Ojo con espiar al cliente que se conecta a su wifi.

Protección de Datos ha puesto la lupa en el internet gratis a cambio de usar información con fines comerciales

Dos mujeres con sus ordenadores conversan en una cafetería de Madrid. VÍCTOR SAINZ

Por **Jorge Velasco**

La Agencia Española de Protección de Datos (AEPD) advirtió el pasado mes de mayo a las empresas sobre los riesgos que supone el uso del wifi *tracking* para la privacidad de las personas. Se trata de una tecnología que permite a las compañías identificar y rastrear los teléfonos y ordenadores que se conecten a su red wifi. Estos puntos gratuitos de conexión a internet son frecuentes en cafeterías, restaurantes museos, grandes eventos, pero también en espacios públicos, como aeropuertos o estaciones de tren. Una vez que las personas acceden a la red, las compañías tienen acceso a sus datos para estudiar las rutinas de los clientes y entender mejor el comportamiento de sus compradores. Pero, cuidado, porque los móviles u ordenadores de los usuarios albergan información privada. Y en caso de bucear más de la cuenta, los negocios pueden meterse en serios problemas legales.

Por ejemplo, a través del seguimiento que hacen las compañías se puede llegar a descubrir que un ciudadano acude frecuentemente a una clínica de reproducción asistida o a un centro oncológico, lo que supone una intromisión en su vida personal. "Localizar una ubicación precisa e inferir información sensible es un riesgo para la intimidad de las personas. Ni las empresas ni la Administración pública deberían poder rastrear qué centros sanitarios, comercios o lugares de culto visita una persona. Esos datos deben permanecer en su esfera privada", señala Paula Garralón, abogada de comercial, privacidad y protección de datos de Bird & Bird.

A pesar de que la técnica del wifi *tracking* navega en aguas legales revueltas, lo cierto es que no es una práctica prohibida. Eso sí, las compañías deberán cumplir una serie de condiciones si quieren utilizar esta tecnología para pescar clientela. El requisito más importante es que garanticen que la información que recopilan, como el número de visitas diarias al establecimiento o las áreas en las que se concentra el mayor número de usuarios, sea anónima. Como confirma Juan Ramón Robles, abogado experto en tecnología y protección de datos de Hogan Lovells, esta tecnología es lícita siempre y cuando los datos recabados se "aglutinen de forma agregada" y no individualizada.

Además, las empresas deben asegurarse de que cuentan con el consentimiento de las personas para recabar sus datos. Si quieren evitar una ola de reclamaciones también tendrán que informar debidamente a los consumidores sobre las condiciones que imponen para utilizar su wifi. Por ejemplo, "te dejo usar mi red a cambio de usar tus datos para enviar promociones". Para ello, precisa Daniel López, socio experto en protección de datos y privacidad en Écija, es obligatorio "disponer de mecanismos informativos, fácilmente accesibles por los usuarios", tales como "formularios de registro, carteles en los espacios donde se desarrollará el wifi *tracking* o a través de aplicaciones corporativas en las que se informe al usuario sobre la política de uso de la compañía para conectarse a la red", ejemplifica el abogado.

Las compañías tienen que cumplir también un último requisito. Solo podrán recoger aquella información que sea necesaria para sus fines comerciales. Un ejemplo de información útil sería el tiempo que los consumidores pasan en una tienda. Por el contrario, utilizar la red de conexión wifi para cotillear los pasos de las personas que se conectan a su red está prohibido. En caso de no cumplir con los requisitos (datos anónimos, interés y transparencia), el reglamento de protección de datos castiga a los infractores con multas que pueden poner en riesgo la estabilidad del negocio.

> **El requisito más importante para las empresas es garantizar el anonimato de todo el conocimiento que obtienen**

Solo hay una excepción para poder utilizar la información privada sin sufrir un perjuicio económico: si está en riesgo la seguridad de las personas. Este método, señala la Agencia Española de Protección de Datos en su guía sobre el tratamiento del wifi *tracking* "será válido para solventar situaciones en las que los intereses vitales de los ciudadanos estuvieran realmente en peligro, tales como emergencias, auxilio o búsqueda y rescate de personas desaparecidas". En cuyo caso, advierte Daniel López, "es imprescindible presentar un análisis que justifique que es realmente necesario acceder a los datos".

Un arma de doble filo

Pese a que se trata de un buen sistema para impulsar el negocio, también es un arma de doble filo. Los expertos advierten que utilizar el wifi *tracking* es arriesgado si no se toman las debidas cautelas. Los negocios que se enganchan a los móviles de los viandantes sin su consentimiento están cruzando una línea roja que afecta a sus derechos. Especialmente, cuando las empresas acceden a una información que toca de lleno la intimidad de las personas. Otro problema es que las empresas desconocen *a priori* el tipo de información al que van a tener acceso y eso implica un riesgo en la privacidad de los usuarios. "Existen datos que identifican unívocamente a cada dispositivo, por lo que es posible llegar a saber quién es la persona que hay detrás de los aparatos tecnológicos", advierte Juan Ramón Robles.

Por último, no hay que perder de vista que los datos recabados a través de esta técnica pueden ser muy golosos para los *hackers* o piratas informáticos. Un pequeño agujero en el sistema de seguridad puede exponer miles de datos confidenciales. Por ello, las empresas usuarias de este sistema deben cerciorarse de que cuentan con un sistema de seguridad óptimo, porque un robo de información puede suponer importantes problemas para los usuarios, como la usurpación de su identidad o la pérdida de confidencialidad de datos sujetos a secreto profesional o sobre su vida sexual o su situación económica.

CLAVES

Acciones legales y sanciones

En caso de que las empresas vulneren el derecho a la privacidad o a la intimidad, los usuarios podrán emprender acciones legales. Si se demuestra que los negocios no han recibido el consentimiento de los usuarios para recoger los datos o han obtenido información confidencial, los afectados podrán reclamar ante la Agencia Española de Protección de Datos (AEPD). El régimen sancionador es muy riguroso. Según Paula Garralón, abogada de comercial, privacidad y protección de datos de Bird & Bird, las multas a las compañías oscilan desde "40.000 euros hasta los 20 millones". En los casos más graves, pueden recibir una sanción "equivalente al 4% del volumen de negocio total que la empresa haya generado durante el ejercicio financiero anterior", señala esta experta.