

Ciencia y TECNOLOGÍA

MUNDO DIGITAL

El teléfono delator

J. ANTONIO GARCÍA MACÍAS/ COLABORACIÓN
Ensenada, B. C. jagm@cicese.mx

A partir de los patrones de movilidad celular es posible determinar la posición de un celular, aunque no con seguridad del cien por ciento como sucede en las películas policíacas norteamericanas.

Una escena muy recurrente en películas hollywoodenses y series policíacas involucra la localización de la guarida del villano, el cual es delatado por las señales de su teléfono celular. Aunque es cierto que las señales de comunicación inalámbrica pueden usarse para determinar la localización de una persona, establecer el lugar preciso donde se encuentra queda aún en el ámbito de las películas.

Localización vía celular

Cuando un teléfono celular está encendido, incluso si no hay una llamada activa, ocurre en forma continua un proceso de comunicación entre el teléfono y la torre base a la que actualmente se encuentra asociado. Cuando un celular se desplaza, llegará un momento en que la señal entre éste y la base no será lo suficientemente fuerte, por lo que buscará asociarse a otra con la que tenga una potencia de señal adecuada. La cobertura o alcance de cada una de dichas estaciones base puede ser de hasta varios kilómetros. Así pues, si se usa como referencia la estación base a la que actualmente se encuentra asociado el teléfono, lo más que se puede decir es que se encuentra en algún punto dentro de un círculo, donde el área de dicho círculo corresponde a la cobertura de la estación base. Usualmente las zonas de cobertura se traslapan un poco, sobre todo para permitir un buen traspaso del teléfono de una a otra. Entonces, si el teléfono se encuentra en una zona donde dos estaciones puedan escuchar su señal, se puede determinar que dicho teléfono se encuentra en la intersección de ambas

zonas de cobertura, con lo que su localización se hace más precisa. De esta forma, se puede extrapolar a la intersección de tres o más zonas, con lo que la precisión en la determinación de la localización será mayor. Aún así, para determinar la localización exacta de la guarida del villano, se requeriría tener una precisión de unos tres o cuatro metros, lo cual no es posible solamente usando la técnica indicada con los teléfonos celulares (las torres no están lo suficientemente juntas). Si el teléfono del villano tuviera GPS y por descuido lo hubiera dejado activo, la historia cambiaría.

Dime dónde andas y te diré quién eres

Si bien la mencionada escena de localizar la guarida del villano mediante las señales de su teléfono celular resulta un poco exagerada, hay otro elemento clave que no se aparece en las películas y que es posible determinar mediante el teléfono celular: quién es el villano.

Un grupo de científicos liderado por Yves-Alexandre de Montjoye obtuvieron acceso a un importante conjunto de datos de una empresa de telefonía celular, consistente en los registros de movilidad (indicando el traspaso entre torre y torre) de un millón y medio de usuarios, correspondiente a un periodo de quince meses. Es importante notar que dichos registros estaban completamente anonimizados.

El mencionado equipo de científicos acaba de publicar un estudio en la prestigiosa revista Nature, en el cual muestran que a partir de los registros de movilidad celular se pueden identificar patrones que permiten determinar la identidad de cada usuario con un nivel de confianza de hasta 95%. Quizás uno de los aspectos más impresionantes del estudio es que, una vez determinados los patrones de movilidad individual, se necesitan solamente cuatro puntos geográficos y las horas a las cuales fueron visitados para determinar de cuál usuario se trata. Según explican los in-

vestigadores, esto se debe a que nuestros patrones de movilidad son únicos, de la misma manera que lo son nuestras huellas digitales. Sin embargo, para determinar la identidad de una persona mediante su huella digital se necesitan doce puntos de comparación, mientras que con los patrones de movilidad bastan sólo cuatro.

Datos personales en las redes

Si bien es cierto que los investigadores tuvieron acceso a datos privilegiados y que las empresas telefónicas no le otorgan los registros a cualquiera, también es cierto que bien pudieron haber conducido el experimento con los datos que los mismos usuarios hacen públicos a diario. Hay que pensar por ejemplo en los datos de localización inmersos en fotografías en Instagram, en publicaciones de Facebook, en mensajes de Twitter, en check-ins de Foursquare, e incluso en registros públicos tales como dirección de casa y de lugar de trabajo. El mismo estudio indica también que si se cuentan con tan sólo dos puntos, se puede identificar a casi la mitad de los usuarios.

Otro hallazgo importante es que incluso si se reduce la resolución de los datos, por ejemplo tomando registro cada determinada cantidad de horas, o bien bajando la precisión de la localización geográfica, de todos modos se siguen teniendo los mismos resultados. Es decir, al reducir la resolución no se anonimizan en mayor medida los datos ni se pierde calidad en las predicciones. Las implicaciones de este estudio nos indican que los rastros digitales que vamos dejando cuando utilizamos redes sociales, o simplemente cuando utilizamos un teléfono celular, pueden revelar información que no queremos que sea pública. Y esto es sólo el inicio, pues ya se están haciendo estudios donde se fusionan diferentes fuentes de datos, lo cual sin duda

dará predicciones de mayor calidad y revelará mayor cantidad de información. Ante esta situación, un aspecto de fundamental importancia consiste en actualizar el marco legal para proteger a los usuarios respecto al uso que se le pueda dar a sus datos. También deben proveerse medios que permitan a los usuarios controlar la calidad y cantidad de datos que se desean revelar. Aunque también es cierto que debemos ser más cuidadosos en cuanto a los rastros que vamos dejando en el mundo digital.

**El autor es investigador del Centro de Investigación Científica y de Educación Superior de Ensenada (Cicese) jagm@cicese.mx*



Fotos: Cortesía

