Il Commissario Straordinario per l'Emergenza sanitaria Domenico Arcuri ha annunciato che l'applicazione di tracciamento dei contatti "*Immuni*" sarà pronta a fine mese, dopo non pochi ritardi.

A quasi tutti è chiara l'utilità di questa applicazione ma non a tutti, probabilmente, è stato chiaro come la discussione riguardo la via da intraprendere per il suo sviluppo ci abbia toccati da vicino in qualità di cittadini.

Si parlava, d'altro canto, dei nostri dati e della possibilità di accedervi aprendo alcune porte che, poi, sarebbe stato difficile chiudere.

Storia di un bando

Come risposta immediata all'arrivo del COVID-19 nel nostro Paese, il MID (Ministero per l'Innovazione tecnologica e la Digitalizzazione), in collaborazione con i Ministeri dell'Istruzione e dello Sviluppo Economico, ha deciso di indire prima una "*Fast call*" di tre giorni (dal 24/3 al 26/3) e poi un "*Call for action*" (ovvero un bando) per "*l'utilizzo di tecnologie utili al monitoraggio e al contenimento del virus*". Nello specifico il Ministero, oltre ad "*app e soluzioni tecniche di teleassistenza per pazienti domestici*" chiese di individuare soluzioni *"per il tracciamento continuo, l'alerting e il controllo tempestivo del livello di esposizione al rischio delle persone*". Nonostante tempi relativamente stretti pare che sul tavolo del Ministero siano arrivate più di 300 proposte da parte di varie aziende o associazioni. Per analizzare la documentazione

è stata dunque istituita una *task force* di 74 esperti suddivisi in vari gruppi (ovviamente non senza polemiche dovute al numero degli esperti interpellati).

Dopo alcuni rallentamenti il bando si è concluso il 17 Aprile con la scelta dell'app "*Immuni*" sviluppata dall'azienda "Bending spoons".
Tale scelta da parte del Ministro pare abbia lasciato perplessi alcuni degli esperti interpellati in quanto, come si evince dalle loro relazioni, alcuni avevano suggerito di scegliere almeno due applicazioni in modo di avere una sorta di "backup" in caso emergessero problemi durante l'implementazione.

Nonostante la scelta di una sola applicazione sia da imputare, probabilmente, ad un tentativo di accorciare i tempi di rilascio, lo sviluppo dell'applicazione sta procedendo, anche stando alle relazioni degli esperti, piuttosto a rilento.
Questo pare sia dovuto a svariati approfondimenti tecnici effettuati dal governo oltre che ad un'evidente mancanza di idee chiare da parte delle istituzioni.

Purtroppo, il mondo della tecnologia richiede spesso di analizzare problemi e di effettuare delle scelte piuttosto velocemente.

Cosa che la Pubblica Amministrazione, ahinoi, non sembra essere abituata a fare.

Privacy vs Emergenza

Qualcuno potrebbe già da subito obiettare (non del tutto a torto) che la problematica della privacy è superflua e che, di fronte a un'emergenza, si sia giustificati a prendere decisioni straordinarie.

È tuttavia importante ricordare, citando un interessante articolo di Harari sull'argomento, che "*le misure temporanee hanno la cattiva abitudine di sopravvivere alle emergenze, soprattutto dal momento che un'altra emergenza si presenta all'orizzonte*".

Basti pensare banalmente a come l'attentato dell'11 settembre 2001 abbia radicalmente cambiato le misure di sicurezza aeroportuali.
Inoltre, non bisogna dimenticare che non si parla di "*poteri temporanei*" ma di raccolta dei dati dei cittadini che, per il fatto stesso di esistere, possono essere sottratti alle istituzioni.
Gli esperti di sicurezza informatica, su questo aspetto, amano citare Eugene Howard Spafford: "*l'unico vero sistema sicuro è un sistema spento, chiuso in una gettata di cemento, sigillato in una stanza rivestita di piombo, protetta da guardie armate. Ma anche in questo caso ho i miei dubbi*".

La privacy, quindi, può senza dubbio essere accantonata. Purché lo si faccia con coscienza e, ovviamente, con la dovuta proporzionalità.

