

<https://www.elcorreo.eu.org/El-Pentagono-mira-tus-citas>

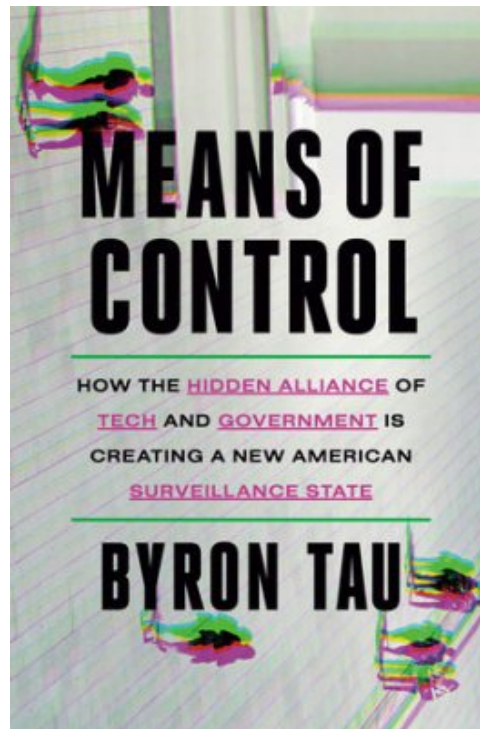
El Pentágono mira tus citas

- Cybersociété -

Date de mise en ligne : samedi 16 mars 2024

Copyright © El Correo - Tous droits réservés

El ecosistema de tecnología publicitaria es la mayor empresa de recopilación de información jamás concebida por los seres humanos. Y no fue construido por el gobierno. Cómo fue que las agencias de inteligencia estadounidenses le encontraron la vuelta para aprovechar al máximo esa fabulosa herramienta.



En su edición del 27 de febrero último la revista mensual estadounidense [Wired](#) (En línea), medio que desde su salida en 1993 se dedica a tomar nota de los impactos de la tecnología en todos los aspectos de la vida, publicó un adelanto del nuevo ensayo de [Byron Tau](#), periodista estadounidense de *The Wall Street Journal*. Su inquietante título es : « Medios de control : cómo la alianza oculta entre tecnología y gobierno está creando un nuevo Estado estadounidense de vigilancia » ([Means of Control : How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State](#)).

En la versión resumida de ese adelanto del libro de Tau -que sigue a continuación-, además de tomar nota de cómo aprendió el Pentágono a utilizar anuncios publicitarios personalizados para encontrar sus objetivos, se relata a través de hechos y personajes cómo fue que las agencias de inteligencia estadounidenses le encontraron la vuelta para aprovechar al máximo el ecosistema de tecnología publicitaria. Junto a los condimentos geopolíticos de indudable interés convive implícito un tema clave para nosotros. En efecto, se trata de una primera toma de vista de cómo todo esto va a impactar en el territorio digital de la política argentina. Son movimientos de las placas tectónicas que hacen a esta más que singular morfología edáfica.

La historia que cuenta Tau comienza en 2019 y trata de la empresa de recopilación de información más grande jamás concebida por el ser humano. Durante ese año, el contratista y tecnólogo del gobierno llamado [Mike Yeagley](#) comenzó a hacer rondas de entrevistas en Washington, DC. Tenía una advertencia contundente para cualquiera del *establishment* de seguridad nacional que quisiera escuchar : el gobierno de Estados Unidos tenía un problema con [Grindr](#) .

Grindr, una popular aplicación de citas y encuentros, se basaba en las capacidades de GPS de los teléfonos

inteligentes modernos para conectar potenciales parejas en la misma ciudad, vecindario o incluso edificio. La aplicación puede mostrar en tiempo real a qué distancia se encuentra una pareja potencial, hasta el metro de distancia. En sus 10 años de funcionamiento, *Grindr* acumuló millones de usuarios y se convirtió en un engranaje central de la cultura gay en todo el mundo.

Pero para Yeagley, explica Tau, *Grindr* era otra cosa : una de las decenas de miles de aplicaciones para teléfonos móviles diseñadas descuidadamente que filtraban cantidades masivas de datos al opaco mundo de los anunciantes en línea. Yeagley sabía que esos datos eran fácilmente accesibles para cualquier persona con un poco de conocimientos técnicos. Entonces Yeagley, de 40 años, cuya vida laboral había transcurrido casi sin excepción al servicio del gobierno, se empeñó en explicar la forma en que esos datos constituían un grave riesgo para la seguridad nacional.

