Datuak Babesteko
Euskal Agintaritza

Autoridad Vasca de
Protección de Datos

Exp.: CN24-007

DICTAMEN Nº D24-018

DICTAMEN RELATIVO A LA UTILIZACIÓN DE DATOS PROVENIENTES DE LA RED WIFI MUNICIPAL EXTERNA DEL AYUNTAMIENTO DE BILBAO

ANTECEDENTES

PRIMERO: Por la Delegada de Protección de Datos del Ayuntamiento Bilbao se ha solicitado informe de la Autoridad Vasca de Protección de Datos, en los siguientes términos:

> *"El objeto de la presente consulta a la Autoridad Vasca de Protección de Datos es confirmar si es conforme a la normativa de protección de datos (o si no le es de aplicación) el nuevo tratamiento que se está planteando con los datos recabados por la red Wifi gratuita, libre y universal de la ciudad de Bilbao.*
>
> *Se pretende utilizar la información sobre el movimiento de los dispositivos móviles conectados a la red WIFI municipal a lo largo del tiempo a fin de identificar las tendencias de movilidad urbana, zonas de aglomeraciones en función de factores externos (festivos, eventos especiales, …), zonas comerciales en función de campañas u otros parámetros.*
>
> *Para ello, a la presente consulta se adjunta "Informe técnico sobre la utilización de datos provenientes de la red WIFI" de la ciudad de Bilbao redactado por BILBAOTIK, S.A. en el cual se hace un análisis acerca del objeto del tratamiento que se pretende realizar de los datos provenientes de la red WIFI municipal, así como un análisis técnico de dicha red WIFI en el que se analizan las medidas técnicas y organizativas adoptadas por el Ayuntamiento de Bilbao.*
>
> *Esperando recibir respuesta por parte de la AVPD en relación con:*
>
> *1. Si le es de aplicación la normativa vigente en materia de protección de datos o bien no lo es al tratarse de datos completamente anonimizados.*
>
> *2. De ser de aplicación, si el tratamiento que se plantea en el informe se ajusta a la normativa.*
>
> *3. Cualquier recomendación que pudieran realizar a nivel de medidas técnicas organizativas".*

SEGUNDO: Corresponde a esta Autoridad Vasca de Protección de Datos la emisión del dictamen en respuesta a la consulta formulada en cumplimiento de lo establecido en el artículo 6 de la Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos y en el artículo 58.3 b) del Reglamento General de Protección de Datos (RGPD).

CONSIDERACIONES

I

La consulta parte de que el Ayuntamiento de Bilbao tiene conocimiento de las orientaciones para responsables de tratamiento en relación con las tecnologías de seguimiento Wi-Fi elaboradas conjuntamente por las cuatro autoridades de control (Agencia Española Protección de Datos, Autoridad Catalana de Protección de Datos, Autoridad Vasca de Protección de Datos, y el Consejo de Transparencia y Protección de Datos).

Estas orientaciones analizan tanto técnica como jurídicamente las implicaciones de la utilización de la tecnología de seguimiento Wi-fi o Wi-fi tracking, identifican los principales riesgos asociados a la misma y ofrecen una serie de recomendaciones concretas para un uso responsable y compatible con la normativa de protección de datos.

Por tanto, a dichas orientaciones nos remitiremos en lo no indicado expresamente en este dictamen.

Lo primero a considerar es si los datos recabados por la red Wifi municipal de Bilbao de los dispositivos móviles conectados a dicha red constituyen un dato personal a la luz del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD o Reglamento General de Protección de Datos).

Según el informe que se acompaña a la consulta, la información obtenida sobre el posicionamiento Wifi registra en lo esencial "el identificador anónimo del dispositivo, la fecha y hora, y la Antena Wifi a la que está conectado"

El artículo 4. 1) del RGPD define el **dato personal** en los siguientes términos:

> *"«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".*

El RGPD, en su Considerando 30, advierte de la capacidad de identificar a las personas a través de las huellas de los dispositivos: "*Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos [...] Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas*".

