TECNOLOGÍAS DE SEGUIMIENTO WI-FI:

Orientaciones para responsables del tratamiento

aepd agencia española protección datos

apdcat Autoritat Catalana de Protecció de Dades

Datuak Babesteko Euskal Agintaritza
Autoridad Vasca de Protección de Datos

Consejo de Transparencia y Protección de Datos de Andalucía

Guía publicada en
mayo 2024

RESUMEN EJECUTIVO

El seguimiento Wi-Fi o Wi-Fi tracking, es una tecnología que permite identificar y rastrear dispositivos móviles a través de las señales Wi-Fi que estos emiten, para detectar la presencia del dispositivo en una zona específica y para identificar patrones de movimiento, por lo que es empleada, por ejemplo, en la estimación de aforos, el análisis de flujos de personas o la medición de tiempos de permanencia.

Pueden encontrarse aplicaciones prácticas en centros comerciales, museos, lugares de especial interés, centros de trabajo, áreas públicas, transporte público o grandes eventos públicos. Sin embargo, esta práctica 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 la misma y sin una base jurídica apropiada.

Es crucial tomar conciencia de que muchos de estos usos de Wi-Fi tracking implican la recogida y otros tratamientos de datos personales y, por tanto, deben someterse al conjunto de principios, derechos de las personas físicas y obligaciones para los responsables del tratamiento establecidos en el RGPD.

Las orientaciones analizan tanto técnica como jurídicamente las implicaciones de la utilización de esta tecnología, 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.

Estas orientaciones han sido elaboradas conjuntamente por la Agencia Española de Protección de Datos, la Autoridad Catalana de Protección de Datos, la Autoridad Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía y surgen fruto de la colaboración de las cuatro autoridades de control ante el impacto que un uso inadecuado de la tecnología Wi-Fi tracking puede tener en la privacidad y protección de datos de las personas físicas.

ÍNDICE

1. INTRODUCCIÓN 8

2. DESCRIPCIÓN DEL MARCO TECNOLÓGICO 10

A. EL USO DE DIRECCIONES MAC FIJAS Y ALEATORIAS 10

B. DATOS DE EMPLEADOS EN WI-FI TRACKING 11

C. IDENTIFICACIÓN DE DISPOSITIVOS 13

3. DATOS PERSONALES Y TRATAMIENTOS INVOLUCRADOS 14

A. ALCANCE DEL TÉRMINO "DATO PERSONAL" 14

B. WI-FI TRACKING Y EL "FINGERPRINTING" COMO DATOS PERSONALES 16

C. WI-FI TRACKING Y DATOS DE LOCALIZACIÓN Y DE TRAYECTORIAS 17

D. TRATAMIENTO DE DATOS PERSONALES 17

4. BASES LEGITIMADORAS DE TRATAMIENTOS DE DATOS PERSONALES 18

A. CONSENTIMIENTO (ARTÍCULO 6.1.A DEL RGPD) 19

B. EJECUCIÓN DE UN CONTRATO (ARTÍCULO 6.1.B DEL RGPD) 20

C. CUMPLIMIENTO DE UNA OBLIGACIÓN LEGAL (ARTÍCULO 6.1.C DEL RGPD) 20

D. PROTECCIÓN DE INTERESES VITALES (ARTÍCULO 6.1.D DEL RGPD) 20

E. INTERÉS PÚBLICO O EJERCICIO DE INTERESES PÚBLICOS (ARTÍCULO 6.1.E DEL RGPD) 21

F. INTERESES LEGÍTIMOS (ARTÍCULO 6.1.F DEL RGPD) 21

5. RIESGOS PARA LOS DERECHOS Y LIBERTADES DE LAS PERSONAS FÍSICAS 23

A. IMPACTO SOBRE LA INTIMIDAD DE LAS PERSONAS 24

B. INTROMISIÓN EN EL DOMICILIO O ZONAS PÚBLICAS 25

C. ESCALA DEL TRATAMIENTO Y LIMITACIÓN DE LIBERTAD DE CIRCULACIÓN 25

D. SEGUIMIENTO POR OMISIÓN: INTROMISIÓN EN LA LIBERTAD RELIGIOSA O EL TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS 26

E. LIBERTAD PERSONAL Y AUTOCENSURA 27

F. EL IMPACTO DE LA REIDENTIFICACIÓN 27

G. RIESGOS ASOCIADOS A LOS DATOS DE LOCALIZACIÓN 29

H. FALTA DE UNA CAPACIDAD DE "ACCOUNTABILITY" DE LOS MEDIOS 30

I. ESCENARIOS DE BRECHAS DE DATOS PERSONALES 31

J. TRANSFERENCIAS INTERNACIONALES Y EL CONTEXTO NORMATIVO INTERNACIONAL 32

K. CONCLUSIÓN SOBRE LA GESTIÓN DE RIESGO 33

6. OBLIGACIÓN DE LLEVAR A CABO UNA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS 33

7. EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO 35

A. EVALUACIÓN OBJETIVA DE LA IDONEIDAD DEL TRATAMIENTO 36

B. EVALUACIÓN OBJETIVA DE LA NECESIDAD DEL TRATAMIENTO DE DATOS PERSONALES 36

8. MEDIDAS TÉCNICAS Y ORGANIZATIVAS APROPIADAS 37

A. ANONIMIZACIÓN 39

B. ENMASCARAMIENTO DE DIRECCIONES MAC Y METADATOS 40

C. DESVINCULACIÓN 41

D. AGREGACIÓN 41

E. MINIMIZACIÓN DE DATOS 41

F. PLAZO DE CONSERVACIÓN DE LOS DATOS 42

G. MEDIDAS DE SEGURIDAD Y AUDITORÍA POR TERCEROS 42

H. MEDIDAS ORGANIZATIVAS 43

I. GESTIÓN CONTINUA DEL RIESGO 44

9. TRANSPARENCIA E INFORMACIÓN 44

A. INFORMACIÓN POR CAPAS 45

10. EJERCICIO DE DERECHOS RECONOCIDOS EN EL RGPD 46

A. DERECHO DE ACCESO (ARTÍCULO 15 RGPD) 47

B. DERECHO DE SUPRESIÓN (ARTÍCULO 17 RGPD) 47

C. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO (ARTÍCULO 18 RGPD) 48

D. DERECHO A LA PORTABILIDAD DE LOS DATOS (ARTÍCULO 20 RGPD) 49

E. DERECHO DE OPOSICIÓN (ARTÍCULO 21 RGPD) 49

F. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES (ARTÍCULO 22 RGPD) 49

11. REGLAMENTO DE INTELIGENCIA ARTIFICIAL 50

ACRÓNIMOS

AP: "Access Point". Punto de acceso Wi-Fi

CEPD: Comité Europeo de Protección de Datos

CNIL: Comisión Nacional de Informática y Libertad de Francia

DPD: Delegado de protección de datos

EEE: Espacio Económico Europeo

EIPD: Evaluación de impacto relativa a la protección de datos

ENS: Esquema Nacional de Seguridad

GT29: Grupo de trabajo del artículo 29

IA: Inteligencia artificial

IEEE: "Institute of Electrical and Electronics Engineers"

IOT: "Internet of things". Internet de las cosas

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

MAC: "Media Access Control"

RGPD: Reglamento General de Protección de Datos

RIA: Reglamento de Inteligencia Artificial

RSSI: "Received Signal Strength Indicator". Indicador de fuerza de la señal recibida

WPS: "Wifi Protected Setup"

1. INTRODUCCIÓN DE LA GUÍA

Actualmente el teléfono móvil es un dispositivo personal omnipresente equipado con diversas tecnologías inalámbricas como Wi-Fi y Bluetooth, además de admitir generaciones presentes y pasadas de tecnologías de redes móviles (es decir, 2G–5G).

Para llevar a cabo las comunicaciones, todas estas tecnologías se basan en el intercambio de mensajes entre dichos dispositivos y otros equipos de red como estaciones base y puntos de acceso.

En particular, la tecnología Wi-Fi es una tecnología inalámbrica basada en protocolos de comunicación estandarizados (familia de protocolos IEEE802.11), caracterizada por un conjunto de terminales (móviles o no) que se conectan a un "Punto de Acceso" (AP, por sus siglas en inglés). Un conjunto de AP administrado bajo una misma entidad conforma una red Wi-Fi.

La comunicación Wi-Fi se realiza a través de mensajes denominados "tramas", un conjunto de bytes que siempre contiene una cabecera que incluye el identificador del dispositivo de origen denominado dirección MAC (Media Access Control). Algunas de estas tramas no se encuentran cifradas y se emiten desde el dispositivo de forma periódica, incluso cuando el mismo no se haya conectado a ninguna red Wi-Fi.

Los datos que contienen dichas tramas, empleando diversas tecnologías disponibles actualmente, pueden ser capturados, analizados y procesados para determinar un identificador que permita singularizar al terminal origen de dichas tramas. Al igual que ocurre en el mundo de Internet, este conjunto de tecnologías se conoce como "device fingerprinting", o simplemente "fingerprinting", en español, huella digital del dispositivo o huella del dispositivo. A lo largo del texto se utilizarán indistintamente estas denominaciones.

La información empleada para la determinación de esta huella digital es enviada por el dispositivo sin que medie acción ni conocimiento por parte de la persona portadora del mismo, lo que hace que estas tecnologías sean especialmente delicadas desde la perspectiva de la privacidad y la protección de datos.

> Mediante la construcción, almacenamiento y análisis de esta huella, es posible la detección de la presencia del dispositivo en una determinada zona y la identificación de patrones de movimiento del mismo y por tanto, de la persona que lo porta.

Este tipo de tecnologías que recogen datos de los mensajes Wi-Fi intercambiados entre terminales y APs, para un posterior procesamiento y análisis se denominan "Wi-Fi tracking".

Los dos tipos principales de analíticas ofrecidas por estas tecnologías son la de presencia y la de localización. La analítica de presencia se centra en el estudio de la existencia de los terminales en una determinada zona y su duración en la misma, mientras que la de localización tiene como objetivo trazar el recorrido seguido por el terminal dentro de una zona de estudio.

Entre sus usos principales pueden mencionarse la estimación de aforos, el análisis de flujos de personas, el cálculo de estadísticas de asistencia y de tiempos medios de permanencia en ubicaciones concretas o de espera en una cola, la determinación de los recorridos más habituales o el cálculo de la tasa de repetición de visitas.

Pueden encontrarse aplicaciones prácticas de las mismas en **centros comerciales, museos, lugares de especial interés, centros de trabajo, áreas públicas, transporte público, grandes eventos públicos, escenarios de emergencias, etc**.

Dependiendo de las características de la huella digital generada por estas tecnologías, del tiempo de almacenamiento y de su procesado, el uso de Wi-Fi tracking puede suponer un tratamiento de datos personales, en ocasiones no solo desconocido por el usuario del terminal, sino también por el propio responsable del tratamiento, en la medida que entienda que no se trata de un dato personal, lo que puede ser erróneo, tal y como se explica en el apartado 3.

A la hora de plantearse desplegar este tipo de tecnologías, **la privacidad de las personas debe ser lo primero**.

Todas las personas deben tener derecho a moverse libremente sin "sentirse espiados", sin que un tercero, ya sea administración pública o empresa privada, pueda observar o llevar un registro de lo que están haciendo.

Nadie debería poder rastrear qué tiendas, centros sanitarios o lugares de culto visita una persona. Estos datos deben permanecer en su esfera privada, para que pueda ser ella misma, sin sentirse cohibida por un posible registro o utilización de dicha información[1].

Las presentes orientaciones analizan tanto técnica como legalmente las implicaciones de la utilización de esta tecnología, 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.

[1] https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_en

2. DESCRIPCIÓN DEL MARCO TECNOLÓGICO

A. EL USO DE DIRECCIONES MAC FIJAS Y ALEATORIAS

La **dirección MAC es un identificador generalmente fijo y unívoco de todo dispositivo**, usado en las comunicaciones entre los distintos elementos de una red.

Cuando un dispositivo se conecta a un AP de una red Wi-Fi, todos sus mensajes se inician identificando la dirección MAC del propio dispositivo. De esta forma, el AP puede leer el contenido de las tramas, y mediante la dirección MAC, identificar unívocamente al terminal.

La cobertura de las redes Wi-Fi la proporcionan los APs que la conforman. Estos APs pueden estar ubicados en espacios públicos abiertos o en el interior de edificios o instalaciones.

Sin embargo, la mayoría de los terminales móviles que entran en la zona de cobertura de las redes Wi-Fi no se conectan a ellas. Aun así, los dispositivos que disponen de capacidad Wi-Fi realizan una búsqueda periódica de las redes que pudieran estar disponibles en su radio de cobertura. Esta búsqueda se realiza mediante el envío periódico de tramas denominadas "Probe Request" que el dispositivo transmite aunque no esté conectado a una red Wi-Fi y en ocasiones ni siquiera activada la funcionalidad Wi-Fi. La finalidad principal de este tipo de tramas es enviar una "solicitud de sondeo" a las distintas redes Wi-Fi que puedan existir en la zona. Los APs están preparados para responder a dichos mensajes, enviando al terminal información que le permitirá conectarse a la misma si así lo elige el usuario.

Hace unos años, en las tramas Probe Request, además de determinada información técnica, se enviaba la dirección MAC fija y única del terminal. Por tanto, mediante la recolección en el tiempo de dichas tramas junto con tecnologías de localización era posible identificar unívocamente al terminal mediante dicho identificador y registrar su recorrido dentro de la zona de cobertura de la red Wi-Fi aun sin estar conectado a la misma.

Debido a los problemas de privacidad que esta situación planteaba, los fabricantes de terminales móviles incorporaron el uso de la dirección MAC aleatoria de forma generalizada. Este proceso se inició en los Apple iOS8 y fue seguido y extendido por Android.

La dirección MAC aleatoria es una dirección "virtual" empleada en las tramas Probe Request. De esta forma, distintos mensajes enviados desde un terminal no comparten el mismo identificador único (dirección MAC fija) y por tanto ya no resulta posible conocer la dirección MAC real del dispositivo capturando mediante el análisis de las tramas Probe Request. Por otra parte, dado que la dirección MAC aleatoria es modificada con frecuencia y las propias tramas son enviadas de forma aleatoria, tampoco resulta sencillo identificar el dispositivo utilizando directamente las direcciones MAC aleatorias.