Yeagley demostraba cómo se accedía a los datos de geolocalización de los usuarios de *Grindr* a través de un punto de entrada oculto pero ubicuo : los intercambios de publicidad que muestran los pequeños anuncios digitales en la parte superior de *Grindr*, y en casi todas las demás aplicaciones móviles y sitios web con publicidad. Esto fue posible gracias a la forma en que se vende el espacio publicitario en línea, a través de subastas casi instantáneas en un proceso llamado oferta en tiempo real. Esas subastas estaban plagadas de potencial de vigilancia.

Geocercas

Trabajando con datos de *Grindr*, Yeagley comenzó a dibujar [geocercas](#), creando límites virtuales en conjuntos de datos geográficos, alrededor de edificios pertenecientes a agencias gubernamentales que realizan trabajos de seguridad nacional. Eso le permitió a Yeagley ver qué teléfonos había en ciertos edificios en ciertos momentos y adónde fueron después. Estaba buscando teléfonos pertenecientes a usuarios de *Grindr* que pasaban el día en edificios de oficinas gubernamentales. Si el dispositivo pasaba la mayor parte de los días laborales en esas oficinas era muy probable que su propietario trabajara para una de esas agencias.

Luego empezó a observar el movimiento de esos teléfonos a través de los datos de *Grindr*. Cuando no estaban en sus oficinas, ¿adónde iban ? Un pequeño número de ellos se había quedado en las paradas de descanso de las autopistas en el área de DC al mismo tiempo y cerca de otros usuarios de *Grindr*, a veces durante la jornada laboral y a veces mientras estaban en tránsito entre instalaciones gubernamentales. Para otros usuarios de *Grindr*, podía inferir dónde vivían, ver adónde viajaban e incluso adivinar con quién estaban saliendo.

Escribe Tau con prosa preocupada que Yeagley, cotejó que toda esa información estaba disponible para la venta por poco dinero. Y no era sólo *Grindr*, sino cualquier aplicación que tuviera acceso a la ubicación precisa de un usuario : otras aplicaciones de citas, aplicaciones meteorológicas, juegos. Yeagley eligió *Grindr* porque generaba un conjunto de datos particularmente rico y su base de usuarios podría ser excepcionalmente vulnerable. Una empresa china había obtenido una participación mayoritaria en *Grindr* a partir de 2016, lo que aumentó los temores entre Yeagley y otros en Washington de que un enemigo geopolítico pudiera hacer un mal uso de los datos.

Del recontra espionaje

Pero el punto de Yeagley no era sólo argumentar en las conferencias que daba que los datos publicitarios presentaban una amenaza a la seguridad de Estados Unidos y la privacidad de sus ciudadanos. Era demostrar que estas fuentes también presentaban una enorme oportunidad en las manos adecuadas.

Tau manifiesta que cuando se habla con un grupo de agencias de inteligencia, no hay mejor manera de llamar su atención que mostrándoles una herramienta capaz de revelar cuándo sus agentes están visitando paradas de descanso en las rutas.

Mike Yeagley vio tanto las promesas como las trampas de los datos publicitarios porque, en primer lugar, había desempeñado un papel clave en llevar los datos publicitarios al gobierno. Su ronda de conferencias de 2019 fue un intento de crear conciencia entre las diversas y a menudo aisladas fuerzas laborales de la inteligencia estadounidense. Pero para entonces algunos rincones selectos del mundo de la inteligencia ya estaban muy familiarizados con su trabajo y lo utilizaban activamente.

Yeagley había pasado años trabajando como « explorador » tecnológico : buscando capacidades o conjuntos de datos que existían en el sector privado y ayudando a incorporarlos al gobierno. Había ayudado a ser pionero en una técnica que algunos de sus usuarios llegarían a llamar en broma « ADINT », un juego de palabras con la jerga de la comunidad de inteligencia para diferentes fuentes de inteligencia, como SIGINT (inteligencia de señales) que se convirtió en sinónimo del auge del descifrado de códigos y líneas telefónicas intervenidas en el siglo XX. También estaba la OSINT ([inteligencia de código abierto](#)) de la era de Internet, de la cual ADINT era una forma. Sin embargo, más a menudo ADINT era conocido en los círculos gubernamentales como datos de tecnología publicitaria.

