Apple-Google e “contact tracing”: e la sovranità (digitale) Europea?

In occasione del lancio della app di contact tracing Immuni in Italia (e analoghe in altri Paesi), si percepisce una certa diffusa diffidenza, perfettamente comprensibile quando si tocchino aspetti di dimensione intime e riguardanti i nostri dati sensibili. D’altro canto, ci viene detto che utilizzare Immuni è un gesto di grande responsabilità e partecipazione volontaria per la salvaguardia della salute collettiva in ambito pandemico.

Si ha però l’impressione che si sia partiti NON da un “progetto” *top down* organico in tal senso, che individui con realismo e concretezza TUTTI i termini del problema sanitario (processi operativi, obiettivi realistici, strumenti a disposizione, vincoli burocratici, fattore tempo, …) da cui identificare requisiti di app e/o altre soluzioni tecnologiche di contrasto al Covid-19, ma sostanzialmente il contrario. Sia stata cioè posta molta enfasi sull’importanza di una app da cui partire, ipotizzando che possa risolvere il problema complessivo, con tutti i suoi interrogativi.

Andrebbe viceversa approfondito lo **scenario complessivo** – sostanzialmente **organizzativo**, sia dal punto di vista sanitario che di sostenibilità socioeconomica -, approfondendo i processi operativi e la compatibilità con infrastrutture, strumenti, tempi, … e soprattutto il **fattore umano**, elemento centrale sia nei processi organizzativi che di garanzia dei diritti fondamentali delle persone, al cui servizio la soluzione tecnologica prescelta dovrebbe operare – *decision*

support system (DSS). Il "tracciamento" umano dei contatti e le corrispondenti decisioni amministrativo-sanitarie restano il fattore dirimente in qualsiasi processo di contrasto alla pandemia, nel rispetto dei requisiti di tutela della *privacy* e protezione dei dati personali.

Certo, riuscire a gestire in modo automatico il "contact tracing" è sicuramente un elemento (*building block*) di notevole rilevanza. Il termine "tracing" è peraltro fuorviante e ci fa sentire in qualche modo spiati – è più corretto parlare di "exposure notification". In ogni caso, sarebbe importante poter sapere se, quando e dove sono avvenuti contatti tra soggetti infetti (o a rischio) e soggetti – almeno sulla carta – sani, o anche incontri tra persone sane (asintomatiche?), anche per poter gestire sia le politiche che le regole di ritorno alla vita normale.

Sin da subito è stata però esclusa la geo-localizzazione GPS, con la motivazione che potesse far risalire in qualche modo alla identità delle persone. In realtà, a detta di molti esperti, utilizzando un *tracking* GPS opportunamente anonimizzato – e.g. tramite un protocollo PPSI (*Privacy Preserving Set Intersection*) – ad integrazione del *Bluetooth* previsto da Immuni, i problemi di tutela della *privacy* sarebbero sostanzialmente analoghi ma basterebbe il **20% di utilizzo** della app da parte della popolazione rispetto ad **oltre il 60%** con il solo *Bluetooth* per una ipotizzata efficacia dei risultati.

In ogni caso, gli sviluppatori della app, di pari passo con i decisori Governativi, assicurano la tutela "by design" della *privacy*, sostanzialmente garantita da **(i)** assenza di accesso ai (e raccolta dei) dati personali di qualsiasi tipo, **(ii)** disaccoppiamento del "tracing" dall'identità della persona fisica, **(iii)** casualità / non tracciabilità della generazione ed assegnazione dei codici identificativi necessari al *tracing* e **(iv)** disaccoppiamento tra tracciamento degli eventuali contatti a rischio e identificazione dell'utente positivo al

virus, che volontariamente segnala la propria positività sotto il controllo e autorizzazione di un operatore sanitario qualificato.

