

La privacidad en los tiempos del coronavirus

Fernando Pérez González

Catedrático Depto. Teoría do Sinal e Comunicaci3ns, Universidade de Vigo

Miembro de la Real Academia Galega de Ciencias

La balsa a la deriva que es Europa durante la crisis del coronavirus ha recibido una nueva sacudida por cuenta de la app móvil que habría de facilitar el seguimiento de los contactos en proximidad una vez iniciada la fase de “desescalada”. Esta app alertaría a los ciudadanos de que se ha estado cerca de un diagnosticado con coronavirus en el periodo en que éste era contagioso y, en función del riesgo, recomendaría la realización de un test. Aunque existe un consenso generalizado en que la tecnología más apropiada--por su rango similar al del contagio--debe ser Bluetooth y que la geolocalización no es necesaria ni recomendable (lo que deja fuera tecnologías como la triangulación o la trilateración empleando GPS o estaciones base de telefonía, adecuadas para estudios de movilidad), se discute sobre cómo debe ser el protocolo que dé soporte a la app.

El debate tiene lugar en el seno del recientemente constituido “Consortio Paneuropeo para el Seguimiento en Proximidad con Preservación de la Privacidad” (PEPP-PT), al que el gobierno español se sumó hace un par de semanas y que cuenta con la anuencia, cuando no el respaldo, de la Comisión Europea. Ésta ha publicado una guía en la que insta a los países a implantar soluciones basadas en datos “seudonimizados” para garantizar la privacidad de los ciudadanos. Habiendo consenso a este respecto, en el fondo de la disputa está si el diseño de la red de soporte debe ser centralizado o no. La propuesta descentralizada (denominada DP-3T), que maximiza la privacidad con un protocolo brillante por su sencillez, es defendida por numerosos expertos europeos en privacidad y seguridad. Además, su diseño es abierto, por lo que puede ser estudiado para identificar posibles debilidades presentes o futuras. Garantizando el anonimato, permite que un infectado envíe el aviso a los potenciales contagiados por él sin intervención de ninguna autoridad central (la comprobación de si hemos estado en contacto con el infectado se hace en nuestro móvil).

En el esquema centralizado la verificación de posibles contagios se realiza en un servidor central. Aunque se siguen usando seudónimos, existe un riesgo mayor de “desanonimización” por parte de un “Gran Hermano” porque se puede cruzar información. Pero lo que se pierde en privacidad se gana en utilidad: estos datos tienen gran valor epidemiológico, por lo que varios países, entre los que están Francia y el Reino Unido, parecen preferir esta solución. El hecho de que estos protocolos no hayan sido desvelados hasta hace muy poco ha dado pie a un alud de críticas de la comunidad criptográfica, que abrumadoramente se ha decantado por DP-3T, con un asomo de miopía semejante a la que aconsejaba primar el confinamiento total sobre la continuidad de cualquier actividad económica, atendiendo a criterios exclusivamente científicos. Así y todo, la solución centralizada en nada se parece a las medidas de control masivo adoptadas por los países asiáticos que mejor han frenado la expansión.

En esta guerra de protocolos que acaba de comenzar, los defensores de la “privacidad a ultranza” han encontrado el apoyo de Apple y--no se rían--Google, que van a integrar variantes de DP-3T con sus sistemas operativos. Europa, bizantina Europa: mientras aquí se discute, en EE.UU. se implementa y se saca provecho, aunque sea en términos de imagen. Pero, ¿cómo es que Google defiende ahora la privacidad? Muy sencillo: porque ya tiene todos los datos que cada uno le regalamos a diario y que también le permitirían inferir quién está infectado y a quién puede haber contagiado. Si quisiera, claro...