Fue una revelación, especialmente por las filtraciones de [Edward Snowden](#), que las agencias de inteligencia pudieran simplemente comprar algunos de los datos que necesitaban directamente de entidades comerciales. Otro consultor tecnológico que trabaja en proyectos para el gobierno de Estados Unidos se lo explicó a Tau de esta manera : « El ecosistema de tecnología publicitaria es la mayor empresa de recopilación de información jamás concebida por los seres humanos. Y no fue construido por el gobierno ».

Funcionamiento

Apple o *Google* han proporcionado a todos los que poseen un teléfono *iPhone* o *Android* un ID de publicidad « anonimizado ». Ese número se utiliza para rastrear nuestro movimiento en el mundo real, nuestro comportamiento de navegación en Internet, las aplicaciones que instalamos en nuestro teléfono y mucho más. Las corporaciones más grandes de los Estados Unidos han invertido miles de millones de dólares en este sistema. Frente a un depósito de datos tan rico y detallado disponible comercialmente, los gobiernos del mundo han abierto cada vez más sus billeteras para comprar esta información de todos, en lugar de piratearla u obtenerla a través de órdenes judiciales secretas, informa Tau.

Para ilustrar como funciona, Tau invita a una mujer imaginaria llamada Marcela. Tiene un teléfono Google Pixel con la aplicación *Weather Channel* instalada. Mientras sale por la puerta para ir a correr, ve el cielo nublado. Entonces Marcela abre la aplicación para comprobar si el pronóstico anuncia lluvia.

Al hacer clic en el ícono azul de *Weather Channel*, Marcela desencadena un frenesí de actividad digital destinada a mostrarle un anuncio personalizado. Comienza con una entidad llamada intercambio de publicidad, básicamente un mercado masivo donde miles de millones de dispositivos móviles y computadoras notifican a un servidor centralizado cada vez que tienen un espacio publicitario abierto.

En menos de un abrir y cerrar de ojos, la aplicación *Weather Channel* comparte una gran cantidad de datos con este intercambio de anuncios, incluida la dirección IP del teléfono de Marcela, la versión de Android que está ejecutando, su operador, además de una serie de datos técnicos sobre cómo está configurado el teléfono, hasta qué resolución

está configurada en la pantalla. Lo más valioso de todo es que la aplicación comparte las coordenadas GPS precisas del teléfono de Marcela y el número de identificación de publicidad pseudoanonimizado que *Google* le ha asignado, llamado [AAID](#). (En los dispositivos Apple, se llama [IDFA](#)).

Para el profano, una identificación publicitaria es una serie de galimatías, algo así como « bdca712j-fb3c-33ad-2324-0794d394m912 ». Para los anunciantes, es una mina de oro. Saben que « bdca712j-fb3c-33ad-2324-0794d394m912 » posee un dispositivo *Google Pixel* con la aplicación *Nike Run Club*. Saben que « bdca712j-fb3c-33ad-2324-0794d394m912 » frecuenta *Runnersworld.com*. Y saben que « bdca712j-fb3c-33ad-2324-0794d394m912 » ha estado deseando un par de nuevos zapatos de carreras *Vaporfly*. Lo saben porque *Nike*, *Runnersworld.com* y *Google* están conectados al mismo ecosistema publicitario, todos destinados a comprender lo que les interesa a los consumidores. En la Argentina con el padrón electoral se harían un picnic.

Los anunciantes utilizan esa información a medida que dan forma y distribuyen sus anuncios. Con base en las enormes cantidades de datos que pueden extraer del éter, podrían crear una « audiencia », esencialmente una lista enorme de ID de anuncios de clientes que se sabe o se sospecha que están en el mercado que les interesa. Luego, en una subasta instantánea, automatizada y en tiempo real, los anunciantes le dicen a un intercambio de anuncios digitales cuánto están dispuestos a pagar para llegar a esos consumidores cada vez que cargan una aplicación o una página web. Sobre esta base se ha construido todo un modelo de negocio : extraer datos de las redes de ofertas en tiempo real, empaquetarlos y revenderlos para ayudar a las empresas a comprender el comportamiento del consumidor.

Existen algunos límites y salvaguardias para todos estos datos. Técnicamente, un usuario puede restablecer su número de identificación de publicidad asignado, aunque pocas personas lo hacen, o incluso saben que tienen uno. Y los usuarios tienen cierto control sobre lo que comparten a través de la configuración de su aplicación. Si los consumidores no permiten que la aplicación que están usando acceda al GPS, [Ad Exchange](#) no puede obtener la ubicación GPS del teléfono, por ejemplo. (O al menos se supone que no deben hacerlo. No todas las aplicaciones siguen las reglas y, a veces, no son examinadas adecuadamente una vez que están en las tiendas de aplicaciones).

