JUSTICIA Y DD.HH

Control social vs. derecho a la privacidad

El Ciudadano · 27 de marzo de 2020

Expertos del portal Recode lanzaron este jueves, tras una investigación, un par de preguntas claves: la recopilación de datos de los usuarios, en medio de la pandemia del coronavirus, ¿puede violar sus derechos de privacidad? Y de ser así, ¿superan los beneficios temporales las implicaciones a largo plazo?

El covid-19 ha costado ya la vida a millares de personas e infectado a más de **500.000 a nivel mundial**. Y en un esfuerzo por detener su propagación,

diversas empresas que se ocupan de la información de los usuarios ofrecen ahora sus servicios de análisis de datos.

Por un lado, esos datos, que generalmente son usados sin su conocimiento o consentimiento y para enriquecer a otras compañías, ahora pueden brindar una ayuda real a otras personas. Pero, por otro lado, la situación actual llama la atención sobre «cuán granular puede ser esta recopilación de datos» y qué poco control tenemos sobre su recopilación, quién los obtiene y qué hacen esas compañías con ellos, opina Recode.

Mapa interactivo para ayudar en la lucha contra el virus

Para su análisis, Recode se centró en la empresa Unacast y su **Marcador de Distanciamiento Social** (Social Distancing Scoreboard, en inglés), un mapa interactivo que, basándose en los análisis de datos de la firma, **asigna calificaciones** a cada estado y condado en EE.UU., dependiendo de qué tan bien los residentes están practicando el distanciamiento social.

«Esta es una iniciativa pro bono. Son 25 científicos de datos que acumulan cinco años de trabajo y pasaron cuatro días preparando esto para ayudar con lo que está sucediendo», señaló la portavoz de Unacast, Jeanne Meyer.

Una forma en la que esos mapas podrían ayudar es al mostrar a los funcionarios de salud de qué manera otros estados o condados vecinos están obteniendo mejores calificaciones, lo que implicaría que su mensaje a los residentes locales sobre el distanciamiento social necesita ser mejorado.

No obstante, una cosa importante sobre este marcador es que, a diferencia de otros programas similares, no pregunta al usuario si quiere que se rastree su ubicación, ya que recopila los datos a partir de **varias fuentes de terceros**.

Según la política de privacidad de Unacast, estas fuentes incluyen a los socios de la compañía, así como el kit de desarrollo de software, o **SDK**, que se coloca en las aplicaciones. El SDK es un paquete de herramientas que, entre otras cosas, puede incluir formas de rastrear los datos del usuario e informarlos al proveedor del SDK, que en este caso es Unacast.

El problema es que cualquier usuario puede otorgar permiso a una de esas aplicaciones, para acceder a sus datos de ubicación, sin saber que tales datos también se enviarán a Unacast. Un análisis realizado por la compañía de inteligencia de aplicaciones móviles Apptopia **encontró el SDK de Unacast en todo tipo de 'apps' en iOS y Android**, incluyendo controles remotos de Smart TV, rastreadores de pasos, juegos, localizadores Wi-Fi gratuitos y pronosticadores del tiempo.

Una empresa desconocida que sabe mucho

De esta manera, resulta que una empresa de la que probablemente nunca haya oído hablar nadie, **tiene datos personales de los usuarios** como el identificador publicitario único de su dispositivo, o datos de ubicación lo suficientemente específicos como para detectar en qué restaurante de comida rápida se encuentra el dispositivo y cuánto tiempo lleva allí.

Los mapas de distanciamiento social de Unacast **no muestran individuos específicos**. Lo que el público ve es solo el análisis de esos datos, y todo se reduce a un nivel de condado. Sin embargo, la empresa **divulga parte de esta información a terceros**, aunque Unacast subraya que nunca comparte datos de identificación, como el nombre o dirección de correo electrónico.

«No hay forma de que alguien sepa que sus datos de ubicación se recopilan de una aplicación en particular y luego se venden a compañías [como Unacast]», señaló la

directora de privacidad del Centro de Internet y Sociedad de la Facultad de Derecho de Stanford, Jennifer King.

«Al menos ahora, tiene el derecho [en California] de solicitar que se eliminen datos de su conjunto, pero fundamentalmente deberíamos tener leyes que limiten la capacidad de terceros para recopilar sus datos de ubicación sin su consentimiento afirmativo», indicó King.

Para King, **los beneficios temporales de estos datos no superan las implicaciones de privacidad** a largo plazo. «El hecho de que podamos hacer mapas bonitos con los datos de las personas no significa que estamos obteniendo información útil o procesable a partir de ellos», señaló la experta.

«Me gustaría saber qué herramientas dicen los investigadores de salud pública que necesitan y que les ayudarían, en lugar de qué pueden preparar los científicos que tienen acceso a los datos de ubicación», concluyó King.

Cortesía de RT

Te podría interesar

Amnistía Internacional advierte el riesgo que supone la vigilancia de Google y Facebook

Google «El gran hermano»: conozca las formas en que se viola la privacidad de sus usuarios

---

Fuente: El Ciudadano