Esta medida **fortaleció la privacidad de las personas**, no obstante, hay que **tener en cuenta los siguientes factores**:

- El procedimiento de generación de MAC aleatorias no está estandarizado, lo que conlleva comportamientos dispares entre los terminales.
- Una vez se ha efectuado la conexión del terminal a un determinado AP, la dirección MAC usada se mantiene constante durante toda la conexión, aunque se haya generado de forma aleatoria y, por tanto, permite vincular las acciones realizadas por el dispositivo durante toda la conexión, por ejemplo, su localización absoluta y relativa con la localización de otros terminales.
- Se estima que actualmente entre un 5% y 10% de los dispositivos no utilizan direcciones MAC aleatorias.
- Existen multitud de técnicas que son capaces de identificar de forma unívoca, en un elevado porcentaje de casos, los dispositivos móviles aunque usen una dirección MAC aleatoria cambiante. Son las técnicas actuales empleadas en Wi-Fi tracking, basadas en la diversa información contenida (o deducida a partir de) en las tramas Probe Request combinada con la detección de patrones estadísticos de las direcciones MACs aleatorias. Las técnicas más avanzadas para vincular la información de distintas tramas a un mismo dispositivo emplean algoritmos de aprendizaje automático y analítica de datos basada en Big Data.

B. DATOS EMPLEADOS EN WI-FI TRACKING

Las diversas técnicas de Wi-Fi tracking tienen como objetivo identificar y rastrear terminales de manera única y precisa en entornos Wi-Fi.
Este método se basa en el empleo de una gran variedad de parámetros y características físicas tanto de los dispositivos como de las propias condiciones de la transmisión para generar una huella digital individualizada para cada dispositivo.

El uso de técnicas de reconocimiento de patrones y la analítica de datos en general, unido a una continua evolución de las técnicas empleadas por los fabricantes de dispositivos en defensa de la privacidad lleva a una situación de cambio permanente. Como resultado, algunas técnicas plenamente eficaces hace pocos años, han perdido su utilidad hoy día. A continuación, se describen los principales métodos empleados en la actualidad.

La trama “Probe Request” es un tipo de trama de gestión contemplado por el estándar Wi-Fi y se usa cuando el dispositivo (por ejemplo, un smartphone) no está conectado a un AP Wi-Fi. El dispositivo, en cada uno de los canales disponibles de la Wi-Fi, hace un sondeo “preguntando” por APs disponibles en su radio de cobertura a los que poder conectarse.

Cuando un determinado AP recibe la trama Probe Request, responde con una trama llamada “Probe Response”. Con esta trama, el dispositivo conoce de la existencia de ese AP y de sus características, en caso de que desee conectarse.

Este tipo de tramas se emite por todos los dispositivos en comunicaciones Wi-Fi de forma automática sin control por parte del usuario y sin cifrar, de forma que puede ser recibido y decodificado no solo por cualquier AP, sino también por cualquier dispositivo de bajo coste a la escucha del canal Wi-Fi.

Las características concretas de la emisión de este tipo de tramas dependen de muchas circunstancias, tales como el fabricante, el modelo y el propio sistema operativo del dispositivo. En algunos casos, los datos enviados

en las mismas (por ejemplo, el SSID) pueden ofrecer directamente información relacionada con la persona.[2]

Las tecnologías de Wi-Fi tracking aprovechan estas características de las tramas Probe Request (envío por todos los dispositivos, envío sin cifrar y con gran cantidad de datos) para generar una huella digital única que permite identificar al dispositivo.

Además de la información directamente enviada en las tramas Probe Request, es posible obtener información mediante mediciones indirectas a partir de combinaciones de éstas o mediante técnicas heurísticas.

En la práctica, cualquier medida o dato que asista en la labor de identificación del dispositivo puede ser utilizado. En las medidas físicas o datos adicionales que pueden emplear este tipo de tecnologías se encuentran, la fuerza de la señal recibida (RSSI por las siglas del inglés Received Signal Strength Indicator), que además puede ser empleada para determinar la ubicación aproximada del dispositivo, el intervalo de tiempo entre el envío de las tramas Probe Request, la distribución estadística tanto del número de secuencia de las tramas como de las MAC aleatorias o las desviaciones inherentes de los relojes de los dispositivos. En resumen, todas ellas pueden acabar permitiendo la generación de una huella digital.

El objetivo de la recogida y análisis de los datos como los anteriormente descritos (y de otros dependiendo de la solución concreta del fabricante) es la generación de una huella digital única que permita identificar a cada dispositivo. El **proceso de generación de la huella digital** de los terminales móviles en una red Wi-Fi **conlleva**, en términos generales, las siguientes fases:

- **Captura de tramas Probe Request:** Se recopilan masivamente las tramas Probe Request recibidas en los distintos APs de la red Wi-Fi en observación. Además de la información de las tramas, se pueden recoger datos relacionados con las condiciones físicas de la transmisión, como el RSSI y otros. Para llevar a cabo esta captura, se puede utilizar equipamiento especializado o incluso equipamiento de red Wi-Fi convencional que proporcione estas capacidades adicionales.

- **Extracción y envío de información:** Se extrae la información relevante de las tramas capturadas y de las características físicas de la transmisión. Esta información se envía a un servidor centralizado para su procesamiento y análisis. Los datos específicos enviados dependerán del modelo de Wi-Fi tracking implementado en la red.

- **Análisis de patrones y generación de la huella digital:** Después de extraer la información, se lleva a cabo un análisis de patrones de los datos recopilados. El objetivo es combinar características específicas de los datos recogidos que permitan distinguir un dispositivo de otro. Este análisis variará según el sistema utilizado y es fundamental para lograr una identificación unívoca de los terminales móviles en la zona monitorizada, siendo ya habitual el empleo de técnicas avanzadas, como el aprendizaje automático (machine learning) y el modelado probabilístico.

  Los algoritmos de aprendizaje automático son capaces de aprender patrones y establecer correlaciones entre los diferentes parámetros de las tramas para determinar la probabilidad de que una trama pertenezca a un dispositivo previamente identificado o sea de uno nuevo. Al combinar estas características en un modelo probabilístico, se genera una huella digital única para cada dispositivo. Estos modelos pueden integrar diferentes fuentes de información, como

[2] https://svs.informatik.uni-hamburg.de/publications/2022/2022-06-08_Probing_for_Passwords.pdf

datos históricos de dispositivos previamente identificados, información contextual y patrones de comportamiento, para generar huellas digitales más robustas y precisas.

En resumen, se crea una huella digital (fingerprint) que representa al dispositivo mediante una combinación de múltiples atributos permitiendo su singularización.

- **Comparación y reconocimiento:** Una vez se han construido las huellas digitales de diferentes dispositivos, se realiza una comparación y reconocimiento para identificar dispositivos y determinar si han sido detectados previamente por el sistema.

C. IDENTIFICACIÓN DE DISPOSITIVOS

Tras generar la huella digital del dispositivo, éste queda identificado. Si se realiza un seguimiento del mismo a través de su huella digital, será posible obtener el siguiente tipo de información:

- **Presencia en la zona de cobertura del AP:** La huella digital permite determinar si el dispositivo está presente o no en la zona donde se encuentra el AP. Esto resulta especialmente útil para contar el número de dispositivos presentes en un lugar o para obtener datos sobre la afluencia de visitantes en diferentes días.

- **Tiempo aproximado de permanencia:** Además de indicar la presencia del dispositivo, la huella digital permite estimar el tiempo aproximado que el terminal móvil pasa en la zona de cobertura. Este dato puede ser útil para comprender los hábitos de los usuarios y obtener información sobre la duración y frecuencia de las visitas.

- **Seguimiento de trayectoria:** La huella digital del dispositivo posibilita el seguimiento de su trayectoria a lo largo del tiempo. Esto implica registrar los movimientos del dispositivo en la zona de cobertura de la red Wi-Fi y obtener información sobre los lugares que ha visitado.

Para mejorar la precisión en el seguimiento de la trayectoria de un terminal móvil se pueden emplear técnicas de triangulación basadas en la potencia de la señal recibida de tres o más APs de la red.

Al combinar la información de estos APs, es posible lograr una alta precisión en la ubicación del dispositivo, llegando incluso a niveles de hasta 0.5 metros, según estudios realizados. Esta mayor precisión facilita el seguimiento y análisis de la trayectoria del dispositivo, proporcionando mayor detalle de los patrones de desplazamiento de los usuarios.

Es importante destacar que la retención de la huella digital de un mismo terminal durante varios días permitiría realizar un seguimiento más intenso y amplio. Así, al almacenar y reconocer la huella digital de un dispositivo a lo largo del tiempo, sería posible identificar patrones de comportamiento, descubrir preferencias o rutinas, actividades diarias, lugares frecuentados, entre otros aspectos íntimos de la vida de las personas.

3. DATOS PERSONALES Y TRATAMIENTOS INVOLUCRADOS

La tecnología Wi-Fi tracking ha evolucionado significativamente, permitiendo recoger y analizar múltiples características de los dispositivos.

Esta capacidad no se limita a la identificación a través de la dirección MAC, sino que también abarca la creación de huellas digitales únicas. Estas huellas, creadas mediante la combinación de múltiples características, permiten identificar dispositivos de manera continua, superando las medidas de anonimización como la aleatorización de direcciones MAC.

A su vez, el teléfono móvil, convertido en un elemento cotidiano e inseparable, actúa como un vínculo directo con su usuario, generando una identificabilidad tanto directa como indirecta[3]. Estos dispositivos forman parte de la esfera privada de los usuarios, por lo que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[4] y la normativa reguladora de la protección de datos personales. Por ello, en este contexto tecnológico, es crucial analizar la posible existencia de tratamientos de datos personales, así como, en su caso, el contenido de los mismos.

A. ALCANCE DEL TÉRMINO "DATO PERSONAL"

El concepto "dato personal" tal como se establece en el RGPD tiene un alcance muy extenso. El artículo 4.1 del RGPD define "dato personal" como "toda información sobre una persona física identificada o identificable".

La referencia a "toda información" en esta definición resalta la intención del legislador de otorgar a este concepto un significado muy amplio, que no se ciñe a los datos confidenciales o relacionados con la intimidad, sino que puede abarcar todo género de información, tanto objetiva como subjetiva, siempre que sean «sobre» la persona en cuestión. Para ello, bastará con que la información esté relacionada con una persona concreta debido a su contenido, finalidad o efectos.[5]

Sobre el concepto "identificable", el mismo artículo 4.1 dispone que se considerará persona física identificable a "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;".

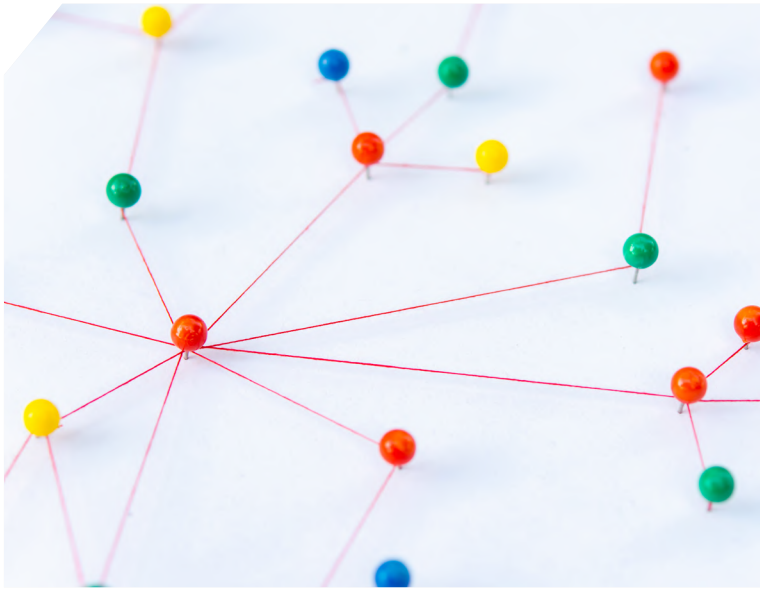
Por tanto, para calificar una información de dato personal, no es necesario que dicha información permita, por sí sola, identificar al interesado.

[3] Apdo. 4.2.2. Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes (GT29,WP185)
[4] Considerando 24 Directiva 2002/58/CE de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas
[5] Párrafos 34 y 35. STJUE de 20 de diciembre de 2017, caso C 434/16

Es más, una persona física es identificable desde el momento en que el poseedor de los datos sea capaz de distinguirla y tratarla de manera diferente, incluso cuando esos datos no basten por sí solos para hacerlo.

En este sentido, resulta útil establecer la diferenciación entre datos identificadores únicos que permiten identificar a la persona de forma inequívoca y "cuasi identificadores". Estos últimos, a primera vista no permiten identificar a una persona determinada. Sin embargo, al combinarlos entre sí o con otros permiten identificar a la persona debido a las "combinaciones únicas". Este fenómeno, conocido como "efecto mosaico", ilustra cómo la acumulación de datos "cuasi-identificadores" puede llevar a la identificación de una persona, proceso que se ve facilitado por tecnologías de análisis de datos masivos. Es perfectamente posible hablar de la existencia de datos personales incluso en supuestos en los que no se cuenta con una identificación directa o expresa del interesado.

Ejemplo:
Se dispone de información de un móvil que ha visitado (conociendo fecha, hora y tiempo de permanencia) en dos ocasiones el comercio A, en 3 ocasiones el establecimiento B, ha pernoctado en el establecimiento hotelero C durante 16 días y está calificado como turista con estancia superior a 15 días y menor de 1 mes. Esta información de por sí ya es tan detallada que con muy poca información adicional se podría identificar a la persona portadora de ese terminal móvil.



Con respecto a la capacidad de ser "identificable" como persona, el considerando 26 del RGPD subraya que se deben considerar "todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física".

Es decir, no es necesario que toda la información que permita identificar al interesado deba encontrarse en poder de una sola persona o dentro de un único tratamiento.

Lo que debe analizarse es que exista una posibilidad razonable de que utilizando otros medios adicionales pueda identificarse a la persona. Por otra parte, se trata de un análisis dinámico, por lo que debe tenerse en cuenta el grado de avance tecnológico en el momento del tratamiento y su posible desarrollo en el período durante el cual se tratarán los datos.