Asimismo el Dictamen 2/2013 del anterior Grupo del Art. 29 sobre aplicaciones de los dispositivos inteligentes de 27 de febrero de 2013 ya establecía:

> *"Son datos personales cuando se refieren a una persona que es identificable directamente (p. ej., por su nombre) o indirectamente por el responsable del tratamiento o un tercero. Los datos pueden referirse al propietario del dispositivo o a cualquier otra persona como ocurre, por ejemplo, con los datos de contacto de amigos que contiene el libro de direcciones. Los datos pueden recopilarse y procesarse en el dispositivo o, una vez transferidos, en otro lugar mediante infraestructuras de los*

desarrolladores de aplicaciones o de terceros, a través de la conexión a una API externa, en tiempo real y sin el conocimiento del usuario final".

Y como ejemplos de esos datos personales que pueden incidir significativamente en la vida privada de los usuarios y otras personas se mencionaban en este Dictamen 2/2013 la localización o los identificadores únicos del dispositivo y del cliente.

Por tanto, los datos transmitidos por las señales Wi-Fi utilizados en este tipo de procesos pueden ser considerados como datos personales en la medida en que están relacionadas con personas identificables y son susceptibles de ser utilizados para su identificación directa o indirecta.

Según se expone en la consulta, entre la información obtenida por la red Wifi municipal se encuentra el identificador del dispositivo (dirección MAC).

Y esta dirección MAC, que identifica al dispositivo, puede ser la que le haya asignado el fabricante (MAC de fábrica) o una MAC aleatoria que el propio dispositivo genera cada vez que se intenta conectar a una red Wifi.

Aun en este último caso, mientras el dispositivo esté conectado a la red Wifi, la dirección MAC se mantiene constante durante toda la conexión, lo que puede permitir vincular las acciones realizadas por el dispositivo durante toda la conexión (localización absoluta y relativa con la localización de otros terminales), y permitir la identificación mediante técnicas ya existentes.

Además cuando se mantenga el ámbito espacial y temporal de los datos recogidos mediante Wi-Fi tracking, éstos pueden ser suficientes por sí solos o en combinación con otros para permitir la identificación de las personas.

El informe que se acompaña a la consulta entiende que el identificador del dispositivo que registra la red Wifi municipal (junto con la posición y fecha/hora) no constituye dato personal en base a que un porcentaje del 90% de los dispositivos se conectan con una MAC aleatoria, y que hay una anonimización posterior de todos los identificadores mediante un algoritmo que no tiene vuelta atrás.

Si existe un proceso de anonimización, vinculando el identificador del dispositivo con un número aleatorio, tal y como expone el informe es porque se parte de un conjunto de datos personales, en este caso, los identificadores de los dispositivos (las direcciones MAC) para conseguir, a través de ese proceso de anonimización, un conjunto de datos anónimos.

Y a partir de que los datos se conviertan en anónimos no le será de aplicación los principios de protección de datos ya que el interesado no será identificable, o dejará de serlo (Considerando 26 RGPD).

Y asimismo el RGPD en el artículo 4.2) define así el **tratamiento**:

"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

La obtención o recogida de información de los dispositivos por la red Wifi municipal, así como el propio proceso de anonimización, y su posterior utilización para los fines indicados

en la consulta en el caso de que se llegase a materializar el riesgo de reidentificación, constituyen tratamientos de datos personales.

El informe que se acompaña a la consulta no indica cuál es el periodo de conservación de la información recopilada y anonimizada. Se debe tener en consideración que puede que la reidentificación no sea factible hoy con el conjunto de los medios que puedan ser razonablemente utilizados en la actualidad, pero si el periodo de conservación previsto es amplio, el responsable del tratamiento debe tener en cuenta que los progresos tecnológicos pueden facilitar la reidentificación.

