece, almeno vigilare su quanto formalmente (cioè per Decreto), questo stato di emergenza sarà tenuto in vita anche quando non ve ne saranno più le ragioni. Ma avremo mai a disposizione tutti gli strumenti necessari per poterlo valutare?

6. Risposte Globali

Anche qui il ragionamento è al netto della non secondaria questione della "delega alla cittadinanza". E' apprezzabile lo sforzo che si sta facendo nella direzione della interoperabilità fra gli Stati membri. D'altra parte questi sforzi risultano vani se non sostenuti dalla trasparenza dei processi.

7. Necessità del dibattito

In questo mese e mezzo sono emerse tante lacune strutturali e culturali del nostro Paese. Quello dell'applicazione per il tracciamento dei contatti è un banco di prova senza precedenti per i governi e per i cittadini. Senza dibattito che elevi il livello di consapevolezza di ciascuno si è destinati a perdere la partita importante delle libertà personali.

***

Conclusioni
Siamo in un momento in cui è davvero difficile capire il reale andamento dell'epidemia. In questo scenario di incertezza sembra che l'unico interesse sia quello di passare alla fase 2, cioè quello della riapertura delle attività produttive. La delega di responsabilità ai cittadini di tracciare i propri contatti, invadendo - seppure con un meccanismo che protegge la privacy (!) - la sfera delle libertà personali degli individui, sembra essere la astuta premessa su cui poi si potranno basare le azioni formali per riattivare la crescita economica, secondo un paradigma che ha tutta l'aria di riproporsi esattamente uguale a se stesso. Come se niente questa esperienza ci stesse lasciando in eredità.

Una seconda considerazione: la forte mediazione umana richiesta da un metodo tecnologico "non autosufficiente" ci mette al riparo dallo spettro della decisione algoritmica. Ma non è un buon motivo per accettarlo acriticamente.

Qualche strategia dovrà essere trovata per evitare che questa clausura continui ancora a lungo. Ma non si può pensare che i Governi agiscano in modo così opaco; esponendo oltretutto le comunità al rischio di vedersi amministrare da Imprese private (Bendings Spoon in Italia, Apple-Google se pensiamo agli scenari Europei e mondiali). **Bisogna dunque invocare e sostenere a gran voce senza tema di smentita la trasparenza: tanto dei processi decisionali, quanto delle modalità con cui quelle decisioni verranno messe in pratica.**

Si impone una riflessione profonda. Così come è per le misure restrittive a cui siamo sottoposti da un mese, in gioco vi è l'ampia e fondamentale questione delle Libertà personali.