En definitiva, esa identificabilidad también se relaciona con que la misma no requiera esfuerzos desproporcionados y, como se acaba de indicar, la constante evolución tecnológica facilita la misma.

B. WI-FI TRACKING Y EL "FINGERPRINTING" COMO DATOS PERSONALES

Esta definición amplia del concepto de datos personales establecida por el RGPD adquiere especial relevancia en el contexto del Wi-Fi tracking. Esta tecnología afecta a todos los dispositivos con funcionalidad Wi-Fi, sin que necesariamente estén conectados a ninguna red concreta, y en ocasiones no estando siquiera activada dicha funcionalidad. Entre estos dispositivos se incluyen móviles, tablets, portátiles, ordenadores fijos, routers, impresoras, electrodomésticos, juguetes, dispositivos corporales (los denominados "wearables", incluyendo marcapasos, sistemas de oxígeno portátiles, dispositivos para diabéticos, implantes neuronales, etc.) e incluso automóviles[8].

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".

De acuerdo con lo anterior, 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. En particular, el "fingerprinting" o huella digital en el contexto del Wi-Fi tracking puede suponer de acuerdo con lo establecido en el RGPD, un tratamiento de datos personales.

El concepto de "fingerprinting" se define como "un conjunto de elementos de información que identifica un dispositivo o instancia de aplicación", abarcando por tanto cualquier información que pueda ser empleada para individualizar, vincular o inferir a un usuario o dispositivo a lo largo del tiempo[9].

Esto puede incluir, entre otros, datos derivados de:

- la configuración de un agente de usuario/ dispositivo;
- o datos expuestos por el uso de protocolos de comunicación de red.

Por tanto, el "fingerprinting" proporciona la capacidad de distinguir un dispositivo de otro y podría utilizarse para rastrear la ubicación o el comportamiento de un usuario en el tiempo, incluso si no se cuenta con una identificación directa o expresa de la persona.

[8] Algunas autoridades de control, como Unabhängige Landeszentrum für Datenschutz (Schlewig Holstein,Alemania) han expresado su preocupación por la aplicación de estas tecnologías sobre los automóviles que incorporen puntos de acceso Wi-Fi, permitiendo el seguimiento de personas. Location Services can Systematically Track Vehicles with WiFi Access Points at Large Scale

[9] Apdo. 3 Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting

C. WI-FI TRACKING Y DATOS DE LOCALIZACIÓN Y DE TRAYECTORIAS

Se puede conocer la posición de un dispositivo bien de forma aproximada por "presencia" (cercanía al sensor), bien de forma más precisa mediante triangulación. Al mantener la identificación o individualización del dispositivo y determinar su posición a lo largo del tiempo, es posible establecer una trayectoria durante el tiempo en que el dispositivo se encuentre dentro de la zona de cobertura de los sensores.

Estos datos de localización representan una tipología de datos personales de alto riesgo para la privacidad de las personas tal y como se detalla en el apartado de riesgos para los derechos y libertades de las personas físicas.

Cuando se mantenga el ámbito espacial y temporal de los datos recogidos mediante Wi-Fi tracking, estos pueden ser suficientes por sí solos o en combinación con otros para permitir la identificación de las personas y el responsable del tratamiento debería considerar este tipo de datos como datos personales.

D. TRATAMIENTO DE DATOS PERSONALES

En sí misma la tecnología Wi-Fi tracking no es un tratamiento de datos personales, pero, en su caso, podría formar parte él. De hecho, en la decisión de cómo desarrollar un tratamiento o alcanzar una finalidad, el responsable puede optar por soluciones distintas al Wi-Fi Tracking o por opciones que no impliquen un tratamiento de datos personales.

La tecnología Wi-Fi tracking puede aparecer en operaciones de tratamiento de datos personales derivadas de dos tipos de analíticas principalmente: la de presencia y la de localización. La analítica de presencia se centra en el estudio de la existencia de los terminales en una determinada zona y su permanencia en la misma, mientras que la de localización tiene como objetivo trazar el recorrido seguido por el terminal dentro de una determinada zona de estudio, incluso por tiempo indefinido.

En muchas ocasiones su finalidad es la de detectar y analizar comportamientos colectivos, sin embargo, no se puede olvidar que se parte de la detección de datos individuales.

A título ilustrativo, se señalan algunos tratamientos en los que se han empleado tecnologías de Wi-Fi tracking[10]:

- Servicio de geolocalización del dispositivo, con conformidad o no del propio usuario.
- Seguimiento de personas en los centros de trabajo.
- Servicios de emergencias, mediante la búsqueda o localización como parte de la prestación de auxilio vital a las personas. Se trata de un mecanismo por el que los centros de atención a llamadas de emergencia pueden recibir de forma automática información sobre la ubicación del llamante, enriquecida por los datos de localización Wi-Fi.
- Vigilancia de personas, empleando Wi-Fi tracking para detectar si hay personas en ciertos recintos o lugares, y control individual del acceso a estas zonas.

[10] El listado ofrecido no supone un posicionamiento ni a favor ni en contra por parte de las autoridades de control de protección de datos.

- Vinculación entre personas, para determinar si dos o más personas han compartido el mismo espacio, se han aproximado, se han detenido en el mismo punto, etc.

- Análisis del flujo de personas en instalaciones privadas (por ejemplo, centros de trabajo o centros comerciales) para optimizar el diseño del espacio físico o de la dotación de personal.

- Gestión de multitudes en lugares de acceso público: en áreas concurridas como aeropuertos, transporte público, estadios, vías públicas etc., para controlar aforos máximos, gestionar el tráfico de personas o rodado de manera eficiente, optimizar rutas o proporcionar información en tiempo real, mejorando la seguridad y la comodidad. Es habitual encontrar estos usos dentro de proyectos de "smart cities".

- Marketing y publicidad dirigida, para enviar promociones o anuncios a los dispositivos de los usuarios cuando acceden o se acercan a una ubicación específica o en función del comportamiento o patrones de movimiento.

- Creación de perfiles de usuario en función de los patrones de movimiento y el comportamiento.

En resumen, es importante tener en cuenta que muchos de estos usos implican la recopilación y el procesamiento de datos personales y, por tanto, deben someterse al conjunto de principios, derechos de las personas físicas y obligaciones para los responsables del tratamiento establecidos en el RGPD y la LOPDGDD.

4. BASES LEGITIMADORAS DE TRATAMIENTOS DE DATOS PERSONALES

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. Para ello es fundamental asegurarse que el tratamiento posterior no se aparta de las finalidades ya establecidas para el tratamiento, y de las que se ha de informar a las personas interesadas. Por ejemplo, si se realizase un tratamiento de datos de los desplazamientos de las personas dentro de un local comercial para optimizar la ubicación física de unos determinados productos basado en un interés legítimo del responsable, posiblemente resultaría difícil justificar

la compatibilidad de un tratamiento que implicase que esas personas recibiesen notificaciones relativas a ofertas comerciales de dichos productos.

Igualmente, es esencial que los datos personales tratados sean adecuados y pertinentes, se limiten a lo estrictamente necesario para su finalidad. Cabe recordar que la finalidad del tratamiento no es realizar Wi-Fi tracking, por lo que si es posible conseguir la finalidad última con una técnica menos intrusiva no se estaría cumpliendo con el principio de minimización de datos. Si no fuese posible otra técnica que no fuera Wi-Fi tracking, para cumplir el principio de minimización los datos tratados tendrían que ajustarse, en sus categorías, frecuencia, granularidad, etc., a lo estrictamente necesario, así como que su plazo de conservación sea el mínimo indispensable, procediendo a su eliminación o anonimización efectiva, mediante procesos automatizados siempre que sea posible.

También será necesario cumplir el principio de exactitud, en particular si se están utilizando técnicas probabilísticas para vincular acciones a un individuo, rectificando o suprimiendo los datos que sean inexactos cuando proceda y garantizar la seguridad y confidencialidad de los datos personales, como se analizará en detalle posteriormente.

El responsable del tratamiento, además de cumplir con los principios anteriormente expuestos 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.

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. No obstante, es posible proporcionar orientaciones generales a los responsables que les guíen a la hora de identificar si se da alguna de las condiciones que legitimaría un tratamiento concreto que emplease tecnologías de Wi-Fi tracking.

A. CONSENTIMIENTO (ARTÍCULO 6.1.A DEL RGPD)

De acuerdo con lo analizado previamente, la mayoría de las técnicas de Wi-Fi tracking operan sin necesidad de que el dispositivo esté conectado a la red Wi-Fi y sin el conocimiento de la persona propietaria del mismo. Es decir, no existe una vía de comunicación entre el interesado y el responsable del tratamiento. Por ello, resultaría materialmente imposible solicitar el consentimiento al interesado y por tanto, debería en principio descartarse como una base legitimadora.

Cabría sin embargo plantear algún escenario concreto, donde el usuario realizara la conexión a la red Wi-Fi de forma voluntaria, y tras dicha conexión se le informara y solicitara el consentimiento para tratar sus datos mediante Wi-Fi tracking. No podemos olvidar que en estos supuestos dicho consentimiento tendría que ser libre, específico, informado e inequívoco.

Un ejemplo práctico:
Podría darse en escenarios donde mediante una aplicación, se invitase a los usuarios a permitir el seguimiento de su localización a cambio de ofertas comerciales.[11]

En estos casos, se deberían articular sistemas que garantizaran el cumplimiento del principio de transparencia, permitiendo que la información sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo y, además, en su caso, se visualice, tal y como se analiza en el **apartado 9**.

En determinados casos, como puede ser en el ámbito laboral, educativo o también el sector público, habrá que analizar si pudiese producirse un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado, por lo que la evaluación de la libertad del consentimiento tendrá que realizarse cuidadosamente.

B. EJECUCIÓN DE UN CONTRATO (ARTÍCULO 6.1.B DEL RGPD)

La ejecución de un contrato o de medidas precontractuales, podría legitimar el tratamiento de datos únicamente si estuviera relacionado con la prestación de un servicio específico en el contexto de Wi-Fi tracking.

En ese caso será esencial poder demostrar que el tratamiento es necesario para cumplir con las obligaciones contractuales, lo que no será habitual, salvo en ciertos casos de servicios de geolocalización solicitados por el usuario.

C. CUMPLIMIENTO DE UNA OBLIGACIÓN LEGAL (ARTÍCULO 6.1.C DEL RGPD)

Esta base sólo sería aplicable cuando existiese una obligación legal que exigiese al responsable el cumplimiento de una finalidad para la que sea necesario el empleo de las técnicas de Wi-Fi tracking. Adicionalmente, de conformidad con la LOPDGDD, dicha obligación tendría que estar prevista en una norma de Derecho de la Unión Europea o una norma con rango de ley.

Dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del TJUE, incluyendo las medidas para garantizar un tratamiento lícito y equitativo, cumpliendo un objetivo de interés público y proporcional al fin legítimo perseguido.

D. PROTECCIÓN DE INTERESES VITALES (ARTÍCULO 6.1.D DEL 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[12].

[11] Considerando 17. Dictamen 01/2017 sobre la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas (2002/58/CE) (GT29,WP247).
[12] Informe 39/2019 del Gabinete Jurídico de la AEPD.

E. INTERÉS PÚBLICO O EJERCICIO DE PODERES PÚBLICOS (ARTÍCULO 6.1.E DEL RGPD)

Fundamentar un tratamiento de datos de estas características en esta base legitimadora implica realizar un cuidadoso análisis de las exigencias establecidas en la normativa de protección de datos. Así, el responsable del tratamiento deberá identificar la norma con rango de ley 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. Dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del TJUE, incluyendo las medidas para garantizar un tratamiento lícito y equitativo, cumpliendo un objetivo de interés público y proporcional al fin legítimo perseguido.

Debe advertirse en contra del empleo de preceptos legales excesivamente genéricos como base de legitimidad. Dado que no existe legislación expresa al respecto, sería recomendable el desarrollo de medidas legislativas, que de acuerdo con lo indicado anteriormente contemplasen y regulasen este tipo de tratamientos.

Debe tenerse en cuenta que la actuación de la Administración se centrará principalmente en espacios públicos y que las personas tienen una legítima expectativa a disfrutar de libertad de movimiento sin ser monitorizados. En estos escenarios la intromisión sobre la privacidad de las personas puede ser muy alta si no se extreman las garantías por parte del responsable del tratamiento.[13]

F. INTERESES LEGÍTIMOS (ARTÍCULO 6.1.F DEL RGPD)

En el sector privado, el interés legítimo puede considerarse una condición de licitud válida siempre que sea necesaria para la satisfacción de dichos intereses y no prevalezcan los intereses o los derechos y libertades de los interesados, teniendo en cuenta las expectativas razonables de los mismos.

En todo caso, se requiere una evaluación meticulosa de si puede llevarse a cabo el tratamiento, prueba de sopesamiento, inclusive si un interesado puede preverlo de forma razonable en el momento y en el contexto de la recogida de datos personales[14].

Corresponde al responsable la acreditación de la prueba de "sopesamiento". En el Dictamen 6/2014, de 9 de abril, sobre el concepto de interés legítimo del responsable del tratamiento, del grupo de trabajo creado por el artículo 29 de la Directiva 95/46/CE -WP 217, se incorporan diversas directrices y orientaciones para analizar la existencia del interés legítimo, así como los elementos de salvaguarda necesarios en atención al respeto y garantía de los derechos de los afectados por este tipo de tratamientos.

[13] Ver decisión Autoridad de Protección de Datos de Países Bajos sobre el tratamiento de datos personales de usuarios de dispositivos móviles en los que se encendió el Wi-Fi en el centro de la ciudad de Enschede sin una base legal apropiada.

[14] Considerando 47 RGPD: "En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior."

En una primera aproximación, se deberán ponderar los intereses y derechos del interesado y los tratamientos que el responsable pretenda llevar a cabo, valorando la afectación a la privacidad. No debe olvidarse que el considerando 47 del RGPD, indica que, a los efectos del interés legítimo, "los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior" y, en el caso del Wi-Fi tracking, la captación de datos, como se ha referido al inicio, en muchas ocasiones es ajena al conocimiento del titular del terminal.

En definitiva, en estos casos, debería poder demostrarse claramente que el interés legítimo del responsable es prevalente.