El dato más valioso

La geolocalización es el dato comercial más valioso que surge de esos dispositivos. Comprender el movimiento de los teléfonos es ahora una industria multimillonaria, afirma Tau. Se puede utilizar para ofrecer publicidad dirigida según la ubicación para, por ejemplo, una cadena de restaurantes que quiera dirigirse a personas cercanas. Puede utilizarse para medir el comportamiento del consumidor y la eficacia de la publicidad. ¿Cuántas personas vieron un anuncio y luego visitaron una tienda ? Y los análisis se pueden utilizar para decisiones de planificación e inversión. ¿Cuál es la mejor ubicación para poner un nuevo local comercial ? ¿Habrá suficiente tráfico peatonal para sostener un negocio así ? ¿El número de personas que visitan un determinado minorista aumenta o disminuye este mes ?

Pero este tipo de datos sirven para otra cosa. Tiene un notable potencial de vigilancia. ¿Por qué ? « Porque lo que hacemos en el mundo con nuestros dispositivos no puede ser verdaderamente anónimo », explica Tau. El hecho de que los anunciantes conozcan a Marcela como « bdca712j-fb3c-33ad-2324-0794d394m912 » mientras la ven moverse por el mundo *online* y *offline* no le ofrece casi ninguna protección a su privacidad. En conjunto, sus hábitos y rutinas son exclusivos de ella. Nuestro movimiento en el mundo real es muy específico y personal para todos nosotros. El lugar donde pasa la mayor parte de las noches un teléfono es un buen indicador del lugar donde vive su propietario. Los anunciantes lo saben. Los gobiernos también lo saben.

Estás localizado

Afirma Tau que « si alguna vez le concedió permiso a una aplicación meteorológica para saber dónde se encuentra, es muy probable que se haya guardado un registro de sus movimientos precisos en algún banco de datos al que tienen acceso decenas de miles de desconocidos. Eso incluye a las agencias de inteligencia ». Según Tau el *Departamento de Seguridad Nacional* (DHS, por su sigla en inglés) ha adoptado con especial entusiasmo la operatoria de comprar este tipo de datos de tecnología publicitaria. Tres de sus componentes (la Oficina de Aduanas y Protección Fronteriza de EEUU, el Servicio de Inmigración y Control de Aduanas de EE. UU., y el Servicio Secreto de EE. UU), han comprado más de 200 licencias de proveedores comerciales de tecnología publicitaria desde 2019.

Usaron estos datos para encontrar túneles fronterizos y rastrear accesos no autorizados de inmigrantes y para resolver crímenes domésticos. En 2023, un auditor general del gobierno reconvino al DHS por el uso de tecnología publicitaria, diciendo que el departamento no contaba con salvaguardas de privacidad adecuadas y recomendando que los datos dejaran de usarse hasta que se elaboraran políticas. El DHS le dijo al auditor general que seguirían utilizando los datos. Las agencias de inteligencia de otros gobiernos también tienen acceso a estos datos y los venden a entidades de seguridad nacional y pública de todo el mundo.

Para recalcar que nada de esto es una preocupación abstracta, Tau refiere que en 2021 un pequeño blog católico conservador llamado [The Pillar](#) informó que [Jeffrey Burrill](#), el secretario general de la Conferencia de Obispos Católicos de EEUU, era un usuario habitual de *Grindr*. La publicación informó que Burrill « visitaba bares gay y residencias privadas mientras usaba una aplicación de conexión basada en la ubicación ». Describió su fuente como « registros disponibles comercialmente de datos de señal de aplicaciones obtenidos por *The Pillar* ».

Dice Byron Tau que « todos tenemos una vaga sensación de que nuestros operadores de telefonía móvil tienen estos datos sobre nosotros. Pero las autoridades generalmente necesitan obtener una orden judicial para conseguirlo. Y se necesitan pruebas de un delito para obtener tal orden. Éste es un tipo diferente de pesadilla sobre la privacidad ». Resta que la política argentina siga durmiendo en el territorio digital sin advertir lo que hace con esas pesadillas sobre la privacidad la derecha dura. Por lo visto está muy despierta.

Cristina Robles* para [¿Y ahora qué ?](#)

[¿Y ahora qué ?](#). Buenos Aires, 16 de marzo de 2024.