Tutti argomenti validi, al contempo però opinabili rispetto all'effettiva protezione dei dati personali, aggirabile più o meno sulla base dello specifico processo sanitario in essere relativamente al **tracciamento, test e terapia – le 3 "T".** Una app di *contact tracing* in supporto al contenimento dell'infezione dovrebbe infatti avere varie funzionalità: informativa, di comunicazione con il proprio medico di base, di gestione di un diario clinico personale ed autogestito, ecc. Tutti possibili punti di *leakage* di informazioni personali sensibili, se non accuratamente regolamentati, specialmente in presenza di soluzioni basate sulla "benevola collaborazione" dei giganti *hi-tech* **al di fuori della giurisdizione e sovranità Europea**. E' quindi opportuno riassumere i vari passaggi della vicenda, che coinvolgono non solo Bending Spoon sviluppatore di Immuni, ma – attenzione – la potentissima alleanza Apple-Google, che controlla con iOS e Android la quasi totalità del mercato degli *smartphone*.

Allo scopo di definire un approccio comune ed interoperabile, il 1° aprile u.s. è nato in Europa il Consorzio *Pan-European Privacy-Preserving Proximity Tracing* (PEPP-PT), che ha definito una serie di linee guida sulle app di contact tracing avocazione **centralizzata**. Pochi giorni dopo (4 aprile) è stato sviluppato un approccio a **gestione decentralizzata** delle informazioni raccolte *(Decentralised Privacy-Preserving Proximity Tracing,* DP-3T), che venivano mantenute ed elaborate solo all'interno degli *smartphone*, assicurando in linea di principio una migliore garanzia di anonimato e protezione della *privacy*. Questo approccio prevedeva un metodo di auto-identificazione dello *smartphone* verso il mondo esterno, basato sulla generazione automatica di codici temporanei ed anonimi (pseudonimi effimeri, Ephid) trasmessi tramite l'uso della tecnologia *Bluetooth Low Energy* (BLE) presente nei

nostri *smartphone*.

Ancora qualche giorno ed il 10 aprile u.s. Apple e Google annunciano una iniziativa congiunta che ricalca il DP-3T, di cui rende più efficiente la gestione degli identificativi temporanei in termini di elaborazione, *storage* e loro comunicazione, aumentando nel contempo il livello di sicurezza dei dati. Inoltre, questa modalità permette la gestione del *Bluetooth* LE ad un livello di efficienza / consumi impossibile da ottenere senza l'impegno dei costruttori dei due sistemi operativi. Dopo pochi giorni, inizia a circolare la notizia che l'app Immuni selezionata dal Governo Italiano adotterà la nuova iniziativa Apple-Google, implementando un meccanismo di notifica dei contatti ("Exposure Notification Service") molto attento alla *privacy*. L'app è in grado di permettere ad un soggetto che si scopre positivo di segnalare il suo *status* ad un Centro di Controllo Sanitario, il quale potrebbe così metterlo a disposizione di tutti; ognuno potrebbe successivamente valutare in modo autonomo se è entrato in contatto con il soggetto positivo (tipicamente per almeno **10 minuti** ed entro i **2 metri** circa rilevabili dalla tecnologia *Bluetooth*) nei **14 giorni precedenti** (o quanto diversamente impostato) alla scoperta dell'infezione. Tutto ciò senza che il Centro di Controllo Sanitario conosca la reale identità dei soggetti coinvolti.

In pratica, ogni *smartphone* comunica al mondo circostante un pacchetto di informazioni anonime, che cambiano mediamente ogni 15 minuti. All'interno di questo pacchetto di informazioni c'è un **identificativo temporaneo** (*Rolling Proximity Identifier* o RPI) generato tramite algoritmi crittografici mediamente **ogni 15 minuti** ed alcuni metadati cifrati che contengono il numero di versione del protocollo e la potenza del segnale *Bluetooth* utilizzato. Il RPI viene generato a partire da una chiave anch'essa temporanea (*Rolling Proximity Identifier Key,* RPIK) a sua volta generata in parallelo da una chiave "primaria" (*Temporary Exposure Key,*

TEK). Le chiavi TEK ed RPIK vengono generate ogni 24 ore, ma **la sola chiave primaria (TEK) viene memorizzata nello *smartphone* per 14 giorni –** o quanto diversamente impostato. Per di più, anche l'indirizzo del *Bluetooth* che si sta utilizzando – tipicamente univoco quando si utilizza per altri scopi – in questa modalità di lavoro viene cambiato in modo casuale mediamente ogni 15 minuti. Inoltre è matematicamente **impossibile ricalcolare la chiave RPIK a partire dalle RPI** o **la chiave TEK a partire dalla RPIK**.