Solo en los casos en que, como resultado de la ponderación efectuada, no prevalezcan los intereses y los derechos fundamentales de los afectados, podrá llevarse a cabo el tratamiento de datos personales justificado en un interés legítimo, lo que además exigiría que se incorporasen al tratamiento las salvaguardas, garantías y medidas técnicas y organizativas, incluyendo las relativas a la seguridad de la información, que resultaren necesarias para proteger los datos personales tratados.

Es decir, la licitud del tratamiento amparada en esta base también queda supeditada a la existencia e intensidad de garantías adecuadas. Estas garantías dependerán sin duda, de la naturaleza más o menos invasiva del tratamiento propuesto y, en gran medida de cómo y cuándo se realice la disociación irreversible de los datos personales.

En términos generales, el tratamiento será considerado menos intrusivo cuando la anonimización de los datos se realice más cerca del momento en que se generaron o recibieron los datos de tráfico a través del dispositivo con Wi-Fi activado.

Sin perjuicio de la necesidad de un análisis caso a caso y siempre con pleno respeto a todas las exigencias del RGPD, medidas como una pronta anonimización de los datos recogidos, obtener exclusivamente información agregada sobre el número de visitantes y las zonas más o menos visitadas (mapas de calor) del interior de un establecimiento, garantizar que no se toman datos en el exterior, ni en zonas comunes de paso, ni en la vía pública y garantizar que no es posible el seguimiento de las personas, podrían acercar a un sopesamiento favorable, sin perjuicio del resultado que pueda arrojar la evaluación de impacto relativa a la protección de datos.

Otros escenarios que contemplen una mayor recogida de datos personales en el espacio (mayores áreas de cobertura), en el tiempo (mayores períodos de tiempo), o en el ámbito (datos de movilidad, de repetición de visitas, etc.) alejan la posibilidad del sopesamiento favorable, atendiendo a la dificultad de mecanismos efectivos y prácticos que permitan a las personas oponerse al tratamiento (mecanismos de opt-out) en el Wi-Fi tracking.

5. RIESGOS PARA LOS DERECHOS Y LIBERTADES DE LAS PERSONAS FÍSICAS

El artículo 24.1 del RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone un tratamiento de datos personales, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento. Por tanto, cualquier organización que tome la decisión de poner en marcha un tratamiento de datos personales deberá gestionar dichos riesgos.

En este apartado se presentan los principales riesgos que podrían asociarse a tratamientos de datos personales que se implementen utilizando tecnología Wi-Fi tracking. No es una lista exhaustiva de riesgos, sino una panorámica de los principales riesgos a considerar y, en cualquier caso, los responsables del tratamiento deberán determinar, en base a las particularidades del tratamiento concreto, qué riesgos son aplicables en su caso y determinar la existencia de otros posibles no identificados en esta guía.

La gestión del riesgo para los derechos y libertades de las personas es distinta a una gestión del riesgo de cumplimiento de los principios establecidos en el RGPD y la normativa de protección de datos aplicable. La gestión de riesgos de cumplimiento normativo, como otras gestiones de riesgo con otros objetivos (legal, financiero, negocio, fraude, proyecto, etc), puede resultar necesaria para alcanzar ciertos objetivos de la organización, pero no da respuesta a las obligaciones de gestión de riesgos para los derechos y libertades de las personas físicas impuestas por el RGPD. Si el tratamiento que se pretende iniciar no cumple los principios del RGPD, por ejemplo, por carecer de una base jurídica adecuada o no cumplir el principio de necesidad y proporcionalidad, el tratamiento sería ilícito y estaría prohibido. El uso de Wi-Fi tracking se enmarcará en un tratamiento de datos personales y la organización que lo implemente está obligada al cumplimiento de los requisitos y obligaciones establecidos en el RGPD, y entre otros a gestionar los riesgos para las personas que se verán afectadas por el tratamiento en su conjunto.

Ejemplo:
Con el propósito de preservar la seguridad de las personas en los accesos a un evento masivo, es posible querer determinar si algunos de los caminos de acceso se están congestionando. Para medir dicha congestión se podría plantear la utilización de tecnología Wi-Fi tracking para realizar un conteo aproximado y será un medio para implementar una de las operaciones del tratamiento, la medición de la congestión. Únicamente midiendo la congestión no se alcanzará la finalidad de preservar la seguridad de las personas, ya que el tratamiento ha de disponer de otras operaciones, como la toma de decisión de reducir la congestión en un momento dado, la capacidad de hacerlo de forma efectiva y acciones para que eso se produzca de forma eficiente y ordenada. Si estas operaciones que dan sentido al fin último del tratamiento no están correctamente implementadas, el tratamiento no está cumpliendo una finalidad que tenga una base legal. Así mismo, si ya existen medios con los que se están alcanzando dichos objetivos (videovigilancia, contadores de personas, etc.) el tratamiento tampoco sería necesario, al mismo tiempo podría resultar no idóneo dado que dicha medida conlleva un riesgo adicional pues existen medios menos lesivos para alcanzar la posible finalidad de este sistema.

La gestión de riesgos debe hacerse considerando el tratamiento de datos personales en su conjunto. Un mero análisis aislado de los posibles riesgos de la tecnología Wi-Fi tracking no tendría sentido y sería insuficiente conforme al RGPD, puesto que esa tecnología es un medio que puede utilizarse en tratamientos de diversa complejidad que impliquen el uso combinado de otras tecnologías (nube, blockchain, IA, IOT, etc.),

Ejemplo:
No implica los mismos riesgos un tratamiento cuya finalidad exclusiva sea el control del aforo para garantizar la seguridad de una tienda física individual de una PYME que se decida implementar utilizando Wi-Fi tracking, que un tratamiento con la misma finalidad pero en todas las tiendas físicas de una cadena a nivel nacional o un tratamiento cuya finalidad sea ofrecer publicidad online dirigida a las personas en función de los establecimientos o secciones visitadas dentro de un establecimiento.

Utilizar la misma tecnología a nivel provincial o autonómico para determinar flujos habituales de turistas, obtener tasas de repetición de visitas turísticas cuyo responsable es una autoridad u organismo público, implicará más riesgo que utilizarla en una única tienda física para estimar aforos. Utilizando en esencia la misma tecnología los tratamientos son distintos y los riesgos también lo son.

A. IMPACTO SOBRE LA INTIMIDAD DE LAS PERSONAS

El uso de la tecnología Wi-Fi tracking implica que en determinadas circunstancias sea posible singularizar[15] a las personas, localizarlas en una ubicación precisa e inferir[16] datos relativos a las personas en función del contexto de la ubicación.

Ejemplo:
La implementación de esta técnica en el ámbito laboral, por ejemplo, en un edificio puede proporcionar información sobre parte de la actividad que actualmente está protegida por la normativa laboral, como el control de cuánto tiempo transcurre en zonas comunes, con quién se dialoga y por cuanto tiempo, la asistencia a los aseos, la localización fuera del horario estrictamente laboral (biblioteca, zonas de esparcimiento), etc.

[15] La singularización hace referencia a la posibilidad de individualizar a una persona en un conjunto de datos resaltando ciertos registros. La singularización puede ocurrir incluso sin necesidad de que la persona sea identificada.
[16] La inferencia ocurre cuando es posible deducir el valor de una característica personal con un alto grado de probabilidad a partir de los valores de una serie de otros atributos, como la localización en determinadas ubicaciones, el contexto de tales ubicaciones, u otros.

B. INTROMISIÓN EN EL DOMICILIO O ZONAS PÚBLICAS

La tecnología Wi-Fi tracking hace difícil establecer límites físicos claros y definidos sobre donde sí se recoge la señal del dispositivo y donde no se puede recoger.

En una videocámara se pueden establecer ciertas máscaras y orientar las lentes, pero este tipo de límites es más costoso de implementar en un sistema basado en radiofrecuencia.

Ejemplo:
La instalación de un sistema de Wi-Fi tracking en un edificio puede estar recogiendo la señal de dispositivos ubicados en hogares o domicilios privados que estén detrás de un muro, de trabajadores de otras entidades, o de la propia entidad que no deberían ser sujetos de datos del tratamiento o, incluso, de personas que transitan por la vía pública. Tal intrusión no sería un riesgo, sino un incumplimiento del principio de legitimación del tratamiento.

C. ESCALA DEL TRATAMIENTO Y LIMITACIÓN DE LIBERTAD DE CIRCULACIÓN

Analizar el impacto de determinados sistemas tecnológicos sólo en función del ámbito de una entidad proporciona una visión limitada de la posible intromisión en la privacidad de las personas.

Las tecnologías se implementan actualmente a gran escala y es necesario analizar su impacto cuando son implementadas de forma masiva, pues pueden producir de forma conjunta un efecto limitador de los derechos y libertades de los ciudadanos.

Ejemplo:
Una empresa de seguridad ofrece, además de los servicios habituales, uno de Wi-Fi tracking para el pequeño comercio, de forma que un 30% de los locales comerciales de una ciudad implementan ese servicio, que permite registrar los identificadores de los transeúntes cercanos al local comercial. De esta forma, sería posible tener registrados y controlado el deambular por la ciudad de cualquier ciudadano en un momento dado.

D. SEGUIMIENTO POR OMISIÓN: INTROMISIÓN EN LA LIBERTAD RELIGIOSA O EL TRATAMIENTO DE CATEGORÍAS ESPECIALES DE DATOS

El registro de qué sitios son visitados por una persona permite inferir hábitos de vida y gustos o intereses con temáticas relacionadas con los puntos en los que se la puede localizar.

Sin embargo, hay que tener en cuenta que también proporcionan mucha información, o incluso más, aquellas áreas que una persona no visita y que pueden permitir un perfilado basado en categorías especiales de datos.

Además, es independiente de que la información revelada por el tratamiento en cuestión sea o no exacta y de que el responsable del tratamiento actúe con el fin de obtener información comprendida en alguna de las categorías especiales[17].

Ejemplo:
En el marco de un tratamiento que incorpore tecnología Wi-Fi tracking a nivel de un centro comercial, que permita singularizar a una persona esta podría ser rastreada visitando tiendas de deporte, restaurantes de comida tradicional de algún país concreto, con pausas en los horarios habituales de culto de una determinada religión, no accediendo a establecimientos vinculados con otras religiones y nunca deteniéndose en los exhibidores de alcohol se podría perfilar su edad, sexo, religión y procedencia estimada, con o sin suficiente fundamento. Del mismo modo, un centro comercial que cuenta con un determinado centro religioso en sus aledaños podría obtener información de las personas que habitualmente asisten a ejercer culto religioso según sus creencias, incluidos menores o personas en riesgo de exclusión social u otras situaciones de riesgo.

En esencia, cuando estos tratamientos se lleven a cabo en lugares relacionados con categorías especiales de datos, como podría ser un centro hospitalario, una clínica de una especialidad médica, o la sede de un partido político, el responsable podría estar incurriendo en un tratamiento de categorías especiales de datos lo que incrementa el riesgo para los derechos y libertades de las personas.

Ejemplo:
La posibilidad de atribuir a una persona individual visitas a una clínica oncológica en un hospital en el que se utiliza la tecnología Wi-Fi tracking puede llevar que se infiera la enfermedad de la persona, y que en el futuro pueda encontrar dificultades para la contratación de un seguro de salud.

[17] TJUE (Sentencia TJUE C-252/21 Meta vs. Oficina Defensa de la Competencia Alemana) considera tratamiento de datos de categorías especiales la recogida de visitas a páginas o Apps relacionadas con una o más categorías especiales de datos, aunque no se recojan datos sensibles en sí. Extrapolando esta decisión al caso de tratamientos que incorporen Wi-Fi Tracking, implicaría que en los casos en los que estos tratamientos ocurran en recintos o establecimientos relacionados con categorías especiales de datos, el responsable podría estar tratando datos de categorías especiales.

E. LIBERTAD PERSONAL Y AUTOCENSURA

El conocimiento por parte de una persona de que va a ser rastreado en su deambular por zonas públicas, un edificio o un centro comercial puede hacer que ejerza la autocensura para preservar su interés por determinadas asociaciones políticas o religiosas, centros culturales o actividades de ocio y puede condicionar su libertad personal, su libertad de movimientos y producir situaciones de autocensura.

Esto puede ocurrir incluso en aquellos casos en los que el interesado sea informado adecuadamente sobre el tratamiento de sus datos personales, debido a las expectativas propias sobre el tratamiento que se aplicará a los datos capturados de su terminal móvil.

Ejemplo:
Una persona que tenga una curiosidad por algún tipo de producto, servicio o de ocio que se ofrezca en un centro comercial pero que contravenga algún precepto ético de su ambiente social, pueda tener una repercusión mediática o puede ser mal interpretado en cualquier otra circunstancia puede cambiar su comportamiento si sabe que el mero deambular cercano al mismo puede ser registrado.

F. EL IMPACTO DE LA REIDENTIFICACIÓN

Incluso cuando lo que se persiga sea obtener datos colectivos o estadísticas agregadas y no se pretenda singularizar a las personas, el origen de los datos partirá de operaciones de tratamiento sobre identificadores únicos, como pueden ser direcciones MAC de los dispositivos, una huella digital o fingerprint de los mismos u otros a los que en el mejor de los casos se les aplicará algún tratamiento de datos personales de seudonimización o de anonimización[18].

La seudonimización es un tratamiento de datos personales que genera, a partir de un conjunto de datos personales, un nuevo conjunto de información seudónima y la información que permite reidentificar a las personas. El RGPD sigue siendo aplicable a un conjunto de datos seudonimizado puesto que las personas son identificables.

Por ejemplo
Sustituir las direcciones MAC de un conjunto de datos por un hash de la dirección MAC, podría ser una operación de tratamiento de pseudonimización.

La anonimización es un tratamiento de datos personales que genera, a partir de un conjunto de datos personales, un nuevo conjunto de información anónima. Por tanto, en todo caso desde que se recopilan los datos hasta que se anonimizan hay siempre una fase en la que hay un tratamiento de datos personales.

En todo tratamiento de anonimización de datos existe cierta probabilidad de que se produzca una reidentificación de los interesados[19].

[18] seudonimización y la anonimización son operaciones de tratamiento distintas y no deben confundirse. Véase Anonimización y seudonimización.
[19] Anonimización (III); el riesgo de la reidentificación.

