Il consorzio PEPP-PT, quello che ha dettato le linee guida scelte anche dall'Italia per la sua applicazione chiede a Apple e Google modifiche del loro sistema: è troppo privacy oriented e non permette la raccolta dei dati su un server. Critici anche altri consorzi: il PEPP-PT è un cavallo di Troia

Il consorzio PEPP-PT, Pan-European Privacy-Preserving Proximity Tracing, composto dagli scienziati e dai tecnici che hanno delineato le linee guida per creare app di tracciamento inter-funzionanti a livello europeo, **ha chiesto a Apple e Google di cambiare il modo in cui le loro librerie funzionano**, perché secondo le bozze rilasciate dai due colossi il modo di funzionare del sistema Apple - Google non è esattamente lo stesso che ora il consorzio PEPP-PT ha deciso di adottare.

Hans-Christian Boos, la persona a capo del consorzio, ha tenuto ieri una conferenza stampa dove ha annunciato che diversi Paesi Europei useranno i principi del PEPP-PT all'interno delle loro app di tracciamento. In tutto sono 7 nazioni, con altre 40 che stanno ancora decidendo che soluzione adottare. Alla conferenza, in streaming, era presente anche Paolo de Rosa, il tecnico italiano del ministero dell'Innovazione che ha confermato, ma già lo sapevamo, **che l'app italiana sviluppata da Bending Spoons sarebbe stata coerente con il sistema PEPP-PT.**

Il sistema PEPP-PT, come gli altri sistemi per il tracciamento, prevede l'uso del bluetooth, non chiede l'uso del GPS e protegge la privacy rendendo anonimi i contatti. Un po' quello che viene fatto dal sistema proposto da Apple e Google, dove stanno quindi le differenze?

La differenza **è nel modo in cui vengono gestiti i dati e caricati i dati. Perché la gestione dei contatti si può fare in due modi, uno centralizzato e uno decentralizzato.**

In un sistema centralizzato tutti i dati di tutti gli smartphone vengono caricati su un server centrale, gestito dalle autorità sanitarie, che controlla se ci sono stati contatti tra le persone e avvisa di conseguenza. Questo vuol dire che vengono caricati sul server i dati anonimi di tutti coloro che hanno una applicazione installata, e **sarà il server a capire se tra due "codici" anonimi c'è stato un contatto.**

Nel secondo caso, quello decentralizzato, vengono caricati sul server solo i codici trasmessi dalle persone positive mentre tutti gli altri dati restano sui dispositivi degli utenti: **è il singolo dispositivo a cercare sul server se il possessore ha incontrato, nei giorni scorsi, un utente positivo avvisandolo**.

La differenza tra i due sistemi è ovvia: nel primo caso le autorità sanitarie hanno a disposizione, oltre al numero dei contagiati, anche un dato relativo al numero dei contatti tra persone contagiate e sane, mentre nel secondo caso l'unica persona a sapere che c'è stato un "contatto" pericoloso è il possessore dello smartphone.

Il sistema PEPP-PT inizialmente **era stato pensato per funzionare in entrambi i modi,** 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**.

Il problema 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, **una 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.

Non si è capito bene cosa abbiano chiesto gli esperti del consorzio PEPP-PT a Apple e Google, ma sicuramente una delle richieste è stata di **rimuovere** quelle restrizioni che i due colossi hanno messo (di proposito) per impedire che il loro sistema venga usato per creare un modello centralizzato.

"*Ci sono diversi punti da discutere* - ha affermato Hans-Christian Boos - *ci sono molti punti dubbi nella loro implementazione. Ma crediamo che ci siano margini di discussione*".

Al momento, proprio per questioni di privacy, **le librerie di Apple e Google sono pensate per impedire il match dei contatti sul server**: tutto deve avvenire sul dispositivo dell'utente.

Dal nostro punto di vista crediamo che ci sia ben poco da fare: forse Google potrebbe anche cambiare idea, ma quando c'è anche quell'azienda che da anni dice che "*Tutto quello che è sul telefono resta sul telefono*" è davvero difficile che possa cambiare qualcosa, che i dati vengano inviati a dei server e elaborati sul server. **Apple non lo permetterà mai, sarebbe contro la sua religione.**

Questa deviazione del PEPP-PT ha creato anche malumore in quello che è l'altro gruppo europeo che si è occupato di creare un sistema di tracciamento sicuro e anonimo, il DP-3T. Creato da esperti della privacy e esperti di sicurezza, **il protocollo DP-3T era stato inizialmente integrato nel PEPP-PT ma poi, giusto ieri, è stato rimosso il riferimento dal sito del PEPP-PT.** E qualcuno se ne è accorto, tanto che alcuni esponenti del DP-3T pensano che ci sia qualcosa da nascondere e che alla fine questo sistema sia diventato una sorta di cavallo di troia.

> **Michael Veale** @mikarv · 16 apr 2020
> Remember this? PEPP-PT has (without notice) removed #DP3T's decentralised, privacy-preserving approach from its site. PEPP-PT stands now ONLY for an intransparent, unpublished centralised database of Bluetooth social graph data, prone to leakage and function creep. twitter.com/mikarv/status/…
>
> > **Michael Veale** @mikarv
> > Important on COVID BT proximity tracing
> >
> > The 'PEPP-PT' protocol is not settled. Our decentralised privacy design (DP-3T) prevents co-optation, function creep. Centralised alternatives do not.

Do not support PEPP-PT w/o making support explicitly CONDITIONAL on decentralisation.

Michael Veale
@mikarv

PEPP-PT now represents closed industrial interests.
PEPP-PT now represents an attempt to get Apple to lower its device-level privacy protections.
PEPP-PT now represents an attempt to deliberately blur #DP3T with a centralised database to enhance its credibility.

129 20:16 - 16 apr 2020

70 utenti ne stanno parlando

"*PEPP-PT è diventato un database centralizzato poco trasparente e inedito di dati*" sono le parole pesanti di Michael Veale, Docente di diritti digitali e regolamentazione dell'Università di Londra e membro del DP-3T.

Sistema che, ricordiamo, **è quello su cui si basa l'applicazione italiana**. Fino ad oggi non sapevamo molto di questa applicazione: ora sappiamo che quasi sicuramente **sarà con server centralizzato e non utilizzerà le api di Google e Apple**. Sempre che non ci siano svolte nei prossimi giorni.

Quali sono le differenze a livello di privacy? In nessuno dei due casi i dati degli utenti vengono esposti, ma nel momento in cui tutti i dati vengono caricati su un server per effettuare la ricerca di possibili contagi si crea uno spiraglio in più per poter associare le chiavi random ai singoli dispositivi, **esiste un log del server, esistono degli IP, esistono delle richieste**. Non è più così anonimo.

Se è lo smartphone a scaricare la lista dei messaggi inviati dai positivi e a controllare, in locale, se per caso ha ascoltato alcuni di questi messaggi il problema non si pone.

È anche vero che questa soluzione **non permetterebbe alla Protezione Civile di avere un'idea della diffusione dell'epidemia**, cosa che potrebbe anche essere importante. Lo sanno bene quelli del consorzio "privacy oriented" DP-3T, che prevedono all'interno dell'applicazione un opt-in che l**ascia agli utenti la scelta di condividere dati anonimi alle autorità per dare informazioni sulla diffusione del contagio**. Cosa che invece con una app basata su PEPP-PT viene fatta di default, e non può essere disattivata.

Per approfondire...