Tutta questa complessità serve ad impedire non solo di identificare in modo stabile il nostro *smartphone* – tutte le chiavi sono generate in modo casuale ed in nessun modo legate alla nostra identità – ma anche di "inseguirlo" nei nostri spostamenti per mezzo di apparecchiature distribuite sul territorio, capaci di ascoltare, memorizzare ed elaborare questi messaggi. Cambiando continuamente e casualmente identificativi ed indirizzi, risulta (quasi) impossibile tracciare i nostri spostamenti – V. ad es. studio su possibili attacchi "Towards Defeating Mass Surveillance and SARS-CoV-2: the Pronto-C2 Fully Decentralized Automatic Contact Tracing System".

Il nostro *smartphone,* oltre a trasmettere al mondo circostante questi pacchetti di dati – con gli identificativi temporanei *Rolling Proximity Identifier* (RPI) -, acquisisce e memorizza nello stesso tempo gli equivalenti pacchetti dati provenienti dagli *smartphone* circostanti con cui viene "in contatto" per un periodo di tempo considerato significativo, aggiungendo anche l'orario dell'evento. Queste informazioni vengono memorizzate nello *smartphone* per il periodo di tempo attualmente considerato rilevante ai fini di un contagio – 14 giorni, valore aggiornabile dal sistema, ove siano necessarie durate differenti. Il fatto che le informazioni vengano

conservate negli *smartphone*, rende questo approccio **decentralizzato** o **distribuito**.

Il sistema prevede che periodicamente ogni *smartphone* si connetta ad un ***Diagnosis Server*** – una sorta di Centro di Controllo Sanitario (auspicabilmente) pubblico – per scaricare gli identificativi giornalieri TEK (*Temporary Exposure Key*) associati ai casi risultati positivi. Fornendo queste TEK al *software* Apple-Google presente nello *smartphone*, verrebbero derivate da queste le RPIK e da esse gli identificativi temporanei (*Rolling Proximity Identifier*, RPI). Sarebbe quindi possibile verificare LOCALMENTE se uno o più di questi RPI calcolati coincida con alcuni di quelli memorizzati nello *smartphone*, cioè con i codici temporanei degli altri *smartphone* con cui è venuto in contatto. La TEK permette di ricalcolare anche la chiave di cifratura dei metadati, da cui il sistema Apple-Google può risalire alla **potenza del segnale** all'origine e quindi (misurandone l'attenuazione) alla **distanza** dello *smartphone* emittente (cioè del possibile contagio). La scoperta di aver avuto un contatto a rischio di contagio ci verrebbe quindi evidenziata **dall'app stessa**, e su base volontaria potremmo essere guidati in una serie di azioni preventive e di controllo – ad es. valutare autonomamente eventuali sintomi, contattare il proprio medico di base, una struttura sanitaria *ad hoc,* il Centro di Controllo Sanitario, ecc.

Ovviamente, affinché il *Diagnosis Server* possa fornire le TEK dei soggetti risultati positivi, è necessario che, quando **un soggetto si scopra positivo, comunichi al *Server*** stesso – tramite l'app ed in coordinamento con la struttura medica di riferimento – **i propri TEK degli ultimi 14 giorni**. Questa operazione può divenire critica per la *privacy* ed aprire scenari si sorveglianza di massa su cui vigilare per il contact tracing degli spostamenti e dei contatti degli utenti. La procedura che permette al soggetto positivo la comunicazione dei propri codici, dovrà prevedere

l’**impossibilità di associare l’identità del soggetto** – nota peraltro al Servizio Sanitario a fronte delle analisi fatte – **al messaggio con gli identificativi degli ultimi 14 giorni**. E’ plausibile prevedere che il *Diagnosis Server* possa accettare solo messaggi verificabili tramite **codici di accettazione forniti al paziente** che abbia deciso di condividere il proprio stato sanitario.

