DIRECTRICES EDPB 2/2023 SOBRE EL ALCANCE TÉCNICO DEL ART. 5(3) DE LA DIRECTIVA EPRIVACY

CONTEXTO

La Directiva ePrivacy, a través de su artículo 5.3 exige de forma exclusiva el consentimiento para el almacenamiento o acceso a cierto tipo de información. Es la normativa por la cual se exige consentimiento para la instalación o acceso a la información que proporcionan las cookies y a la que la industria de publicidad digital da generalmente cumplimiento vía la finalidad 1 del TCF "Almacenar la información en un dispositivo y/o acceder a ella".

El Comité Europeo de Protección de Datos (EDPB) es un organismo europeo independiente cuyos objetivos son garantizar la aplicación coherente de la regulación de protección de datos y promover la cooperación entre las autoridades de protección de datos de los Estados de la UE (las cuales, a su vez, forman parte del EDPB)

---

1. INTRODUCCIÓN

Las Directrices analizan diferentes soluciones técnicas que han ido surgiendo durante estos años, o ya eran aplicadas, en sustitución o complementación a la instalación o acceso a información a través de cookies. Así como analiza las diferentes nociones que se exigen para la aplicación de la normativa de referencia.

El artículo 5.3 de la Directiva ePrivacy expone lo siguiente: *"únicamente se permite el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado."*

El objetivo de las Directrices es llevar a cabo un análisis técnico del ámbito de aplicación del artículo 5.3 de la normativa de referencia, y en concreto, aclarar qué abarca la frase *"almacenar información o acceder a la información almacenada en el equipo terminal de un abonado o usuario".* En este sentido las nociones analizadas por el EDPB, son las de:

- Equipo terminal de un abonado o usuario
- Redes de comunicaciones electrónicas
- Obtención de acceso
- Información (siendo un concepto con mayor amplitud que el de datos personales)
- Información almacenada y almacenamiento.

A su vez, Las técnicas/tecnologías analizadas por el EDPB son las siguientes:

- Tracking vía pixels o URLs

- Capacidades de procesamiento local de un dispositivo
- Tracking realizado de forma exclusiva por IPs
- Información generada vía dispositivos IOT
- Identificadores únicos

---

2. NOCIONES/CONCEPTOS ANALIZADOS

El EDPB ha determinado que el artículo 5.3 de la Directica ePrivacy se aplicaría en caso de cumplirse varios criterios:

1. Las operaciones llevadas a cabo se realizan con "información" (*almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario)* lo cual es un concepto más amplio que el de datos personales
2. Las operaciones se refieren a un "equipo terminal" de un abonado o usuario
3. Las operaciones efectuadas se realizan en el contexto de una "prestación de servicios de comunicaciones electrónicas disponibles al público en redes públicas de comunicaciones".
4. Las operaciones constituyen "acceso" o un "almacenamiento" en el equipo terminal de un abonado o usuario. Además, el acceso o almacenamiento no tienen por qué producirse dentro de la misma comunicación y no necesitan ser realizados por la entidad que produce la comunicación (entidad que accede)

- **El concepto de "información"**

En relación con el concepto de "información" el EDPB considera que es un término de mayor amplitud y aplicabilidad al de datos personales, ya que entre otras, y en virtud del Considerando 24 de la normativa, (así como del artículo 5.3) hay casos protegidos por la normativa como el "almacenamiento de virus" que no implican tratamiento de datos personales pero que buscan proteger la esfera de privacidad de los usuarios (objetivo principal del artículo en cuestión). Lo anterior ha sido confirmado por el TJUE *"Esta protección se aplica a cualquier información almacenada en dichos equipos terminales, con independencia de que se trate o no de datos personales, y tiene por objeto, en particular, como se desprende de dicho considerando, proteger a los usuarios del riesgo de que se introduzcan identificadores ocultos y otros dispositivos similares en los equipos terminales de dichos usuarios sin su conocimiento"* así como por el Grupo de trabajo del artículo 29 (antiguo EDPB) en su Dictamen 9/2014 *"No es correcto interpretar que el tercero no necesita consentimiento para acceder a esta información simplemente porque no la ha almacenado. El requisito de consentimiento también se aplica cuando se accede a un valor de sólo lectura (por ejemplo, solicitar la dirección MAC de una interfaz de red a través de la API del sistema operativo)".*

Para concluir con lo anterior, el EDPB expone que "información" se refiere tanto a datos personales como no personales con independencia de cómo hayan sido almacenados y por quién. Es decir, si por una entidad externa (incluidas también otras entidades distintas de la que tiene acceso), por el usuario, por un fabricante o cualquier otro escenario.