La prima decisione da prendere: la scelta delle tecnologie

La prima domanda che si sono dovute porre le aziende che hanno partecipato al bando e gli esperti che hanno dovuto valutare le opzioni è stata: usiamo il *Bluetooth* o usiamo il *GPS*?

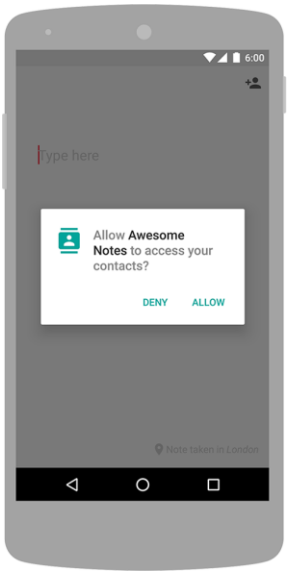
Per chi non lo sapesse il *Bluetooth* è una tecnologia che consente ai dispositivi di connettersi tra loro per comunicare a breve distanza e che può essere usata, con una certa precisione, per identificare "*vicino a chi*" siamo stati.
Il *GPS*, invece, è la stessa tecnologia usata dai navigatori satellitari e consente di tracciare, in ogni momento, il luogo in cui si trova il dispositivo.

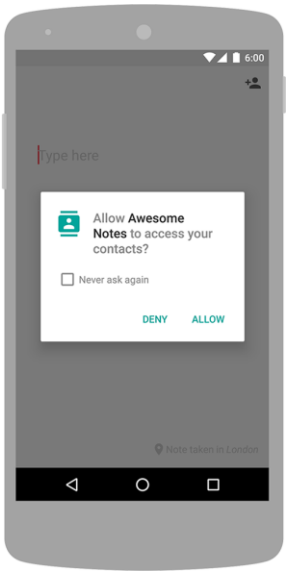
Ovviamente ciascuna tecnologia ha i suoi pro e i suoi contro e, mentre con il *GPS* sarebbe possibile capire dove vanno le persone e, di conseguenza, identificare il grado pericolosità di determinati luoghi "*sensibili*" (ospedali, case di riposo, supermercati) basandosi sulla quantità di persone che li visitano, con il *Bluetooth* è molto più facile ed efficace capire "*chi è stato in contatto con chi*".

Quindi è possibile tracciare i cittadini tramite gli smartphone?

No. Né tecnologicamente né, tanto meno, legalmente.
Questo il punto.

Tutti i cittadini europei, infatti, sono tutelati da un regolamento (detto GDPR) che impone ai fornitori di servizi di non conservare nessun dato che non sia strettamente necessario al servizio stesso.
Cosa che, ovviamente, vincolerebbe l'applicazione a trattenere solo i dati strettamente necessari. Se i problemi legali non bastassero, poi, vi si sommano dei problemi di tipo





tecnico: i sistemi operativi degli smartphone, infatti, impongono una serie di vincoli alle applicazioni, volti anch'essi a garantire la privacy degli utenti.
Un importante vincolo, ad esempio, impone che l'utilizzo del *Bluetooth* da parte di un'applicazione sia possibile solo se l'app in questione sia aperta a schermo.
Inoltre, da policy di ogni sistema operativo, l'accesso a quasi qualsiasi funzionalità (come *Bluetooth* e *GPS*) deve essere consentita dall'utente in fase di installazione.
In breve: qualsiasi app di tracciamento, per funzionare, richiede necessariamente la complicità consapevole degli utenti che dovranno essere tracciati.

Le linee guida europee

A provare a dirimere l'incognita riguardante le tecnologie da utilizzare ci ha pensato l'eHealth Network (una commissione di esperti designati dai paesi membri dell'unione europea tra cui l'Italia) che ha emesso un documento contenente delle linee guida per lo sviluppo dell'applicazione.

Innanzitutto, il team di esperti pone l'accento sulla natura "temporanea e volontaria" dell'applicazione, che non deve essere resa obbligatoria e che, al termine dell'emergenza, deve eliminare tutti i dati raccolti.

In secondo luogo, sottolinea l'importanza di attenersi alla legge sulla conservazione dei dati (e quindi sconsiglia ai Paesi di derogare al GDPR), invitando ad una **politica di conservazione dei dati proporzionale e limitata al necessario**.