C’è da dire che, appena iniziata la sperimentazione lo scorso 8 giugno in quattro Regioni Italiane, ci si è accorti che l’app Immuni non sarebbe in grado di tenere conto della citata distanza di 2 metri, con ciò limitandone l’efficacia di contact tracing */ alerting*. E’ altresì illuminante riportare due brevi incisi di quanto dichiarato nei documenti “Exposure Notification v 1.0” e “ExposureNotification-FAQv1.1.pdf” di Apple-Google:

*“On April 10, 2020, Google and Apple announced a **two-phase exposure notification solution** that uses Bluetooth technology on mobile devices to aid in contact tracing efforts.”*

*“In the second phase, available in the coming months […] After the operating system update is installed and the user has opted in, the system will send out and listen for the Bluetooth beacons as in the first phase, **but without requiring an app to be installed**.”*

Il servizio Apple-Google è stato quindi pensato in **due fasi**, nella seconda delle quali **l’app non è più necessaria**, e tutte le operazioni descritte (dalla generazione degli identificativi temporanei alla loro comunicazione, registrazione, elaborazione ed uso) verranno **svolte direttamente dal sistema operativo** dello *smartphone*. In pratica, Apple e Google (possono e) **decidono di fare tutto da sole**. Chi volesse farne a meno, dovrebbe superare difficoltà non banali (V. Corea).

Ora, il fatto che siano grandi Aziende non fuga dubbi e

interrogativi su possibili comportamenti più o meno etici (già visti in passato). Senza contare la potenziale **violazione delle norme *antitrust*** di un accordo tra di loro per una soluzione sostanzialmente "chiusa", capace di limitare lo sviluppo del mercato. Essa rende molto arduo (se non impossibile) ad altri fornitori sviluppare soluzioni alternative in regime di concorrenza, specialmente rivolte a non possessori di *smartphone – smart band* o simili. E anche per chi li possiede, sarebbero Apple e Google a decidere su quali *smartphone* può funzionare l'app Immuni. I due giganti *hi-tech* potrebbero pertanto spingere milioni di "esclusi" ad acquistare nuovi *device*, traendone un vantaggio commerciale, e rendere plausibile che abbiano in qualche modo favorito l'approccio decentralizzato, facendo apparire quello centralizzato come "Grande Fratello" governativo. Inoltre, il sostanziale "lock-in" della soluzione non assicurerebbe l'**interoperabilità** con altre app, basate su modelli centralizzati (ad es. Francia) o decentralizzati ma diversi dal *framework* Apple-Google, con ciò non garantendone il funzionamento (quantomeno) all'interno UE.

Che due giganti del web possano **parlare da pari a pari ai Governi UE**, spiegando (se non imponendo) loro cosa fare e come farlo rappresenta un rischio serissimo per la sovranità digitale del nostro Continente. A differenza dei passati fasti nelle reti e servizi di telecomunicazioni, tecnologie informatiche, … siamo da decenni estremamente dipendenti tecnologicamente dall'Estero. La crisi creata dal Covid-19 dovrebbe farci riflettere sulle nostre dipendenze e renderci attori consapevoli di un "**nuovo Rinascimento**", investendo in processi e piattaforme *data driven* strategici per la nostra auspicabile **indipendenza tecnologica da USA e Cina**.

Potrebbe ad es. essere arrivato il momento di sviluppare un **sistema operativo UE** (**"EurOS")** per *smartphone,* e una **rete 5G completamente europea** con i nostri Campioni UE?

(Le considerazioni sopra ripotate riflettono le opinioni

personali degli autori)

https://www.key4biz.it/apple-google-e-contact-tracing-e-la-sovranita-digitale-europea/310153/