- **El concepto de "equipo terminal de un abonado o usuario"**

Con relación al concepto de "equipo terminal" el EDPB parte de la definición dispuesta en la Directiva 2008/63/CE, de competencia en los mercados de equipos terminales de telecomunicaciones (ya que no se define en la directiva ePrivacy). *"El equipo conectado directa o indirectamente a la interfaz de una red pública de telecomunicaciones para transmitir, procesar o recibir*

información; en ambos casos (conexión directa o indirecta), la conexión podrá realizarse por cable, fibra óptica o vía electromagnética; la conexión será indirecta si se interpone un aparato entre el equipo terminal y la interfaz de la red pública. Se considerarán también como equipos terminales los equipos de las estaciones terrenas de comunicación por satélite". Es por ello que cuando un dispositivo no sea un punto final de una comunicación, y solo transmita información sin realizar ninguna modificación de dicha información, no se considerará equipo terminal.

Por otro lado, un equipo terminal puede estar compuesto por un numero de piezas de hardware que, en su conjunto, dan forma al equipo terminal. Pueden adoptar, o no, la forma del dispositivo con funciones de visualización, almacenamiento, procesamiento (por ejemplo, teléfonos inteligentes, ordenadores portátiles, coches conectados o televisores conectados, gafas inteligentes)

La Directiva ePrivacy reconoce la protección de la confidencialidad de la información almacenada en el equipo terminal de un usuario y la integridad de dicho equipo no se limita a la protección de la esfera privada de las personas físicas, sino que también afecta al derecho al respeto de su correspondencia o a los intereses legítimos de las personas jurídicas. Por ello, un equipo terminal que permita llevar a cabo esta correspondencia y los intereses legítimos de las personas jurídicas está protegido por la normativa de referencia. El usuario o abonado puede ser propietario del equipo terminal, alquilarlo o disponer de el de otro modo. Varios usuarios o abonados pueden compartir el mismo equipo terminal en el contexto de múltiples comunicaciones (por ejemplo, en el caso de un coche conectado) y una única comunicación puede implicar más de un equipo terminal. A su vez, la protección que dispone el ePrivacy al equipo terminal asociado al usuario o abonado implicado en la comunicación, no depende de si la comunicación electrónica ha sido iniciada por el usuario o incluso de si el usuario es consciente de dicha comunicación.

- **El concepto de redes de comunicaciones electrónicas**

El ámbito de aplicación de la normativa se refiere a *"la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad."* El concepto de red de comunicaciones electrónicas no se define en la normativa ePrivacy, es por ello el EDPB parte de la definición realizada en la Directiva 2018/1972 (Código Europeo de las Comunicaciones Electrónicas) *"red de comunicaciones electrónicas: los sistemas de transmisión, se basen o no en una infraestructura permanente o en una capacidad de administración centralizada, y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos de red que no son activos, que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes fijas (de conmutación de circuitos y de paquetes, incluido internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada".*

Según esta definición, una red de comunicaciones electrónicas es cualquier sistema de red que permita la transmisión de señales electrónicas entre sus nodos, independientemente de los equipos y protocolos utilizados. No dependiendo de la naturaleza pública o privada de la infraestructura, ni de la forma en que la red está desplegada o gestionada. Así como la definición incluye redes gestionadas o no por un operador, redes cogestionadas por un grupo de operadores, o incluso redes ad-hoc en las que un equipo terminal puede de forma dinámica unirse o abandonar una red electrónica mallada (inalámbrica) de otros equipos terminales (vía protocolos de transmisión de corto alcance). La definición, a su vez, no impone requisitos en cuanto al número de equipos terminales presentes en la red en un momento dado (por ello

también aplicaría a redes asíncronas en la que puede haber solo dos pares comunicándose- P2P. Siempre aplicaría la normativa cuando el protocolo de red permita la inclusión posterior de otros pares.) En este sentido, y por último, el EDPB expone que para que la normativa fuera aplicable sería necesaria la disponibilidad pública del servicio de comunicación que se realiza a través de la red de comunicaciones electrónicas (especificando además que el hecho de que la red se ponga a disposición de un subconjunto limitado del público- por ejemplo, abonados, de pago o no, sujetos a condiciones de elegibilidad- no convierte a dicha red en privada.