Esto es, un conjunto de datos supuestamente anónimo deja de ser anónimo[20] porque los interesados han sido identificados o pueden ser identificados.

Cuando esto ocurre, se materializa el riesgo para los derechos y libertades de las personas porque, entre otras consecuencias, posibilita la singularización, vinculación o inferencia.

Incluso aplicando estrategias de anonimización, es necesario evaluar la probabilidad de reidentificación y de brecha de datos personales, así como el impacto que puede tener sobre los derechos y libertades de los interesados.

Para ello hay que considerar las condiciones del peor caso, como intentos de reidentificación por personas internas o externas a la organización, con acceso a datos auxiliares, incluyendo los disponibles por medios ilegales, por órdenes judiciales o por agencias de información, además de considerar de que se cuenta con los recursos adecuados y teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

Ejemplo:
En algunas aplicaciones se pretende garantizar la imposibilidad de reutilización de la información de Wi-Fi tracking por la utilización de un método de hash específico, a la utilización de "sales" o claves para cada propietario. Si bien es un método para aumentar la seguridad, hay que tener en cuenta que se está siguiendo una técnica de "seguridad a través de la oscuridad", que cualquier principio de seguridad establece que no ha de ser el pilar de las garantías por su debilidad intrínseca. En cualquier caso, puede ser una de las muchas medidas a adoptar, sin garantía de eficacia absoluta.

Tal probabilidad existe debido al tipo de datos que se recogen, a una posible ausencia de mecanismo robusto de anonimización, al momento o fase del tratamiento en el que se aplica la anonimización, a que la anonimización pueda no serlo realmente o a la existencia de la tecnología que permitiría llevar a cabo esa reidentificación.

Ejemplo:
En una base de datos supuestamente anonimizada con datos de más de 8 millones de tramas Probe Request, a través de uno de los campos (WPS) contenido en este tipo de tramas, fue posible reidentificar más del 90% de datos identificativos de aquellos terminales que transmitían dicho campo.[21]

[20] A. Di Luzio, A. Mei and J. Stefa, "Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests," IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 2016, pp. 1-9, doi: 10.1109/INFOCOM.2016.7524459.

[21] Mathy Vanhoef, Célestin Matte, Mathieu Cunche, Leonardo Cardoso, Frank Piessens. Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms. ACM AsiaCCS, May 2016, Xi'an, China. ff10.1145/2897845.2897883ff. ffhal-01282900

G. RIESGOS ASOCIADOS A LOS DATOS DE LOCALIZACIÓN

Es preciso incidir en la especial dificultad de anonimizar conjuntos de datos cuando incluyen diversos datos de localización de una misma persona o datos de trayectorias[22] por la facilidad de reidentificación que presentan.

Ejemplo:

Se publicaron las carreras de 173 millones de taxis en Nueva York, anonimizando (supuestamente) el número de licencia de cada taxi con un hash. Los datos incluían hash del número de licencia, inicio, final, duración, tiempo, coste y propina. En muy poco tiempo el número de licencia de los taxis se reidentificó y con búsquedas en Google se obtuvieron imágenes de personas con relevancia pública tomando los taxis reidentificados.[23]

El Comité Europeo de Protección de Datos (CEPD) y anteriormente el Grupo de Trabajo del Artículo 29 han advertido en diversas ocasiones sobre la naturaleza especialmente sensible de los datos de localización[24]. Los desplazamientos de una persona pueden proporcionar información reveladora, como su lugar de trabajo, lugar de residencia y centros de interés, incluyendo lugares de culto o actividades relacionadas con su orientación sexual, lo que podría permitir crear un perfil detallado de los comportamientos de la misma.

La capacidad de identificación de los datos de localización es bien conocida y a menudo solo se necesitan unos pocos puntos espaciales para singularizar a una persona dentro de una población con alta precisión, considerando los patrones habituales de movilidad. Esto significa que, incluso cuando se suprimen identificadores únicos como la dirección MAC, al estar el dispositivo singularizado, los datos de localización pueden llevar a la identificación de una persona. Lógicamente, mientras mayor sea el ámbito temporal y espacial de la localización, más factible será la identificación.

Un patrón de datos que contiene la localización de una persona a lo largo del tiempo no puede ser completamente anonimizado, incluso si se reduce la precisión de las coordenadas geográficas registradas o se eliminan detalles específicos del itinerario.

Además, esto también se aplica a datos de localización agregados de forma incompleta. Es decir, simplemente anonimizar datos no garantiza la protección de la privacidad, ya que si los patrones de movilidad son lo suficientemente únicos, puede utilizarse información externa para vincular nuevamente los datos con un individuo específico.

Así, se pueden dar circunstancias específicas como la existencia de áreas poco concurridas a ciertas horas donde sería sencillo identificar a la persona y sus comportamientos o, incluso, combinar la captación de un indicador con las imágenes de un sistema de videovigilancia dando lugar a la identificación automática de la persona.

[22] de Montjoye, YA., Hidalgo, C., Verleysen, M. et al. Unique in the Crowd: The privacy bounds of human mobility. Sci Rep 3, 1376 (2013).
[23] On Taxis and Rainbow Tables: Lessons for researchers and governments from NYC's improperly anonymized taxi logs.
[24] Ver Dictamen 13/2011 y 01/2017 del GT29, y las Directrices 04/2020 del CEPD

H. FALTA DE UNA CAPACIDAD DE "ACCOUNTABILITY" DE LOS MEDIOS

Lo habitual es que los responsables de tratamientos que incorporen en sus tratamientos tecnologías de este tipo lo hagan mediante encargados del tratamiento o proveedores que ofrecen servicios de Wi-Fi tracking, incluso en combinación con otras tecnologías.

En este tipo de proyectos, se observa con frecuencia un control insuficiente por parte del responsable del tratamiento de los medios que se están empleando para implementar el tratamiento. Muchos responsables, en vez de una asesoría profesional independiente, tomarán decisiones basadas en información puramente comercial con desconocimiento de las implicaciones para los derechos y libertades, los posibles tratamientos colaterales y la pérdida de control del tratamiento.

Los datos se hallan habitualmente en el entorno tecnológico de encargados de tratamiento con relaciones muy complejas, con múltiples cesiones de datos, en los que suelen intervenir infraestructuras en nube, sometidos a analítica avanzada de datos e incluyendo en muchos escenarios técnicas de aprendizaje automático y tratamientos por cuenta de los encargados de tratamiento.

Ante una eventual generalización de este tipo de servicios, y ante la competitividad de las economías de escala, la situación probablemente será que un mismo encargado de tratamiento, o unos pocos, presten sus servicios a casi todos o muchos de los responsables. Por tanto, esos encargados tratarán datos de múltiples orígenes distintos, de varios responsables, con el impacto multiplicador que ya están teniendo las brechas de datos personales en encargados que dan servicio a múltiples entidades y podrían utilizarlos para finalidades propias[25] como pueden ser mejoras en su servicio, ofrecer publicidad online personalizada u obtener rentabilidad de los datos poniéndolos a disposición de terceros. Esto supone un riesgo para los derechos y libertades de las personas que debe ser gestionado por el responsable del tratamiento.

Ejemplo:

Un proveedor de servicios de Wi-Fi tracking proporciona de forma gratuita a todos los establecimientos de una calle, galería o centro comercial la posibilidad de ofrecer un servicio de conectividad Wi-Fi a sus clientes que incluye tecnología Wi-Fi tracking de la que podrán aprovecharse todos los responsables de forma independiente. Cada responsable únicamente obtendrá datos estadísticos y supuestamente anonimizados de los clientes que entren en su establecimiento. Sin embargo, el encargado de tratamiento recibirá los datos de todos los establecimientos. El encargado puede mantener los datos sin anonimizar o incluso haber vinculado los datos con otras bases de datos propias o de terceros para mantener singularizados o identificados a las personas y basar su modelo de negocio en la venta de esos datos personales, en cuyo caso, podría estar utilizando datos al margen de su rol de encargado y convertirse en responsable de un tratamiento para el que no estaría legitimado.

De hecho, aunque el responsable no tenga la intención de identificar a los interesados y no tenga la intención de realizar tratamientos con otras finalidades, algún encargado de tratamiento o tercero sí podría tener la intención

[25] En tal caso, el encargado se convierte en responsable para esos tratamientos propios y no los puede llevar a cabo sin informar al responsable inicial, obtener su visto bueno y que las nuevas finalidades sean compatibles con las iniciales.

de realizar otros tratamientos, aprovechar los datos para finalidades propias, vincular[26] los datos con otras bases de datos que permitan la identificación de las personas y conseguir que la anonimización de los datos no sea realmente efectiva.

Aunque estos tratamientos serán manifiestamente ilícitos, el entorno de este tipo de tratamientos impide en muchos casos tener garantías o control sobre si se están produciendo.

I. ESCENARIOS DE BRECHAS DE DATOS PERSONALES

El hecho de que ni el responsable ni los encargados pretendan singularizar, ni identificar a los interesados, ni perfilar a los interesados no implica que no pueda suceder[27]. En particular, este riesgo se materializa cuando se producen brechas de datos personales tanto por parte de elementos internos o externos a la propia organización. Cualquier tratamiento de datos personales es susceptible de sufrir una brecha de datos personales independientemente de las medidas técnicas y organizativas implantadas en el tratamiento.

Cuando una brecha de datos personales se produce no solo en un responsable, sino en alguno los encargados o subencargados de tratamiento que dan servicio a múltiples responsables, el impacto podría ser mucho mayor tanto por el volumen de datos como por los distintos ámbitos de la vida personal de los interesados afectados.

En general, en tratamientos de datos personales que utilicen Wi-Fi tracking es especialmente importante considerar la probabilidad de que ocurra una brecha de confidencialidad, bien porque se produzca una exfiltración de datos, bien porque se pueda revertir la anonimización aplicada al conjunto de datos.

Ejemplo:
Una empresa de seguridad ofrece, además de los servicios habituales, uno de Wi-Fi tracking para el pequeño comercio, de forma que un 30% de los locales comerciales de una ciudad implementan ese servicio, que permite registrar los identificadores de los transeúntes cercanos al local comercial. Los datos son anonimizados por la empresa de seguridad, de forma que los pequeños comercios únicamente tienen acceso a datos anonimizados. La empresa de seguridad sufre un ciberincidente y se exfiltran datos que incluyen logs del sistema de Wi-Fi tracking de los últimos 5 años de una fase del tratamiento en la que los datos todavía no están anonimizados. Esos datos permiten singularizar a las personas, en algunos casos identificarlas, obtener su ubicación y seguir sus recorridos por la ciudad durante los últimos 5 años.

La realidad de las brechas de datos personales hace evidente que la materialización de las amenazas sobre conjuntos de datos es cuestión de tiempo, y que la única incógnita es la dimensión que va a alcanzar la brecha.

[26] Se habla de vinculabilidad cuando es posible vincular al menos dos registros sobre el mismo sujeto de datos o grupo de sujetos de datos (en la misma base de datos o en dos bases de datos diferentes).

[27] Ver decisión Autoridad de Protección de Datos de Países Bajos sobre el tratamiento de datos personales de usuarios de dispositivos móviles en los que se encendió el Wi-Fi en el centro de la ciudad de Enschede sin una base legal apropiada. “El hecho de que no utilicen estos recursos en la práctica para identificar a las personas en el centro de la ciudad no resta valor al hecho de que podrían hacerlo razonablemente.”

En estos casos, el problema no solo está en el conjunto de datos que se han filtrado de un responsable, sino cuando ese conjunto de datos se vincula con datos de brechas anteriores, no solo en el marco de tratamientos utilizando Wi-Fi tracking, sino también de otros servicios de Internet.

Ejemplo:
Una base de datos de Wi-Fi tracking puede filtrarse a la dark web. Hay que plantearse que en la dark web pueden encontrarse otras bases de datos que permitan vincular acciones de un mismo individuo en dos entornos completamente distintos, o incluso se ha podido filtrar una base de datos previamente que permita vincular los datos Wi-Fi con otros datos personales.

Por lo tanto, antes de poner en marcha un tratamiento con tecnología Wi-Fi tracking, en particular a la hora de la selección de los proveedores tecnológicos y encargados, es imprescindible plantear qué puede salir mal y qué consecuencias puede tener una brecha de datos personales para los derechos y libertades de las personas físicas para, antes de implementar el tratamiento, diseñar las salvaguardas de privacidad para minimizar el impacto de la materialización de una brecha, y establecer los mecanismos de reacción ante la misma para así minimizar los riesgos para los derechos y libertades de los afectados[28].

J. TRANSFERENCIAS INTERNACIONALES Y EL CONTEXTO NORMATIVO INTERNACIONAL

De la mano del uso de infraestructuras tecnológicas de encargados del tratamiento y del uso combinado de múltiples tecnologías, muchas veces con subencargados del tratamiento e infraestructuras tecnológicas en la nube, existe la posibilidad de que el tratamiento suponga transferencias internacionales de datos a países fuera del Espacio Económico Europeo (EEE).

En situaciones en los que se produzcan transferencias internacionales de datos, el responsable debe valorar escenarios como quiebras del estado de derecho, emergencias nacionales o internacionales o crisis en las relaciones y acuerdos internacionales.

Ejemplo:
Un tratamiento que incorpore Wi-Fi tracking, que posibilite la vinculación de una persona con la sede de un partido político o sindicato vinculado a una ideología determinada, que utilice encargados de tratamiento con tecnologías en la nube, podría implicar transferencias internacionales de datos a terceros países. La posibilidad de identificarla podría implicar consecuencias, incluso legales, sobre las personas (por ejemplo, denegación de un visado o imputación de cargos penales).

[28] Considerando 83 RGPD: …Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

K. CONCLUSIÓN SOBRE LA GESTIÓN DEL RIESGO

El responsable debe tener en cuenta y gestionar todos los riesgos para los derechos y libertades fundamentales de los interesados aplicables en el tratamiento, revisando cada una de las amenazas, cómo pueden afectar a los derechos fundamentales, teniendo en cuenta el caso concreto en su contexto, ámbito, naturaleza y fines, y analizando el tratamiento completo, no únicamente algunas de las operaciones de tratamiento.