II

Cualquier tratamiento de datos personales debe adecuarse a los principios establecidos en el artículo 5 RGPD y cumplir con alguna de las condiciones de licitud enumeradas en el artículo 6 RGPD, lo que es aplicable al Wi-Fi tracking en los casos en los que el responsable del tratamiento opte por una opción tecnológica que haga posible dicho tratamiento.

El tratamiento deberá ser leal y transparente, debiendo quedar totalmente claro para las personas qué datos y cómo se están tratando mediante Wi-Fi tracking y proporcionar dicha información de forma fácilmente accesible y fácil de entender, con independencia de las dificultades técnicas o prácticas que el Wi-Fi tracking pueda suponer al responsable del tratamiento para el cumplimiento de estos principios.

Los fines del tratamiento mediante Wi-Fi tracking deben ser explícitos, es decir, deben indicarse claramente, deben ser legítimos y deben comunicarse a las personas interesadas, a más tardar, en el momento de la recogida.

Adicionalmente, los datos recogidos para una finalidad concreta mediante Wi-Fi tracking no podrán ser utilizados para una finalidad posterior que sea incompatible.

El responsable del tratamiento, además de cumplir con los principios recogidos en el RGPD y ser capaz de demostrarlo, deberá asegurarse que el tratamiento cumple con alguna de las condiciones de licitud establecidas en el artículo 6.1 RGPD.

No obstante, antes de determinar o considerar la aplicación de cualquier condición de licitud, es importante recordar que los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios.

Tal y como se indica en la consulta, se pretende utilizar la información sobre el movimiento de los dispositivos móviles conectados a la red Wifi municipal a lo largo del tiempo a fin de identificar las tendencias de movilidad urbana, zonas de aglomeraciones en función de factores externos (festivos, eventos especiales,…), zonas comerciales en función de campañas u otros parámetros.

Hay que tener en cuenta que para cumplir con el principio de limitación de la finalidad los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

El cumplimiento del principio de limitación de la finalidad hace necesaria una mayor concreción de la finalidad pretendida con el tratamiento, en lo relativo al tiempo de conservación, los factores externos y la posibilidad que se deja sin mayor concreción con expresiones como “otros parámetros”.

En lo relativo al cumplimiento del principio de licitud, la base legitimadora aplicable a cada tratamiento requiere de un análisis pormenorizado del caso concreto por parte del responsable del tratamiento, en virtud del principio de responsabilidad proactiva (artículo 5.2 RGPD), que tendrá en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento.

El tratamiento pretendido deberá ampararse en alguna de las bases jurídicas contempladas en el artículo 6.1 del RGPD, y teniendo en cuenta que el responsable del tratamiento es una Administración Pública estas bases jurídicas quedarían reducidas a:

- El cumplimiento de una obligación legal aplicable al responsable del tratamiento (artículo 6.1 c) RGPD). Esta base requiere que el Derecho de la Unión o una norma con rango de ley exigiese al responsable el cumplimiento de una finalidad para la que sea necesario el empleo de las técnicas de Wi-Fi tracking.
- El cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (art 6.1 e) RGPD). El responsable del tratamiento deberá identificar la norma con rango de ley o el Derecho de la Unión que le atribuya una competencia concreta en la que pueda demostrar que dicho tratamiento mediante Wi-Fi tracking es necesario y proporcionado para realizar una misión de interés público o para ejercer poderes públicos.
- Proteger intereses vitales del interesado o de otra persona física (art. 6.1 d) RGPD). Esta condición de licitud solo podría aplicarse cuando el tratamiento fuese necesario para proteger la vida o la integridad física de una persona. En principio el tratamiento de datos personales en el contexto de Wi-Fi tracking difícilmente podría justificarse por estas razones. Sin embargo, no puede descartarse por completo su aplicación en situaciones en las que los intereses vitales estuvieran realmente en peligro, tales como emergencias, auxilio o búsqueda y rescate de personas desaparecidas lo que requeriría de un riguroso análisis del caso concreto que justificara su aplicación.