- **El concepto de "obtención de acceso"**

En este caso el EDPB parte del artículo 1 del ePrivacy, que marca el objetivo de la misma Directiva *"garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad."* En palabras del EDPB: la Directiva ePrivacy es un instrumento jurídico de preservación de la intimidad destinado a proteger la confidencialidad de las comunicaciones y la integridad de los dispositivos. El equipo terminal del usuario, o persona jurídica, forma parte de su esfera privada y acceder a la información almacenada en él sin su conocimiento puede suponer una grave intromisión en su intimidad. Por otro lado, no es necesario que el almacenamiento y el acceso se den acumulativamente para que se aplique el artículo 5.3 ya que La noción de "obtener acceso" es independiente de la noción de "almacenar información". Además, no es necesario que las dos operaciones sean realizadas por la misma entidad (haciendo referencia al Dictamen 9/2014) y, por lo tanto, la información almacenada por una parte (incluida la información almacenada por el usuario o el fabricante del dispositivo) a la que posteriormente acceda otra parte entra en el ámbito de aplicación de la normativa en cuestión (Siempre que la entidad que accede a la información almacenada en el equipo terminal tome activamente medidas para ello será de aplicación la normativa).

Ejemplos de lo anterior es enviar instrucciones específicas al equipo terminal para recibir de vuelta la información deseada (es el caso de las cookies a través de las llamadas HTTP) o cuando la entidad que accede distribuye software en el terminal del usuario que luego llamará, a través de la red, utilizando una API. Otros ejemplos serían incluir código JavaScript, dando instrucciones al navegador del usuario para que envíe la información objetivo del JavaScript. En algunos casos, la entidad que da instrucciones al terminal para que envíe los datos y la entidad que recibe la información pueden no ser la misma. Esto puede deberse a la provisión y/o uso de un mecanismo común entre las dos entidades. Por ejemplo, una entidad puede haber utilizado protocolos que implican el envío de información por parte del equipo terminal que puede ser recibida y/o procesada por una entidad diferenciada. En estas circunstancias, podría eguir aplicándose el artículo 5.3 de la normativa.

- **El concepto de "información almacenada" y de "almacenamiento"**

El EDPB explica que el almacenamiento se refiere a la colocación de información en un medio físico de almacenamiento que forma parte del equipo terminal de un usuario o abonado. Ello se realiza normalmente, mediante instrucciones al software del equipo terminal para que genere información específica. Esto incluye el uso de protocolos como el almacenamiento de cookies del navegador, independientemente de quién haya creado o instalado los protocolos en el equipo terminal. La normativa no diferencia, siendo por tanto indiferente para su aplicación, el tiempo en el que la información persiste en el equipo del usuario o la cantidad de información almacenada.

El soporte de hardware donde se almacene la información no es relevante para la normativa (HDD, SSD, RAM, caché de las CPUs) así como tampoco es relevante si es almacenamiento interno (conexión SATA), externo (USB) o a través de protocolos de red (dispositivos de almacenamiento conectados a la red que tengan funcionalidad equivalente a medios de almacenamiento local). Todos ellos son ejemplos y se considerarán parte del equipo terminal.

La información almacenada también puede ser aquella almacenada como resultado de sensores integrados en el termina, o producida a través de procesos y programas ejecutados en el equipo terminal (que pueden o no producir información dependiente o derivada de la información almacenada.)

3. TÉCNICAS/TECNOLOGÍAS ANALIZADAS. CASOS DE USO.

El EDPB ha analizado, de manera no exhaustiva, algunas técnicas o tecnologías que podrían estar sujetas a la aplicación del artículo 5.3 de la Directiva ePrivacy. Antes de ello, introducen la tipología de información que puede generarse a través, o no, de las técnicas analizadas.