A menudo los riesgos están vinculados entre sí, y la materialización de algunas amenazas o factores de riesgo implica que otros también puedan materializarse.

Las medidas técnicas y organizativas para minimizar estos riesgos serán abordadas en un apartado específico posterior.

6. OBLIGACIÓN DE LLEVAR A CABO UNA EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

El RGPD establece las obligaciones relacionadas con la evaluación de impacto relativa a la protección de datos (EIPD) en los artículos 35 y 36. No obliga a hacer una EIPD a cualquier tratamiento de datos personales, pero sí a aquellos en los que sea probable que entrañe un alto riesgo.

La existencia de un grado razonable de presunción de que el tratamiento puede entrañar un alto riesgo hace imprescindible la realización de una EIPD.

La EIPD es un proceso de evaluación de un tratamiento que se extiende en el tiempo, a lo largo de todo su ciclo de vida, y que debe revisarse de forma continua, como mínimo cuando exista un cambio del riesgo que representen las operaciones de tratamiento. En ningún caso debe considerarse un mero formalismo documental.

En términos generales, **una EIPD**:

- Es exigible cuando pueda haber alto riesgo para derechos y libertades.
- Es una obligación específica del responsable.
- Exige superar una evaluación de la idoneidad, necesidad y proporcionalidad del tratamiento con relación a sus fines.
- Exige que la evaluación determine que se ha conseguido reducir el riesgo residual mediante la aplicación de medidas y garantías a un nivel tolerable.
- Exige su realización antes del inicio de las actividades de tratamiento.
- Exige el asesoramiento del DPD cuando deba estar designado o lo haya sido a voluntad del responsable.
- Tendrá en cuenta el cumplimiento de los códigos de conducta aprobados y certificaciones que fueran aplicables.

- Su resultado se debe tener en cuenta para evaluar la viabilidad o inviabilidad del tratamiento desde el punto de vista de la protección de datos. El resultado de la EIPD es vinculante para el responsable del tratamiento, y en función del nivel de riesgo residual obliga a realizar una consulta previa a la autoridad de control de protección de datos competente o incluso a decidir no llevar a cabo el tratamiento.

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[29] 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.[30]

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, también será necesaria realizar una EIPD.

Algunos de los criterios relevantes de esta lista para **tratamientos que incorporen Wi-Fi tracking** son:

- que impliquen la **observación, monitorización, supervisión, geolocalización o control** del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

- que impliquen el **uso de categorías especiales de datos** a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

- que impliquen el **uso de datos a gran escala**. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "Directrices sobre los delegados de protección de datos (DPD)" del Grupo de Trabajo del Artículo 29.

- que impliquen la **asociación, combinación o enlace de registros de bases de datos** de dos o más tratamientos con finalidades diferentes o por responsables distintos.

- que impliquen la **utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas**, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

[29] WP243 explica el término gran escala y no exclusivamente en términos absolutos del número de interesados.
[30] Considerando 91 del Reglamento General de Protección de Datos.
[31] Guía Gestión del riesgo y evaluación de impacto en tratamientos de datos personales – Apartado XIII. Evaluación de la necesidad y proporcionalidad del tratamiento.

Estos criterios deben tenerse en cuenta tanto para el propio responsable del tratamiento como para el encargado o encargados de tratamiento utilizados por el responsable.

Conviene además recordar la obligación de encargados y subencargados de ayudar al responsable en la realización de la EIPD y la diligencia debida de los responsables en la contratación de encargados que ofrezcan garantías adecuadas. Dados los factores y elementos de riesgo inherentes a la utilización de la tecnología Wi-Fi tracking expuestos en esta guía, en general, se cumplirán las condiciones para que la EIPD sea obligatoria en tratamientos de datos personales que empleen tecnología Wi-Fi tracking. Incluso en aquellos casos en los que el responsable pueda no tener clara la obligatoriedad de realizar una EIPD, lo que no excluye el análisis y actualización de los riesgos asociados, la recomendación de las autoridades de control de protección de datos, dados los factores de riesgo expuestos en esta guía, es llevarla a cabo.

Finalmente, cabe recordar que cuando proceda, el responsable deberá recabar la opinión de los interesados o de sus representantes en relación con el tratamiento previsto. En particular, en el ámbito de las administraciones públicas 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.

7. EVALUACIÓN DE LA NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

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[31].

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.

Ejemplo

Un responsable pretende controlar el aforo máximo de un local con la finalidad de garantizar la seguridad de las personas. En la implementación del tratamiento podría decidir utilizar elementos básicos para el conteo de personas que entran/salen del local, utilizar medios humanos, o cualquier otro conjunto de sensores, volumétricos, de CO2, células fotoeléctricas, de presión, videovigilancia con algún grado de análisis o utilizar tecnología Wi-Fi tracking. Aun persiguiendo la misma finalidad en todos los casos, algunas de las opciones no implican en principio un tratamiento de datos personales, mientras que otras pueden implicar tratamientos de datos personales con distinto grado de intrusismo en la privacidad de las personas, incluso podríamos hablar de tratamientos de alto riesgo para los derechos y libertades de las personas físicas, y será necesario determinar la necesidad y la proporcionalidad de las distintas opciones disponibles.

A. EVALUACIÓN OBJETIVA DE LA IDONEIDAD DEL TRATAMIENTO

A la hora de definir los requisitos del tratamiento que se podría implementar con Wi-Fi tracking hay que determinar si la calidad del dato que puede obtenerse mediante esta tecnología es idónea para ejecutar las acciones necesarias del tratamiento, teniendo en cuenta que no va a ser infalible.

Ejemplo:
Sea un tratamiento para aplicar una obligación legal de que no más de 30 personas están en una determinada sala. Utilizando Wi-Fi tracking se puede dar la situación de que algunas personas pueden no llevar teléfono, ser menores sin teléfono, llevarlo desactivado para no ser contabilizados o sin batería, otros pueden llevar dos o más móviles (personal, profesional, etc.) y todo ello puede depender de la edad, del tipo de servicio, de la actividad previamente realizada y otros. Por lo que dicho sistema no sería idóneo.

Ejemplo:
Sea un tratamiento para tomar decisiones sobre ampliar superficie o personal en un servicio de atención al cliente. Para ello se quiere obtener una estadística de ocupación de un determinado local o sala de espera. En primer lugar, hay que determinar el nivel y grado de confianza del dato que permite tomar una decisión, por ejemplo, de un 90% +- 2%.

Eso permitirá determinar qué métodos o tecnologías serán adecuados.

B. EVALUACIÓN OBJETIVA DE LA NECESIDAD DEL TRATAMIENTO

En función de la finalidad del tratamiento, cierto grado de singularización puede ser intrínsecamente necesario para cumplir con los fines del tratamiento, pero en otras ocasiones la singularización no será necesaria para la finalidad que se persigue.

Ejemplo:
Un tratamiento que incorpora Wi-Fi tracking en una tienda física con varias estancias y cuya única finalidad es determinar el aforo de cada estancia para no superar el aforo máximo, en principio no necesitaría singularizar a las personas en modo alguno. Bastaría con determinar el número total de dispositivos presentes en cada momento. Podría ser incluso innecesario tratar cualquier identificador sino solo llevar un conteo de las tramas Probe Request que se están generando.

Sin embargo, un tratamiento similar en un museo en el que se pretende obtener los recorridos habituales entre estancias necesitará singularizar a los individuos como mínimo durante determinados periodos de tiempo y antes de anonimizar los datos para determinar, por ejemplo, el orden de visita de las estancias de cada individuo o un mapa de calor de los espacios más transitados.

En cualquier caso, para tratamientos que ya se estén realizando y se decida realizar una actualización tecnológica que implique un mayor intrusismo en la privacidad de los usuarios, habrá que plantearse qué necesidad se está cubriendo que antes no se alcanzaba dentro de unos márgenes de efectividad razonables:

Ejemplo:
Se pretende actualizar el control de presencia utilizando Wi-Fi tracking. El control de presencia es un tratamiento que se viene realizando por muchos años con un grado de eficacia razonable. Hay que plantearse la necesidad de cambiar a una tecnología más intrusiva que puede incorporar además limitaciones en su eficacia y posibilidades de fraude que no se conocen.

Así mismo, a lo largo del ciclo de vida del tratamiento será necesario verificar que dichas necesidades siguen siendo conseguidas y siguen siendo necesarias para los fines objetivos del tratamiento, estableciendo caducidades para limitar la ejecución de un tratamiento que ya no diera respuesta a dichas necesidades.

8. MEDIDAS TÉCNICAS Y ORGANIZATIVAS APROPIADAS

Una vez identificados los factores de riesgo y determinado el nivel de riesgo del tratamiento, se debe disminuir dicho nivel de riesgo a un valor aceptable a través de controles y medidas apropiadas de índole técnica y organizativa, políticas de protección de datos, protección de datos y privacidad desde el diseño y medidas de seguridad. Estas medidas deben estar orientadas a disminuir el impacto o la probabilidad de la materialización de uno o varios factores de riesgo específicos. Acumular medidas y garantías sin un objetivo específico pueden generar nuevas vulnerabilidades.

No obstante, no debe confundirse la gestión de riesgos para los derechos y libertades de los interesados con el estricto cumplimiento del resto de los preceptos y principios impuestos por la normativa de protección de datos. La naturaleza del RGPD da libertad al responsable y el encargado en el modo de implementar las garantías de cumplimiento de los principios y resto de obligaciones del RGPD, sin que esto implique que el responsable o el encargado puedan elegir qué preceptos cumplir y cuáles no. Una de las medidas de protección de datos desde el diseño a aplicar es la anonimización, pero ni es la única opción posible, ni el responsable debe renunciar a la aplicación de otras medidas adicionales como son la privacidad diferencial[32], "compute-to-data" y otras.

En su Informe jurídico 2019/017, la AEPD pone de manifiesto las obligaciones para responsables del tratamiento que utilicen la tecnología Wi-Fi tracking. Deben entenderse como obligaciones establecidas por la normativa de protección de datos y entre las que también pueden encontrase algunas **medidas técnicas y organizativas**. Se relacionan a continuación algunas de ellas:

- Deben adoptarse medidas que garanticen la anonimización[33] temprana de los datos.

[32] Anonimización y seudonimización (II): la privacidad diferencial

- Deberá valorarse el ámbito en el que se realiza el Wi-Fi tracking. Por ejemplo, en el ámbito privado se atenderá a la existencia de una relación comercial, de modo que se trate de clientes o potenciales clientes, evitándose, en todo caso, su empleo en la vía pública.

- Deberán limitarse y acotarse las zonas en las que se realiza, evitándose un control de los movimientos en zonas muy amplias, así como en aquellas que puedan suponer una injerencia excesiva en la privacidad de la persona, como pudiera ser, por ejemplo, en el caso de los aseos.

- No podrán utilizarse, sin el consentimiento de los afectados, en aquellas zonas en que puedan revelar categorías especiales de datos como, por ejemplo, las que tengan productos relacionados con la salud.

- En ningún caso se podrán cruzar los datos de geolocalización así obtenidos con otros datos procedentes de otras fuentes (como, por ejemplo, los pagos con tarjeta de crédito o las imágenes captadas por los sistemas de videovigilancia) que puedan permitir la identificación de la persona.

- Atendiendo al criterio de minimización de datos, aunque la recogida de datos tuviera que ser continua, el almacenaje y posteriores operaciones de tratamiento de la posición ha de limitarse a señalar las áreas indicadas como de interés impidiendo una recogida detallada y continua de los movimientos de los interesados.

- No se deberán cruzar los datos recogidos de un interesado en los locales de distintos responsables. Si el responsable dispone de varios locales, también deberán recogerse distintos identificadores.

- No se deberá asignar el mismo identificador a un mismo dispositivo móvil en las distintas visitas que en el tiempo realice a la misma ubicación.

- No se condicionará el acceso a la Wi-Fi del responsable al consentimiento en el tratamiento de datos mediante Wi-Fi tracking del interesado.

- Cuando la base jurídica del tratamiento sea el interés legítimo del responsable o el cumplimiento de una misión de interés público, se ha de permitir a los interesados ejercer su derecho de oposición mediante una opción de opt-out a la recogida de sus datos[34].

- Deberá garantizarse que las personas tienen pleno conocimiento de que se está procediendo al tratamiento de sus datos personales en cada momento que se produzca, así como el ejercicio de sus derechos en virtud del RGPD.

En la misma línea, se expresan la Comisión Nacional de Informática y Libertad de Francia (CNIL)[35] y el CEPD[36], en concreto, éste último indica además, las siguientes medidas:

- La anonimización deberá realizarse justo después de la recogida, de tal forma que volver a identificarlos esté técnicamente excluido.

[33] No confundir con seudonimización de los datos.
[34] El uso de probe requests con MACs aleatorias puede dificultar seriamente la posibilidad de ofrecer una opción de opt-out.[35] No confundir con seudonimización de los datos.
[35] CNIL: Audience and attendance measurement devices in spaces accessible to the public: the CNIL recalls the rules
[36] Dictamen 01/2017 sobre la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas (2002/58/CE) (GT29,WP247)

- Si la anonimización inmediata no fuese posible habida cuenta de la finalidad (por ejemplo, por estar registrando una trayectoria), los datos personales podrán ser tratados durante un periodo en el que no estén anonimizados únicamente en las siguientes condiciones:
  - la finalidad de la recogida de datos debe limitarse al mero recuento estadístico.
  - el seguimiento se limita en el tiempo y el espacio en la medida estrictamente necesaria para tal fin.
  - los datos se eliminan o anonimizan inmediatamente después.
  - existe la posibilidad efectiva de exclusión voluntaria

Los responsables del tratamiento también deben tomar otras medidas de mitigación para garantizar que no haya impacto en los derechos fundamentales de terceros, por ejemplo, proteger la privacidad de las personas que viven junto a un punto de recopilación.

En el apartado VIII. Controles para disminuir el riesgo de la Guía de Gestión del riesgo y evaluación de impacto en tratamientos de datos personales se presenta una panorámica completa de controles para disminuir el riesgo que pueden ser apropiados para cualquier tratamiento de datos personales. El responsable que decida implementar un tratamiento con tecnología Wi-Fi tracking deberá implementar todas aquellas que le sean de aplicación al tratamiento concreto que pretende llevar a cabo.