III

Una de las obligaciones contempladas por el RGPD es la relativa a la realización por el responsable de una evaluación de impacto relativa a la protección de datos personales (EIPD), tal y como se contempla en sus artículos 35 y 36, evaluación que será necesaria para aquellos casos en que el tratamiento entrañe un alto riesgo.

Para los tratamientos que incorporen la tecnología Wi-Fi tracking, como para cualquier otro tratamiento, la evaluación de riesgos y la evaluación de la necesidad de realizar una EIPD debe considerarse teniendo en cuenta el tratamiento en su conjunto, esto es, teniendo en cuenta su propósito, su naturaleza, su ámbito o alcance y su contexto.

De acuerdo con el artículo 35.3 del RGPD, en aquellos tratamientos que incorporen Wi-Fi tracking y que supongan una observación sistemática a gran escala de una zona de acceso público, la EIPD será obligatoria. Aunque el responsable del tratamiento no pretenda realizar tal observación sistemática a gran escala, la EIPD también será obligatoria, pues a la vista del riesgo inherente del tratamiento estaríamos hablando de un tratamiento de alto riesgo y, en consecuencia, le aplican las exigencias del RGPD para dichos tratamientos. Igualmente, deberá considerarse como un agravante, debido a la propia naturaleza de

muchas de las operaciones que forman parte del Wi-Fi tracking, que resultará más difícil para los interesados el ejercicio de sus derechos.

Si el tratamiento cumple con dos o más criterios de la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4) publicada por la AEPD y por la AVPD, también será necesaria realizar una EIPD.

La primera medida en el proceso de una EIPD es la obligación de realizar una evaluación de la necesidad y proporcionalidad del tratamiento en relación con la finalidad que se persigue, e implica realizar una ponderación atendiendo a tres criterios: juicio de idoneidad, juicio de necesidad y juicio de proporcionalidad en sentido estricto. Esta evaluación debe terminar con una decisión sobre si llevar o no el tratamiento, o en su caso, modificarlo hasta que supere el análisis del triple juicio antes señalado. El responsable deberá optar por la opción menos intrusiva para la privacidad y que implique menos riesgos para las personas.

Además, dentro este proceso de realización de una EIPD, y siendo el responsable una Administración Pública podría ser oportuno llevar a cabo un procedimiento de participación para que la ciudadanía afectada pudiera expresar su opinión al respecto, cuando se trate de actuaciones realizadas al amparo de las letras c) y e) del artículo 6.1 RGPD.

IV

En cuanto a las recomendaciones que pudiera realizar esta Autoridad a nivel de medidas técnicas y organizativas apropiadas al tratamiento pretendido, hay que destacar que el seguimiento WiFi o Wifi tracking plantea serios riesgos para la privacidad, ya que puede permitir el seguimiento de los movimientos de las personas sin que medie acción ni conocimiento por parte de éstas y sin una base jurídica apropiada. Las citadas orientaciones para responsables de tratamiento sobre tecnologías de seguimiento Wi-Fi elaboradas por las cuatro autoridades de control detallan en su apartado octavo las medidas técnicas y organizativas a aplicar.

Respecto al proceso de anonimización, convendría que éste se lleve a cabo mediante un proceso que sea no reversible, que en ningún momento la versión anonimizada de la dirección MAC pueda permitir encontrar la dirección MAC original. El informe que se acompaña a la consulta no llega a detallar la tecnología empleada para anonimizar (sustitución por otro código único que se guarda en una base de datos cifrada a la que nadie tiene acceso).

Estas son las consideraciones que realiza la Autoridad Vasca de Protección de Datos en relación con la consulta planteada, remitiéndonos asimismo a las orientaciones publicadas por esta Autoridad junto con las demás Autoridades de Control.

En Vitoria-Gasteiz, 10 de octubre de 2024