COVID19: Servidores nacionales para el almacenamiento de los datos.

Por: Alfredo Moreno. alai. 05/05/2020

Para que la trazabilidad epidemiológica mediante APPs funcione, al menos el 60% de la población se la debería descargar. Es decir, 50 millones de alemanes, 30 millones de españoles o 25 millones de argentinos. Esta es la cifra que los gobiernos europeos estiman para el proyecto DP-3T, una alternativa al almacenamiento centralizado de los datos.

En las últimas semanas de la cuarentena se está hablando constantemente de aplicaciones basadas en tecnologías de informática y comunicaciones TIC para monitorear los contagios y evitar una nueva expansión de la covid-19. Es decir, realizar la trazabilidad de los contactos que cada persona tiene en sus teléfonos móviles registradas como conexiones Bluetooth.

Siguiendo el ejemplo de países como Singapur, China y Corea del Sur, los gobiernos europeos han decidido apoyar los planes de salud pública para contener el virus con la utilización de tecnologías y datos digitales. Las estrategias para la llamada “fase 2” incluyen una mezcla de acciones para controlar la tasa de mortalidad a través de medidas selectivas de confinamiento, tests rigurosos y aplicaciones digitales para trazar los contactos y evaluar el impacto de las reaperturas selectivas en las áreas o sectores con más riesgos.

Según el estudio publicado por los científicos del Nuffield Department of Medicine de la Oxford University[i], el rastreo de contactos es una medida fundamental. La aplicación será un soporte al rastreo de contacto manual. Para ser eficaz, la aplicación deberá ser utilizada por una gran parte de la población, alrededor del 60%.

A principios de abril se creó el consorcio paneuropeo con ocho países y 130 investigadores llamado Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)[ii] para analizar los modelos centralizados y descentralizados sobre el rastreo personalizado. Existían enfoques distintos, pero había una voluntad común de desarrollar un sistema de rastreo de contactos que tuviese como objetivo la privacidad (sin geolocalización) y la protección de los datos de los ciudadanos. Las

divergencias técnicas se convirtieron rápidamente en una batalla política sobre la dirección a seguir. En plena polémica, académicos del consorcio PEPP-PT decidieron hacer pública la solución descentralizada mediante el uso del protocolo DP-3T, desarrollado por investigadores europeos sobre privacidad y ciberseguridad.

Cómo funciona el protocolo DP_3T

La APP que implemente el DP-3T, realizará el almacenamiento de los datos en forma descentralizado. Es decir, los datos, son protegidos con sistemas de anonimización que ocultaran los datos sensibles de las personas.

Los datos, se conservan localmente en los dispositivos donde se hace también el análisis del riesgo de infección. Si fuese necesaria la utilización de servidores centrales, deberán transmitirse solo unas claves anónimas y temporales correspondientes a los usuarios infectados, de manera que no sea posible conocer la identidad de las personas.

La solución descentralizada responde perfectamente a la exigencia, propia de la normativa para la protección de los datos que deja a los ciudadanos el control sobre sus datos personales. Esta modalidad evita que toda autoridad, agencia gubernamental o sujeto pueda utilizar de forma impropia los datos sanitarios que tienen un alto valor comercial y de inteligencia.

La trazabilidad de contactos se realizará mediante la tecnología Bluetooth que permite que los celulares detecten otros dispositivos cercanos sin la necesidad de registrar los datos sobre la posición de las personas (sin georreferenciación). Cada vez que dos celulares se “encuentran”, se intercambian su identificativo anónimo ID, utilizando el protocolo Bluetooth: comunicación por radio frecuencia.

Los dueños del tráfico

Para garantizar la interoperabilidad de los dispositivos Apple y Google han propuesto un enfoque común para implementar en sus sistemas operativos Android e iPhone.

El sistema operativo de Android e iPhone estará listo a partir de mayo y las APP podrán implementar el DP-3T que utilizará la lista de contactos almacenada en cada dispositivo, los ID Bluetooth para alertar a los dispositivos que han estado en el radio de un dispositivo de una persona con positivo de covid-19.

Cuando las personas están próximas, sus teléfonos celulares intercambian por Bluetooth un código identificador anónimo que cambia aleatoriamente.

El celular guarda dos listas durante 15 días; uno con los códigos enviados y otro con los recibidos. En caso que una persona dé positivo se sube al servidor en la nube el código de identificación propio de los últimos 15 días y ese es utilizado por el resto de dispositivos para ver si existe coincidencia.

El análisis de coincidencia se realiza en el propio teléfono celular. Es decir, lo que hace el sistema descentralizado es descargar del servidor de la nube los códigos de quienes han dado positivo y compararlos con los códigos almacenados en el móvil.

La propuesta de Apple y Google se coloca en la filosofía y los principios del modelo descentralizado inspirado por DP-3T al crear una API –es decir una interfaz de programación que permite a los programadores interactuar con la plataforma– a la cual las aplicaciones de los diferentes gobiernos se podrán conectar.

La propuesta de Google y Apple afianza el poder de los gigantes de internet. Francesca Bria, una de las mayores expertas en temas de innovación digital en Europa, sostiene que este debate sería importante en el sentido de que la Unión Europea reconociera que los enfoques basados en descentralización y privacy-by-design no son opuestos a los esfuerzos europeos para recuperar soberanía tecnológica: al contrario, deberían representar la base para conseguir este objetivo.

El Computer Chaos Club[iii], una de las mayores asociaciones europeas de hackers, ha desarrollado un decálogo con recomendaciones para evitar abusos que puedan vulnerar la privacidad de las personas. Por eso, la tecnología que capte los datos de los ciudadanos para combatir el coronavirus deberá reunir estas condiciones:

- Propósito epidemiológico
- Uso voluntario por parte de los ciudadanos.
- Privacidad.
- Transparencia.

- Los datos no se deberán gestionar de forma centralizada.
- Solo se podrán recopilar los datos indispensables.
- Los usuarios habrán de gozar de la garantía de permanecer anónimos.
- No deberá crear perfiles de movimiento de los usuarios.
- Las claves cifradas para que la tecnología funcione deben ser temporales y no vinculables.
- Las comunicaciones entre dispositivos deben ser inobservadas.

Las TIC deben ayudar de una forma realista a combatir la pandemia. Por ello, los países no deben exigir el uso de estas APPs ni tampoco que quienes se nieguen a ello sean castigados.

El DP-3T es un protocolo diseñado en colaboración por varias universidades y centros tecnológicos suizos, belgas, neerlandeses, alemanes, italianos y británicos. En su repositorio en GitHub se puede encontrar un manifiesto con propósitos y requisitos para su tecnología, en el que se insiste en la necesidad de mantener la privacidad de los usuarios.

Apple y Google sólo son el medio, no el sistema. Los gobiernos deben usar servidores nacionales para el almacenamiento de los datos de la población, fuera del control de esas multinacionales. Además, disponer medidas legislativas que frenen la ambición desmedida sobre la facturación de los servicios prestados por empresas de Telecomunicaciones.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: alai.

Fecha de creación
2020/05/05