



En algunos casos, dicen, pueden activarse por error, pero esa información no debería ser utilizada:

# ¿Nos espían los teléfonos? Surgen dudas tras una demanda contra la asistente virtual Siri

Los especialistas explican que es muy importante leer los términos y condiciones de los aparatos tecnológicos y las apps para evitar sorpresas.

MANUEL HERNÁNDEZ

El asistente virtual de Apple, Siri, nos escucha cuando le pedimos ayuda y también cuando no queremos. Eso dijo una demanda colectiva presentada en un tribunal de California en 2019. Todo esto, luego que el diario británico The Guardian publicara un artículo alegando que el micrófono de Siri fue encendido a escondidas para grabar conversaciones sin el conocimiento de los usuarios.

Y hace cuatro días, Apple acordó pagar 95 millones de dólares para resolver el conflicto, aunque no se confirmaron las acusaciones que tildaban a Siri como un espía que escuchaba a usuarios de iPhone y otros dispositivos más allá de cuando las personas autorizaban su escucha con la frase "Hey Siri".

Pero esta no es la única empresa con ese tipo de acusaciones. Un caso similar contra el asistente virtual de Google aún está en los tribunales de EE.UU.

La *security researcher* de ESET Latinoamérica, Martina López, aclara que "este acuerdo que hace Apple no es efectivamente para confirmar que esto sucedió, sino que es un acuerdo preliminar, probablemente para evitar problemas".

Pero ¿nos espían o no? Marcel Goic, investigador del Instituto Sistemas Complejos de Ingeniería y académico de la Universidad de Chile, explica que "en los cuerpos legales actuales no está permitido hacer uso de datos personales con propósitos distintos de los exclusivamente hechos por la aplicación original. En este sentido, aunque la tecnología para monitorear este tipo de registro existe, prácticamente no hay casos documentados. En efecto, en el caso de Apple, la firma no ha reconocido traspasar la regla".

Coincide Renzo Gandolfi, abogado de la U. Andrés Bello y experto en nuevas tecnologías, quien detalla que "nuestra legislación en cuanto a



Los especialistas recomiendan revisar la configuración de los teléfonos y limitar la configuración de los asistentes virtuales. Además, aclaran no hay registro de que se usen otras herramientas sin consentimiento, como la cámara.

## Los autos también captan información

Muchos de los autos más modernos no solo saben dónde se ha estado y adónde se va, sino que también tienen acceso a contactos, registros de llamadas, textos y otra información sensible gracias a la sincronización con teléfonos móviles.

Uno de los casos más recientes fue la explosión del Cybertruck de Tesla cargado con fuegos artificiales que estalló frente al Trump International Hotel de Vegas. De hecho, a las pocas horas de la explosión, Tesla pudo rastrear los movimientos en detalle desde Denver hasta Las Vegas, y también confirmar que el problema eran los explosivos en el camión, no el camión en sí. Además, Tesla utilizó datos recopilados

de estaciones de carga y del software a bordo, y recibió elogios. Esos datos fueron útiles para que la policía rastreara los movimientos del conductor. Pero David Choffnes, director ejecutivo del Instituto de Ciberseguridad y Privacidad de la Universidad Northeastern de Boston, alertó que, "cuando sucede algo malo, es útil, pero es una espada de doble filo. Las empresas que recopilan estos datos pueden abusar de ellos". General Motors, por ejemplo, fue demandada en agosto por el fiscal general de Texas por supuestamente vender datos de 1,8 millones de conductores a compañías de seguros sin su consentimiento.

eso ciertamente tiene estándares que son muy altos desde el punto de vista de cómo se protege la privacidad del usuario en este caso. Entonces, todo va a depender del consentimiento que yo acepte en los términos y condiciones del contrato de servicios, en este caso, de Apple". Y añade que "tanto nuestro código penal como la nueva ley de protección de datos personales establecen que esto no se puede (hacer)".

Martina López precisa que es po-

sible que las compañías utilicen los datos para hacer mejoras en el funcionamiento del teléfono o de las apps o que vendan los datos para publicidad, siempre que esté en el contrato que el usuario acepta. "Pero el decir 'nos graban, nos espían', es una cuestión un poquito más sensible, sobre todo con la importancia que les dan cada una de las compañías a las leyes de protección de datos".

Eso sí, la especialista reconoce

que en algunos casos estos aparatos pueden grabar por error: "Una activación accidental, porque reconoció algún tipo de sonido, que también es una opción configurable bastante popular en los asistentes, puede causar que nuestra información quede grabada sin siquiera tener un motivo malicioso puramente".

Frente a eso, López recomienda "leer los términos y condiciones y la política de privacidad, que es donde están detalladas acciones co-

mo estas. ¿A quién va la información que nosotros colocamos? ¿Qué información se registra? Si es solo de uso (para fines de optimización del servicio), se podría saber desde cuánto tiempo estuvimos leyendo un artículo, dónde hicimos clic, hasta la marca y modelo de nuestro teléfono celular. Toda esta información, de nuevo, es la que está detallada en el contrato".

Para resguardar nuestra privacidad, el director de Tech-Law y académico de la U. Central, Gonzalo Álvarez, recomienda partir revisando la configuración de privacidad de todos los dispositivos inteligentes: "En el caso de Siri, hay que revisar la configuración del iPhone y desactivar o limitar la configuración de 'Oye Siri'".

Y también sugiere controlar los permisos que tiene el micrófono, "porque muchas aplicaciones tienen la autorización de uso del micrófono incluso cuando no se está usando la aplicación". Concluye que "con Android también hay ajustes para 'desactivar sensores', y así tienes la plena seguridad de que no te está escuchando nadie".