A tal proposito, la commissione sottolinea come i dati relativi agli spostamenti degli utenti non siano né necessari né raccomandati al fine del tracciamento dei contratti.

Alla luce di queste indicazioni, tutti i Governi europei, Italia compresa, pare abbiano deciso di convergere su sistemi di tracciamento prevalentemente basati sul *Bluetooth*.

La scelta dell'Italia

Da questo punto di vista la commissione di esperti è stata quanto mai sicura nello scegliere di basarsi su un tracciamento *Bluetooth*.

Quindi nessuno verrà seguito nei suoi spostamenti.
Per onor di cronaca, ogni tanto si è parlato della possibilità di effettuare qualche campionamento GPS per comprendere il modo in cui il virus si diffonde geograficamente ma, qualora ciò accadesse, si è specificato che il tracciamento sarebbe del tutto volontario.

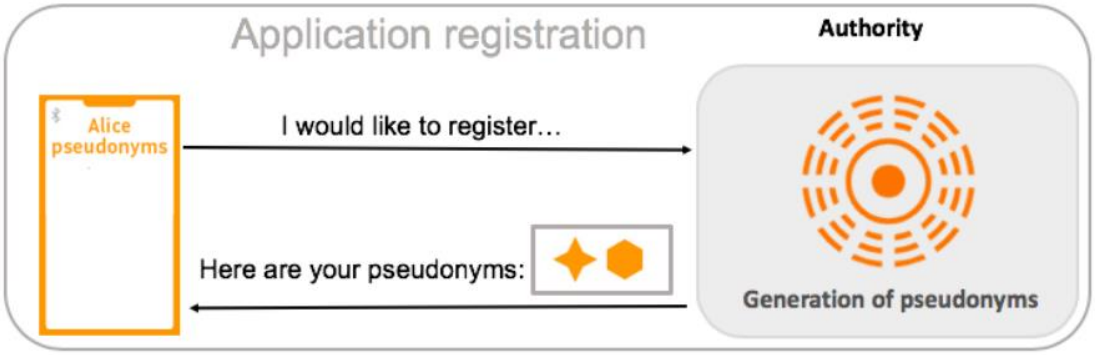
La seconda decisione: la battaglia sul protocollo

Per definire i metodi di tracciamento la comunità scientifica si è messa sin da subito in azione per studiare e proporre diversi protocolli.

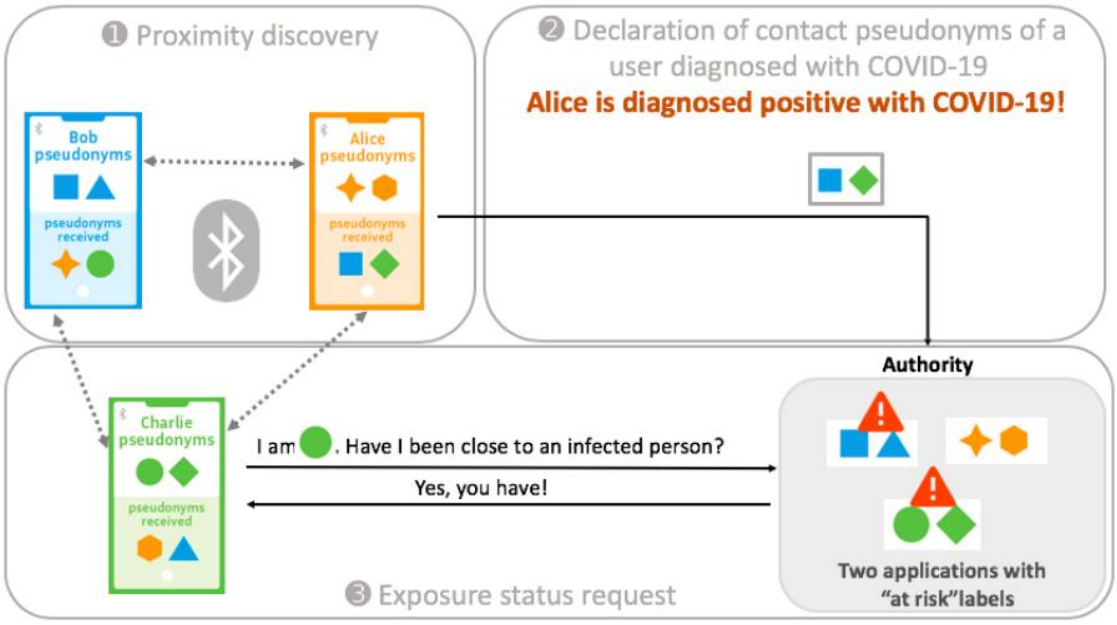
Sono emersi principalmente due diversi approcci alla gestione dei dati.