A continuación, se relacionan de forma no exhaustiva algunas medidas técnicas y organizativas relevantes que podrían ayudar a gestionar los riesgos en tratamientos que incorporen tecnología Wi-Fi tracking.

A. ANONIMIZACIÓN

La anonimización es un tratamiento de datos personales que genera, a partir de un conjunto de datos personales, un nuevo conjunto de información anónima.

Como todo tratamiento, ha de cumplir los principios del RGPD, entre ellos el de responsabilidad proactiva. Esto implica que el responsable ha de tomar las medidas adecuadas para ejecutar el tratamiento de anonimización con las garantías necesarias y, en particular, tiene que plantearse qué riesgo supone para las personas que el proceso de anonimización se pueda revertir.

La AEPD pone a disposición de los responsables diversas herramientas con amplia información sobre la anonimización de datos en el microsite de Innovación y Tecnología así como el Dictamen 05/2014 sobre técnicas de anonimización del Grupo de Trabajo del Artículo 29.

El tratamiento de anonimización no es un proceso trivial y comporta una probabilidad de reidentificación que depende de diversos factores, entre otros:

- Momento en el que se anonimizan los datos. En general, cuanto antes se produzca la anonimización de los datos, menor tratamiento de datos personales y menor es el riesgo para los interesados[37]. Sin embargo, para acometer determinadas finalidades en un tratamiento es posible que sea necesario anonimizar en fases más tardías. Por ejemplo, cuando lo que se pretende es seguir trayectorias de personas en un intervalo de tiempo importante, existe la posibilidad de que los datos se almacenen sin anonimizar durante periodos de tiempo prolongados. La anonimización tardía de los datos supone un aumento de algunos riesgos.

[37] Artículo 25.2 RGPD.

- Técnica de anonimización utilizada: Existe el riesgo de utilizar procedimientos de anonimización débiles y que puedan ser revertidos.

- Independientemente de la anonimización propuesta, se pueden dar circunstancias específicas como la existencia de áreas poco concurridas a ciertas horas o la disponibilidad de varios puntos de localización sobre un mismo dispositivo[38], donde sería sencillo identificar a la persona o incluso sus comportamientos.

Por todo ello, tras un tratamiento de anonimización el responsable debe determinar mediante análisis y pruebas prácticas que no es posible reidentificar el conjunto de datos. El responsable debe realizar un análisis de los riesgos de reidentificación y considerar las condiciones del peor caso, siendo conveniente que se realizasen por un tercero periódicamente. Si en esas condiciones se puede reidentificar todo o parte del conjunto de datos no cabe hablar de riesgo de reidentificación, simplemente dicho conjunto de datos no es anónimo.

En cuanto al momento en el que se realiza la anonimización, la anonimización temprana es la medida más eficaz para proteger los derechos y libertades de las personas.

Para ello es necesario acercar el proceso de anonimización al momento de adquisición de los datos tanto como sea posible. Un sistema que adquiera los datos personales y los anonimice en el punto de adquisición, antes de cualquier otro tipo de procesado e incluso antes de su almacenamiento, en general comportará menos riesgos para los derechos y libertades de las personas que un sistema que anonimice los datos pasados unas horas, días o meses.

En esencia, siempre que sea posible, la anonimización debe aplicarse de forma inmediata y lo más cerca posible al punto de recogida de los datos, preferiblemente de forma local en el dispositivo de captura.

En aquellos casos en los que la finalidad que se persigue exija retrasar el momento en el que se realizan las operaciones de anonimización, la seudonimización temprana deberá aplicarse hasta el momento en que la anonimización sea posible. Sin embargo, la seudonimización no puede ser un sustituto de la anonimización, ni la seudonimización de los datos justifica retrasar o no aplicar la anonimización de los datos.

B. ENMASCARAMIENTO DE DIRECCIONES MAC Y METADATOS

El enmascaramiento es una medida técnica de protección de datos ampliamente utilizada en tratamientos de datos personales. El enmascaramiento de identificadores únicos, como por ejemplo la dirección MAC, en el mismo momento de la captura de los datos y por el mismo interfaz de captura antes de que sean almacenados ni siquiera en logs, es una medida que en determinados escenarios puede resultar eficaz para dificultar la singularización e identificación de personas.

Ejemplo

Una dirección MAC tiene 24 bits que identifican al fabricante y 24 bits para asignación libre por el fabricante. Si se pretende controlar a distintas personas en un local, podría no ser necesario utilizar los 48 bits, es posible enmascarar desde el momento de la captura de los datos y utilizar únicamente un fragmento de la dirección MAC, por ejemplo los últimos 24 bits.

[38] de Montjoye, YA., Hidalgo, C., Verleysen, M. et al. Unique in the Crowd: The privacy bounds of human mobility. Sci Rep 3, 1376 (2013).

Si se pretende distinguir a 1000 personas a la vez, con 14 bits solo existirá un 6% de posibilidades de que dos coincidan. Si se pretende distinguir entre 100 personas, con 11 bits únicamente existirá un 5% de posibilidades que dos coincidan.

Sin embargo, esta técnica no será útil cuando la dirección MAC no sea el identificador empleado o los dispositivos envíen las tramas Probe Request con direcciones MAC aleatorias. Cuando lo que se utilice para identificar los dispositivos de usuario sea una huella digital, el enmascaramiento de los metadatos en el momento de la captura será la medida a aplicar para dificultar la singularización e identificación de personas.

C. DESVINCULACIÓN

Consiste en aplicar medidas que permitan desvincular los datos capturados en distintas zonas geográficas y en distintos periodos de tiempo.

Ejemplo:
Las huellas digitales del dispositivo (o cualquier otro identificador) se sustituyen por un hash con salt, con la particularidad de que se utiliza una salt distinta en cada ubicación y que cambia aleatoriamente cada cierto tiempo (cada 12/24 horas) El histórico de salts utilizadas no se almacena, al ser descartadas y eliminadas cada vez que se genera una nueva.

D. AGREGACIÓN

Consiste en agrupar la información relativa a varios sujetos utilizando técnicas de generalización y supresión[39]. Se utiliza cuando no se requieren registros individuales y los datos agregados son suficientes para el propósito que se persigue, como puede ocurrir en algunos tratamientos que utilicen Wi-Fi tracking.

Ejemplo:
Para obtener mapas de calor sobre las principales trayectorias seguidas por las personas en un Museo no harían falta identificadores únicos, bastaría con un simple recuento estadístico.

E. MINIMIZACIÓN DE DATOS

Consiste en adoptar medidas destinadas a garantizar el cumplimiento del principio de minimización de datos establecido en el RGPD (los datos personales serán “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”) en el diseño de tratamientos que utilicen Wi-Fi tracking.

[39] La k-anonimidad como medida de la privacidad.

Ejemplos prácticos de ello serían:

- Limitar el periodo de actividad de los sensores al mínimo imprescindible.
- Limitar el área sujeta a Wi-FI tracking, evitando incluir zonas privadas.
- Limitar al máximo el área sujeta a monitorización de las trayectorias de la personas[40].
- Evitar la captura y almacenamiento de datos de las tramas Wi-Fi que faciliten la identificación de las personas (por ejemplo, el SSID).
- Evitar la captura de datos procedentes de determinados tipos de dispositivos (dispositivos fijos, sensores IOT, implantes corporales/sanitarios, etc.)

F. PLAZO DE CONSERVACIÓN DE DATOS

Como en cualquier tratamiento de datos personales, tiene especial relevancia la limitación efectiva del plazo de conservación de los datos, tanto los no anonimizados como los anonimizados por el riesgo residual de reidentificación.

G. MEDIDAS DE SEGURIDAD Y AUDITORÍA POR TERCEROS

Las medidas de seguridad han entenderse en un sentido amplio. En caso de tratamientos puestos en marcha por Administraciones Públicas, los sistemas de información utilizados estarán sometidos al Esquema Nacional de Seguridad (ENS)[41] en la categoría correspondiente al nivel de riesgo para los derechos y libertades según la correspondiente EIPD. Esta obligación incluye igualmente a sistemas de información de las entidades del sector privado, cuando presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. Las medidas adecuadas de seguridad no se limitan a aquellas enumeradas en el ENS, sino que se deben extender, si cabe, a las necesarias para garantizar un nivel de seguridad adecuado al riesgo para los derechos y libertades fundamentales de cada tratamiento específico de acuerdo al artículo 32 del RGPD.

En caso de tratamientos que no estén sometidos a la obligación de cumplimiento del ENS, se tendrán que implementar las medidas necesarias para gestionar el nivel de riesgo para los derechos y libertades fundamentales de cada tratamiento específico de acuerdo al artículo 32 del RGPD.

Hay que recordar que el artículo 32 del RGPD, en su apartado 1.d), exige un proceso de verificación, evaluación y valoración regulares de las medidas de seguridad.

Auditorias independientes por terceros ayudan a demostrar el cumplimiento de las medidas de seguridad adecuadas al nivel de riesgo para los derechos fundamentales.

[40] Únicamente cuando sea necesario monitorizar trayectorias para la finalidad que se persigue con el tratamiento.

[41] Disposición adicional primera LOPDGDD: "Medidas de seguridad en el ámbito del sector público: 2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan a las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado."

H. MEDIDAS ORGANIZATIVAS Y SOBRE LOS ENCARGADOS DEL TRATAMIENTO

El RGPD obliga a los responsables a mantener diligencia debida para garantizar que el tratamiento se ajusta a la normativa de protección de datos y estar en condiciones de demostrarlo. El responsable deberá seleccionar encargados de tratamiento con garantías suficientes para aplicar medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con los requisitos del RGPD. Esta previsión se extiende también a los encargados cuando subcontraten operaciones de tratamiento con otros subencargados.

El tratamiento por el encargado deberá regirse por un contrato o cualquier otro vinculo legal equivalente. Así mismo, el encargado no podrá tratar los datos para finalidades propias, sino únicamente siguiendo las instrucciones documentadas del responsable, y evitando transferencias internacionales de datos sin garantías suficientes.

Siguiendo las obligaciones del RGPD para los contratos de encargo del tratamiento, estos deben contener explícitamente cláusulas que impidan recurrir a otro encargado sin la autorización previa por escrito del responsable y el tratamiento de los datos personales por parte del encargado del tratamiento para finalidades propias, o en su caso que limiten y condicionen qué tratamientos compatibles con la finalidad del tratamiento inicial puede realizar el encargado por cuenta propia. Además, deben establecer explícitamente la respuesta a una brecha de datos personales que pueda producirse en el encargado, tanto para el tratamiento realizado por cuenta del responsable como para posibles tratamientos propios del encargado.

El responsable debe asegurarse de impedir transferencias internacionales de datos sin garantías adecuadas.

Igualmente, los responsables deben implantar medidas de protección de datos desde el diseño y por defecto para minimizar los riesgos sobre los derechos y libertades que podría causar una brecha de datos personales. En cuanto a las medidas de seguridad, es preciso recordar que, según la experiencia y la doctrina del Tribunal Supremo , suponen una obligación de medios, pero no de fines.

En general, en tratamientos de datos personales que utilicen Wi-Fi tracking es especialmente importante considerar la probabilidad de que ocurra una brecha de confidencialidad, por lo que el responsable deberá adoptar medidas a priori para minimizar los riesgos sobre los interesados y en el caso que sucedan tener prevista la respuesta del responsable y encargados para minimizar el impacto sobre los derechos y libertades de las personas.

Es importante identificar de antemano el grado de responsabilidad de cada uno de los intervinientes en el tratamiento en los distintos escenarios en los que se pueda producir una brecha de confidencialidad, y qué obligaciones acometerá cada uno de ellos para gestionar adecuadamente la brecha, incluyendo las obligaciones de notificación a la autoridad de control de protección de datos competente y comunicación a los afectados, cuando sean obligatorias.

[42] C.G.P.J - Noticias Judiciales (poderjudicial.es)

I. GESTIÓN CONTINUA DEL RIESGO

El responsable del tratamiento debe analizar los riesgos del tratamiento atendiendo a todas sus particularidades y circunstancias, y si en algún momento se produce un cambio en el tratamiento o en factores que afecten al tratamiento, los riesgos deberán volver a ser evaluados y gestionados.

El RGPD, (artículo 24) y la Ley Orgánica 7/2021 (artículo 27 que traspone el artículo 19 de la Directiva 680/2016) exigen que el responsable del tratamiento revise y actualice las medidas implantadas en el tratamiento para garantizar que cumple con la normativa de protección de datos. La propia norma establece que hay que llevar a cabo dicha revisión y actualización cuando resulte necesario[43].

9. TRANSPARENCIA E INFORMACIÓN

Debe considerarse que el uso de la tecnología Wi-Fi tracking en la que se recoge información como resultado de la comunicación entre un terminal (teléfono móvil o cualquier otro dispositivo) de una persona física y una red Wi-Fi, a fin de generar una huella digital del dispositivo que lo diferencie del resto de terminales, puede suponer un tratamiento de datos personales, y por tanto el responsable y encargado del tratamiento deberán respetar los principios y derechos recogidos en el RGPD.

Entre esos principios, el artículo 5.1 a) del RGPD reconoce el principio de transparencia conjuntamente con los principios de licitud y lealtad.
La particularidad que implica que este tratamiento pueda pasar inadvertido a las personas titulares de los terminales hace más necesario aún el cumplimiento del principio de transparencia a través de una información clara y accesible.
El artículo 13 del RGPD detalla la información necesaria que deberá facilitarse al interesado cuando los datos personales se obtengan del mismo.

Las personas deberán ser previamente **informadas** en relación con los siguientes aspectos:

- Identidad y datos de contacto del responsable del tratamiento y, en su caso, de su representante.
- Datos de contacto del delegado o delegada de protección de datos.
- Fines y base jurídica del tratamiento.
- Intereses legítimos del responsable o de un tercero.
- Destinatarios o categorías de destinatarios de los datos personales.
- Transferencias internacionales previstas.
- Plazo de conservación.
- Derechos de acceso, rectificación o supresión, limitación del tratamiento, oposición y portabilidad.
- Posibilidad de revocación del consentimiento.
- Derecho a presentar una reclamación ante una autoridad de control.

[43] Cuándo hay que revisar las medidas de protección de datos.

