



Carmela **Troncoso**

Tenure Track Assistant Professor en la École Polytechnique Fédérale de Lausanne (Suiza)

El debate sobre la gobernanza, más allá de la privacidad

Carmela Troncoso (Ingeniera de Telecomunicación por la Universidad de Vigo) ha realizado su carrera investigadora en el ámbito de la seguridad y la privacidad. Realizó su Tesis Doctoral en Katholieke Universiteit Leuven (Bélgica) para incorporarse después al centro tecnológico Gadiant (Galicia) y posteriormente al IMDEA Software Institute (Madrid). Actualmente dirige el grupo SPRING en EPFL (Suiza), grupo que ha desarrollado el protocolo DP-3T, núcleo de la aplicación SwissCovid en Suiza y que ha sido adoptado por Google y Apple como base para su API de notificación de exposición al coronavirus.

La utilización de apps móviles se ha planteado como una solución para el rastreo de COVID-19 y se ha utilizado en diversos países, con mayor o menor éxito. ¿Porqué piensas que se ha tardado tanto en implantar en España una app móvil similar?

Porque no se ha implementado antes en España lo desconozco. El código está ahí. En Suiza el piloto se puso en

marcha en mayo y la aplicación a principios de junio, en Alemania a mediados y en Irlanda a finales, por ejemplo. El verdadero bloqueo tecnológico residía en *bluetooth*, pero en el momento en que Google y Apple lo solucionaron, ese problema ya dejó de existir.

¿Cual fue el problema con bluetooth?

Las “balizas” (*beacons*) *bluetooth* fue-

ron creadas con la idea de ser herramientas de publicidad, por lo que fueron diseñadas para ser invasivas. En el sistema operativo de Apple, para la que es esencial la protección de sus usuarios respecto a terceros - es uno de sus mensajes comerciales más fuertes, está en su ADN-, la aplicación no podía utilizar estos *beacons* cuando estaba en *background*, es decir, cuando se está



Es la primera vez que los gobiernos han desplegado herramientas que no están basadas en datos. Eso es un precedente: no siempre se necesitan tantos datos de los usuarios para dar servicios

ejecutando pero no está activa. Este fue uno de los problemas en Singapur: los usuarios debían tener todo el rato encendida la aplicación con lo que ello supone de gasto de batería. Para que este *contact tracing* funcionase necesitamos que Apple modificara su modelo de permisos y la aplicación pudiera usar los *beacons* en *background*.

Este fue el principal escollo pero ha habido otros.

¿Cuáles fueron?

Aunque ha sido muy importante que Apple y Google trabajasen juntos, vimos en nuestros experimentos que, a nivel de *bluetooth*, aunque iOS y Android usan estos tipos de *beacons*, cuando “hablaban” entre sí había pequeños fallos (no se leían bien, se perdían algunos...). Era muy importante que se pusieran de acuerdo para hacer un sistema interoperable.

En tercer lugar, estaba la cuestión de cómo usar la aplicación para no consumir mucha batería. Al final son Apple y Google los que tienen la capacidad para cambiar el *framework*, la potencia de uso, etc...

Todo esto me lleva a un punto muy importante y es que todo el mundo está muy preocupado por la privacidad, pero creo que tenemos que pensar que la privacidad nunca es el fin, es un medio para protegernos de terceros y preservar nuestra autonomía y nuestra democracia. Cuando nosotros hicimos presión para que el protocolo que se implantase a nivel mundial fuese muy seguro, la idea era proteger a los ciudadanos de los gobiernos.

Es un hito que Google y Apple se pusieran de acuerdo. ¿Cómo lo valoras?

Que Google y Apple apoyaran esta iniciativa es maravilloso, pero también muestra el poder que tienen y la dependencia que tenemos de ellos. Es la primera vez que ha quedado patente y es brutal. Son los que han decidido cómo el planeta va a implementar *contact tracing*. Al final hay una discu-

sión que es más importante que la de la privacidad y es la de la gobernanza. No porque algo sea *privacy preserving* es algo estupendo y maravilloso. Esperemos que la app ayude a salir de esta situación de emergencia. Pero cuando se decide introducir la tecnología, se crean dependencias y hay que tener claras sus implicaciones sociales.

Por otro lado, es un hito histórico que los gobiernos por primera vez han desplegado herramientas que no están basadas en datos. Y esto genera un precedente: no se necesitan todos esos datos que nos piden para hacer las cosas. Es algo que, como ingenieros, debemos tener siempre en cuenta.

¿Cómo funciona el rastreo? ¿Dónde está la inteligencia?

Al bajarse la aplicación se da una orden a la API del móvil para que genere cada día una clave privada nueva. A partir de esa clave se derivan unos números aleatorios de manera que nadie puede identificarlos ni relacionarlos con nada. La aplicación va emitiendo uno de esos números, cambiando de vez en cuando para evitar seguimientos. Cuando dos teléfonos que tienen la aplicación se acercan, escuchan estos números y los guardan junto con el día y hora y la potencia con la que lo han escuchado. Esta potencia es lo que se utiliza para saber la distancia a la que han estado. Al cabo del tiempo, el teléfono tiene dos listas, la de números que ha emitido y la de números que ha escuchado.

Cuando una persona da positivo por COVID, y siempre que quiera participar en este protocolo de notificación, recibe un código que introduce en la aplicación y los números que ha ido emitiendo se suben a un servidor. Estos números no están asociados a ningún nombre, ni contienen datos de movilidad ni de contactos. Todos los teléfonos periódicamente acuden a este servidor y se bajan estos números y comprueban internamente si los han visto. En ese caso hace un cálculo con todos los números para decidir si has pasado suficiente tiempo muy cerca del virus. Si el resultado está por encima de un determinado umbral, el móvil te muestra una notificación. Da igual si los números son de una misma persona o no porque eso la aplicación no lo sabe. A partir de ese momento no sabemos que hace cada persona: la privacidad en el diseño hace que se pierda la visibilidad de lo que está pasando.

En ese sentido, lo único que, por ejemplo, va a conocer la Administración es cuánta gente sube estos datos, lo que de hecho ya sabe porque conoce cuántos tests positivos tiene. Pero es que este sistema no tiene como objetivo ayudar a la Administración a obtener datos. Es un dispositivo de alerta temprana que permite avisar a la gente de forma rápida (más que con rastreadores “manuales”), incluso a desconocidos del que ha dado positivo, para cortar las cadenas de contagio cuanto antes. ■