L'approccio centralizzato

Promosso dal consorzio PEPP-PT *(Pan European Privacy Protecting - Proximity Tracing*), l'approccio centralizzato prevede che ad ogni utente venga assegnato uno pseudonimo e che, periodicamente, i dati di prossimità vengano inviati ad un server centrale.



There are three main phases of the protocol: proximity discovery, declaration of contac pseudonyms of users diagnosed with COVID-19, and exposure status request.



Questo implica che, di volta in volta, si sia in grado di risalire ai contatti tra persone e, eventualmente, si possano rintracciare coloro che sono stati a contatto con qualcuno che sia poi risultato infetto.
In questo approccio il fatto che si conoscano i dati di prossimità dei cittadini è al contempo un punto di forza e una debolezza.

Da un lato, infatti, le autorità potranno vigilare sul fatto che i cittadini rispettino l'isolamento ma, d'altro canto, il fatto stesso che quei dati esistano implica che, potenzialmente, possano essere resi di dominio pubblico (sia per mano di malintenzionati sia a causa di eventuali malfunzionamenti, come pare sia già accaduto in Olanda)

L’approccio decentralizzato

Promosso dal consorzio DP3T (*Decentralized Privacy Protecting Proximity Tracing*), nato da una costola del precedente consorzio, l’approccio decentralizzato vorrebbe risolvere i problemi derivanti dall’utilizzo di un server centrale.

Con questo protocollo ciascun device genera periodicamente degli pseudonimi temporanei che scambia con gli altri device con cui viene a contatto.
Se e quando un utente dovesse risultare positivo al virus, l’applicazione invierebbe al server centrale gli pseudonimi utilizzati negli ultimi 15 giorni (tempo di incubazione del virus) e, a quel punto, chiunque sia venuto in contatto con il soggetto risultato positivo verrebbe avvisato dall’applicazione di un possibile rischio di contagio.
Il punto di forza di questo approccio è dato dal fatto che i dati vengono inviati ad un sistema centrale solo quando necessario e, anche a quel punto, essendo tali dati totalmente anonimi, sarebbe impossibile associare ai codici un nome e, quindi, risalire a quali sono stati i rapporti tra le persone. Ovviamente, ciò comporta anche che sia impossibile un controllo da parte di un’entità centrale e che, quindi, siano richiesti collaborazione e buon senso da parte dei cittadini nel rispettare l’eventuale quarantena.

(Immagine di https://twitter.com/mikarv/status/1249053871172976642)

L’intervento della Silicon Valley

Nel dibattito pubblico tra chi tifa per un approccio centralizzato (che offre maggior controllo) e chi, invece, vorrebbe una miglior salvaguardia della privacy, sono entrate di prepotenza Apple e Google.

Le due aziende, infatti, hanno deciso di collaborare e di rilasciare nei loro sistemi operativi una funzionalità che, sfruttando la logica del protocollo *DP3T*, faciliti lo sviluppo delle applicazioni fornendo nativamente determinate funzionalità *Bluetooth*.
Questo significa che, utilizzando i loro servizi, lo sviluppo di un'applicazione di tracciamento dei contatti con approccio decentralizzato avrebbe la strada spianata dalla maggior parte dei vincoli tecnici.

Nota: utilizzare i servizi di Apple e Google nell'affrontare la crisi non significa affatto mettere ulteriori dati sensibili nelle mani delle due aziende dal momento che l'approccio decentralizzato, per definizione, non ne raccoglie.

La scelta di "*Immuni*"

Nella scelta di "Immuni", inizialmente aveva pesato anche il fatto che l'azienda Bending Spoon facesse parte del consorzio *PEPP-PT*.