A. INFORMACIÓN POR CAPAS

La información que se facilite debe ser concisa, transparente, accesible, fácil de entender y presentarse en un lenguaje claro y sencillo, en especial la dirigida específicamente a los niños y niñas.

Así, el artículo 11 de la LOPDGDD ha previsto que el responsable pueda dar cumplimiento al deber de información establecido en el artículo 13 del RGPD, facilitando al interesado una información básica, e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información (es lo que se ha venido a denominar "información por capas").

El **contenido mínimo** que debe tener la información básica es:

- La identidad del responsable del tratamiento.
- La finalidad del tratamiento.
- La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD.
- Información sobre si los datos personales obtenidos fueran a ser tratados para la elaboración de perfiles, y de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre el afectado o le afecten significativamente de modo similar, cuando concurra este derecho conforme al artículo 22 del RGPD.
- La información será facilitada por escrito u otros medios, incluso electrónicos, si procede. La información podrá facilitarse verbalmente, cuando lo solicite el interesado, siempre que se demuestre la identidad del solicitante por otros medios.

Las Directrices del Grupo de Trabajo del artículo 29 sobre la transparencia en virtud del RGPD, adoptadas el 29 de noviembre de 2017 (revisadas el 11 de abril de 2018), recogieron como **vías posibles de transmitir la información a los interesados**, en un entorno como el de Wi-Fi tracking la utilización de:

- paneles claramente visibles con información.
- señalización pública en toda el área de cobertura.
- campañas públicas de información.
- iconos (iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto, según art. 12.7 RGPD).
- alertas de voz.
- detalles por escrito incluidas en instrucciones de configuración.
- vídeos integrados en instrucciones digitales de configuración.
- información por escrito sobre dispositivos inteligentes, mensajes por SMS o correo electrónico.

En el caso concreto del empleo de estas tecnologías por parte de las administraciones públicas, se recomienda adicionalmente el siguiente conjunto de **medidas de transparencia**, mediante la publicación de[44]:

- Un registro de sensores de Wi-Fi tracking desplegados en la vía pública.
- Los objetivos concretos que se persiguen, indicando las fechas de inicio y de finalización del tratamiento.

[44] Más información en Investigation Report on the Protection of Personal Data in the Development of Dutch Smart Cities

- Un extracto adecuado (sin información sensible) de las evaluaciones de impacto que se realicen.
- La información relevante de los algoritmos de anonimización empleados.
- La información accesible en varios idiomas si fuera una zona de gran afluencia turística.

En cualquier caso, de conformidad con el artículo 31 LOPDGDD, los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del RGPD, salvo que sea de aplicación la excepción prevista en su apartado 5. Los sujetos enumerados en el artículo 77.1 LOPDGDD deberán hacer público un inventario de sus actividades de tratamiento accesible por medios electrónicos y su base legal.

10. EJERCICIO DE DERECHOS RECONOCIDOS EN EL RGPD

De conformidad con el artículo 11 del RGPD, si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, éste no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el RGPD, y en esos casos, si el responsable es capaz de demostrar que no está en condiciones de identificarle, le informará en consecuencia, de ser posible, y no serán de aplicación los artículos 15 a 20 del RGPD (derechos de acceso, de rectificación, de supresión, derecho a la limitación del tratamiento, y a la portabilidad de los datos), excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

Este será el caso cuando el responsable del tratamiento haya llevado a cabo un proceso de anonimización de los datos personales tratados y sea capaz de demostrar que no está en condiciones de identificar al interesado. Los artículos 15 a 20 del RGPD no serán de aplicación a los datos anonimizados, pero sí serán de aplicación a los datos personales que el responsable esté tratando en fases del tratamiento previas a su anonimización.

El responsable del tratamiento estará obligado a informar a la persona afectada sobre los medios a su disposición para ejercer los derechos reconocidos en los artículos 15 a 22 del RGPD. Los medios deberán ser fácilmente accesibles para la persona afectada. El responsable debe establecer mecanismos visibles, accesibles y sencillos, incluidos medios electrónicos, para el ejercicio de derechos.

Estos mecanismos, en particular, cuando se trate del ejercicio por medios electrónicos, deben incorporar procedimientos para verificar la identidad de las personas afectadas que los utilizan, así como de la recepción del ejercicio del correspondiente derecho, y su oportuna contestación.

A. DERECHO DE ACCESO (ARTÍCULO 15 RGPD)

El interesado tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la información que se detalla en el artículo 15.1 del RGPD.

Se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello (art. 13.3 LOPDGDD), ante lo cual el responsable del tratamiento podrá cobrar un canon razonable en función de los costes administrativos o negarse a actuar respecto de la solicitud.En todo caso, el interesado tiene derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, las categorías de datos personales, los destinatarios, el plazo de conservación, información sobre su origen, la existencia de decisiones automatizadas, incluida la elaboración de perfiles a que se refiere el artículo 22 del RGPD y, al menos en tales casos, información sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Incluso cuando el responsable haya llevado a cabo procesos de anonimización por los que no pueda identificar los datos del interesado y facilitarle una copia de sus datos personales objeto del tratamiento, sí deberá ofrecer toda la información necesaria sobre el tratamiento para cumplir con el principio de transparencia.

B. DERECHO DE SUPRESIÓN (ARTÍCULO 17 RGPD)

El interesado tiene derecho a obtener sin dilación indebida del responsable del tratamiento la **supresión de los datos personales** que le conciernen **cuando** concurra algunas de las circunstancias siguientes:

- Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
- La persona interesada retire el consentimiento en que se basa el tratamiento, de conformidad con el artículo 6.1.a), o el artículo 9.2.a), del RGPD y este no se base en otro fundamento jurídico.
- La persona interesada se oponga al tratamiento con arreglo al artículo 21.1 del RGPD, y no prevalezcan otros motivos legítimos para el tratamiento, o la persona interesada se oponga al tratamiento con arreglo al artículo 21.2 RGPD.
- Los datos personales hayan sido tratados ilícitamente.
- Los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
- Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8.1 RGPD.

Cuando el responsable del tratamiento haya hecho públicos los datos personales y concurriendo alguna de las circunstancias referidas, esté obligado a suprimir dichos datos, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén

tratando los datos personales de la solicitud, de la persona interesada, de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. No procederá la supresión de los datos personales en los supuestos contemplados en el artículo 17.3 del RGPD.

El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su supresión (artículo 32 LOPDGDD). Los datos bloqueados quedarán a disposición exclusiva de los jueces y tribunales, del Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y por el plazo de prescripción de las mismas. Transcurrido ese plazo deberá procederse a la destrucción de los datos. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de las así señaladas. Las autoridades de control podrán fijar excepciones a la obligación de bloqueo.

El responsable del tratamiento comunicará la supresión a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado, e informará al interesado acerca de dichos destinatarios si éste así lo solicita (artículo 19 RGPD).

C. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO (ARTÍCULO 18 RGPD)

Permite a la persona afectada solicitar al responsable del tratamiento que **suspenda el tratamiento de datos cuando**:

- Se impugne la exactitud de los datos, mientras se verifica dicha exactitud por el responsable.

- La persona afectada ha ejercitado su derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los de la persona afectada.

- Solicitar al responsable del tratamiento que conserve sus datos personales cuando:

  - El tratamiento de datos sea ilícito y la persona afectada se oponga a la supresión de sus datos y solicite en su lugar la limitación de su uso.

  - El responsable ya no necesita los datos para los fines del tratamiento, pero la persona afectada sí los necesite para la formulación, ejercicio o defensa de reclamaciones.

Limitado el tratamiento de los datos personales de la persona afectada, dichos datos sólo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento de la propia persona afectada o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un Estado miembro.

El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable del tratamiento (artículo 16.2 LOPDGDD).

Toda persona interesada que haya obtenido la limitación del tratamiento será informada por el responsable antes del levantamiento de dicha limitación. El responsable del tratamiento comunicará la limitación a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado, e informará al interesado acerca de dichos destinatarios si éste así lo solicita (artículo 19 RGPD).

D. DERECHO A LA PORTABILIDAD DE LOS DATOS (ARTÍCULO 20 RGPD)

El interesado tiene derecho a recibir los datos facilitados al responsable de tratamiento en un formato estructurado, de uso común y lectura mecánica, así como que los datos cedidos a un responsable de tratamiento puedan ser transmitidos directamente a otro responsable, siempre que el tratamiento esté basado en el consentimiento del interesado o en el marco de la ejecución de un contrato y que dicho tratamiento se efectúe por medios automatizados.

No obstante, este derecho no se aplicará cuando el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos concedidos al responsable del tratamiento.

E. DERECHO DE OPOSICIÓN (ARTÍCULO 21 RGPD)

El interesado tiene derecho a oponerse en cualquier momento, por motivos relacionados con su situación personal, a que los datos personales que le conciernan sean objeto de un tratamiento por el responsable basado en lo dispuesto en el artículo 6.1, letras e) y f) del RGPD, incluida la elaboración de perfiles sobre la base de dichas disposiciones.

Ante el ejercicio del derecho de oposición, el responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

El derecho de oposición debe comunicarse explícitamente a la persona interesada, presentándose claramente y al margen de cualquier otra información.

Se deberá facilitar a los interesados oponerse al tratamiento de manera sencilla.

Como una garantía adicional para reducir o mitigar el impacto sobre los interesados, a los que se recogen sus datos personales a través del Wi-Fi tracking el responsable podría optar por posibilitar una “exclusión voluntaria” general, más allá de la propia oposición; cesando en el tratamiento de datos sin necesidad de justificación alguna.

F. DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA LA ELABORACIÓN DE PERFILES (ARTÍCULO 22 RGPD)

La propia naturaleza de la tecnología Wi-Fi tracking hace viable llevar a cabo tratamientos basados en la misma que impliquen la toma de decisiones automatizadas, incluida la elaboración de perfiles.

El interesado tiene derecho a no ser objeto de una decisión realizada por el responsable del tratamiento basada únicamente en el tratamiento automatizado de su información de carácter personal, incluida la elaboración de perfiles, que produzca efectos jurídicos en ella o le afecte significativamente de modo similar.

No obstante, **será lícito efectuar el tratamiento y tomar una decisión automatizada**:

- Cuando sea necesaria para la celebración o la ejecución de un contrato entre la persona interesada y un responsable del tratamiento o cuando se basa en el consentimiento explícito de la persona interesada.

- Cuando está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de la persona interesada.

En ambos casos, el responsable deberá adoptar las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de la persona interesada, como mínimo, el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

En estos tratamientos no se emplearán categorías especiales de datos personales contempladas en el artículo 9.1 RGPD, salvo que el tratamiento se realice mediante el consentimiento de la persona interesada o se trate de un interés público esencial impuesto por el Derecho de la Unión o del Estado miembro. En estos casos, se asegurará que se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de la persona interesada.

11. REGLAMENTO DE INTELIGENCIA ARTIFICIAL

Dada la situación tecnológica actual, es posible que se realicen tratamientos de datos personales en los que se combine el uso de la tecnología Wi-Fi tracking y sistemas de inteligencia artificial (IA). Este tipo de tratamientos de datos personales está sujeto al sistema de principios, obligaciones para los responsables y derechos para los interesados que establece el RGPD. Adicionalmente, el uso de determinados sistemas de IA se encontrará regulado por el Reglamento de Inteligencia Artificial (RIA).

En el momento de la publicación de esta Guía, aún no ha sido publicado el Reglamento de Inteligencia Artificial (RIA), el cual entrará en vigor en el plazo de 20 días tras su publicación y será aplicable en la mayoría de sus disposiciones a los dos años de esta.

Desde la perspectiva de la protección de datos personales, el RIA no tiene por objeto afectar a la aplicación del derecho fundamental a la protección de datos. El RIA es complementario al RGPD y se aplicará sin perjuicio del mismo con el propósito de permitir que responsables y los encargados estén en condiciones de cumplir sus obligaciones en materia de protección de datos cuando incorporan sistemas de IA en sus tratamientos (considerando 78 RGPD) para implementar la protección de datos desde el diseño del tratamiento.

Por ello, la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA deben facilitar la aplicación efectiva y permitir el ejercicio de los derechos y otras vías de recurso de los interesados garantizados por la normativa de protección de datos, así como de otros derechos fundamentales.

Esto incluye las obligaciones de proveedores y responsables del despliegue, o de otros intervinientes y operadores cuando proceda, de sistemas de IA en la medida en que el diseño, el desarrollo o el uso de sistemas de IA impliquen el tratamiento de datos personales, así como las funciones y competencias de las autoridades de control independientes de protección de datos. Entre otras, estas últimas tendrán la facultad de solicitar cualquier documentación creada o

conservada con arreglo al RIA relativa a sistemas de IA de alto riesgo mencionados en el anexo III de ese Reglamento cuando el acceso a dicha documentación sea necesario para el cumplimiento efectivo de sus competencias.

También conviene aclarar que los interesados siguen disfrutando de todos los derechos y garantías que les confiere la normativa de protección de datos, incluidos los derechos relacionados con las decisiones individuales totalmente automatizadas, como la elaboración de perfiles.

En este sentido, como ejemplo, cuando partiendo de los datos obtenidos mediante la tecnología Wi-Fi tracking como información de entrada, se implementen decisiones que produzcan efectos jurídicos a una persona o le afecten significativamente mediante sistemas de inteligencia artificial (con independencia del tipo que sean) basadas únicamente en el tratamiento automatizado de datos personales, se aplicará lo ya previsto en el RGPD (artículos 13,14,15 y 22 y considerando 71 RGPD).

Además, para este supuesto, en el caso concreto de que el sistema de inteligencia artificial en el que se basa la decisión fuese de alto riesgo de acuerdo con el RIA, de manera complementaria a los derechos contemplados en el RGPD, cuando la persona considerase que la decisión tiene un impacto adverso sobre su salud, seguridad o sus derechos fundamentales, será de aplicación lo previsto en la Regulación de IA en relación a que la persona afectada pueda tener derecho a recibir explicaciones claras y significativas sobre el papel del sistema de inteligencia artificial en el procedimiento de toma de decisiones y los principales elementos de la decisión adoptada.


aepd
agencia
española
protección
datos


apdcat
Autoritat Catalana de
Protecció de Dades


Datuak Babesteko
Euskal Agintaritza
Autoridad Vasca de
Protección de Datos


Consejo de Transparencia
y Protección de Datos
de Andalucía