Successivamente, in seguito a diverse polemiche riguardo a problemi di trasparenza interni al consorzio e alla separazione da esso del neonato consorzio *DP3T*, gli esperti ministeriali hanno iniziato a rivedere le proprie posizioni.
Dopo vari tira e molla, infine, pare che il Governo abbia ceduto alle richieste degli esperti di sicurezza internazionali che premevano per un approccio decentralizzato e abbia deciso di utilizzare le API fornite da Google e Apple superando, così, anche buona parte degli ostacoli tecnologici.

L'importanza di essere Open Source

Dalla platea di coloro che con il software ci lavorano, sin dall'inizio del progetto, si leva una costante richiesta di rendere il progetto *Open Source*. Ovvero di libera consultazione e fruizione per chiunque abbia la voglia e le capacità di metterci le mani.

Per alcuni questa richiesta potrebbe risultare essere stata soddisfatta nel momento in cui il Ministro ha garantito che il codice dell'applicazione sarebbe stato consultabile: ciò, , purtroppo, non significa open source.

Ricordo che, all'università, il mio professore amava ripetere che "*Open Source is about community*".
Open Source non è solamente il poter aver accesso al codice, ma vuol dire poter segnalare problemi e proporne le soluzioni. L'importante non è leggere il codice, ma aiutare

nell'analisi.
Per quanto, personalmente, io abbia la massima fiducia nelle capacità tecniche degli sviluppatori di Bending Spoon, l'idea che essi abbiano alle spalle un'intera *community* che li supporta e li aiuta a non fare errori grossolani mi darebbe una maggiore sicurezza sul fatto che i miei dati non siano vittima di problemi tecnici.
Se il software verrà reso open source solo dopo il rilascio, di fatto, questo lavoro di controllo non solo sarà più scomodo ma, purtroppo, sarà anche inutile.

L'*Open Source*, insomma, non è una velleità di qualche nerd che vuole ficcare il naso nel codice ma una proprietà (a mio parere imprescindibile in un'applicazione governativa) che è importante venga soddisfatta il prima possibile per limitare possibili problemi.

NDR: tra le fasi di revisione e di pubblicazione dell'articolo sono stati pubblicati i codici sorgente del progetto. È senza dubbio un ottimo punto di partenza e ci auguriamo che il processo di revisione e correzione si svolga nel migliore dei modi.
https://github.com/immuni-app/immuni-app-android

La vera sfida

Le conseguenze di tutte queste decisioni sono importanti per svariati motivi: privacy, sicurezza e capacità dei governi di gestire la crisi (che è poi il motivo primario per cui l'applicazione è stata sviluppata).

Non dobbiamo dimenticarci, però, dell'importanza della trasparenza nell'iter decisionale che porta all'assunzione di determinate scelte e, soprattutto, dell'importanza, per i cittadini, di sentirsi tutelati nell'uso di un'applicazione di questo tipo.

Sembra banale ma, affinché funzioni, l'applicazione deve innanzitutto essere installata. Nello specifico, secondo alcuni esperti, l'applicazione sarebbe pressoché inutile se installata da meno del 25% della popolazione, e inizierebbe a fare davvero la differenza solo se installata dal 60% dei cittadini.

Impresa tutt'altro che banale.

Proviamo a mettere le cose in proporzione:

- Il 73,8% degli Italiani possiede uno smartphone;
- Gli utenti Facebook sono poco meno di 35 milioni (circa il 58% della popolazione);

- Trace Together, l'app di contact tracing governativa di Singapore, nonostante l'adozione tempestiva e la campagna pubblicitaria introdotta, è stata installata dal 12% degli utenti.

In poche parole, perché l'applicazione sia utile, dobbiamo sicuramente fare meglio di Singapore ma, idealmente, fare anche meglio di Facebook.

Cosa tutt'altro che facile.

Per questo è fondamentale che qualsiasi esperto, se interpellato, sia messo nelle condizioni di esprimere la propria opinione in ordine al livello di sicurezza degli strumenti tecnologici utilizzati dal Governo.
Nell'affrontare questa crisi non possiamo permetterci dubbi.