Ejemplos de información generada podrían ser las direcciones MAC, direcciones IP del equipo terminal o a identificadores de sesión (SSRC, identificador Websocket), o a tokens de autenticación. También podría incluir información generada a través de mecanismos que proporcionan datos de contexto (como el encabezado HTTP, incluido el campo "aceptar" o el agente de usuario), mecanismos de almacenamiento en caché (como ETag o HSTS) u otras funcionalidades (las cookies son una de ellas). Otros mecanismos por los que aplicaciones locales instaladas en el terminal utilizan alguna información estrictamente dentro del terminal (APIs de los Sistemas Operativos de los smartphones- acceso a la cámara, micrófono, sensor GPS, acelerómetro, chip de radio, acceso a archivos locales, lista de contactos, acceso a identificadores, etc.). También podría aplicarse a la información generada por los navegadores web que procesan información almacenada o generada dentro del dispositivo (como cookies, almacenamiento local, WebSQL o incluso información proporcionada por los propios usuarios). El uso de este tipo de información estaría sujeto al ePrivacy cuando la información salga del dispositivo, o cuando se acceda a esta información, o a cualquier derivación de la misma, a través de redes de comunicaciones electrónicas.

- **Tracking vía Pixels o URLs**

El EDPB define los pixels de seguimiento como hipervínculos a incrustados recursos (normalmente un archivo de imagen) en un contenido como una página web o un correo electrónico. Se explica que los píxels no suelen cumplir ningún propósito relacionado con el contenido en sí, aduciendo que su única finalidad es establecer una comunicación por parte del cliente con el host del píxel, que de otro modo no se habría producido.

El propósito de los Pixels puede ser confirmar la lectura de un correo electrónico, enlazar con entidades para seguir el comportamiento de los usuarios así como para identificar el origen de su fuente de tráfico entrante (por ejemplo para que un retailer pueda identificar de cual de sus socios comerciales proviene un usuario que pueda realizar una compra y así pagar una comisión-marketing de afiliación)

El EDPB expone que siempre que un pixel o enlaces/URLs de seguimiento se haya distribuido a través de una red pública de comunicación se deberá cumplir con los requisitos expuestos por

el artículo 5.3 de la normativa ePrivacy ya que constituiría un almacenamiento en el equipo terminal del usuario de la red de comunicación, como mínimo a través del mecanismo de almacenamiento en caché. La inclusión de píxeles o enlaces/URLS de seguimiento constituye una instrucción al equipo terminal para que envíe de vuelta determinada información. A su vez, los pixeles de seguimiento de generación dinámica (normalmente a través de código JavaScript) también quedarían incluidos.

En conclusión, puede considerarse que la recogida de identificadores proporcionados por los píxeles y URLs de seguimiento constituyen una "obtención de acceso" en el sentido del artículo 5.3 de la Directiva ePrivacy (y por tanto se necesita consentimiento del usuario)

- **Información generada mediante las capacidades de procesamiento local de un dispositivo.**

Algunas tecnologías se basan en las capacidades de procesamiento local del dispositivo del usuario. La información generada se puede poner en disposición de determinados actores a través de APIs. Ejemplo de la anterior es APIs proporcionadas por el navegador web para el acceso remoto a información generada de forma local en el dispositivo del usuario. Si en algún momento la información procesada/generada localmente se pone a disposición/se envía a través de una red de comunicaciones electrónicas ello constituiría una "obtención de acceso a información ya almacenada" en el sentido del artículo 5.3 de la Directiva ePrivacy (y por tanto se necesita consentimiento del usuario).

- **Tracking realizado de forma exclusiva por IPs.**

El EDPB expone que algunos proveedores están desarrollando soluciones publicitarias que sólo se basan en la recopilación de la dirección IP para así rastrear la navegación del usuario (en algunos casos realizando Cross-site tracking. En ese contexto, podría aplicarse el artículo 5.3 de la normativa ePrivacy, aunque la instrucción de poner a disposición la IP haya sido cursada por una entidad distinta de la receptora.

A menos que la entidad pueda garantizar que la dirección IP no se origina en el equipo terminal de un usuario o abonado la obtención de acceso a las direcciones IP desencadenaría la aplicación del artículo 5.3. Por ello, según el EDPB, las IPv4 estáticas salientes originadas en el router de un usuario entrarían dentro del ámbito de aplicación, así como las direcciones IPV6, ya que están parcialmente definidas por el host. Un caso que parece quedar excluido por el EDPB serían aquellas IPs agrupadas por tecnología CGNAT ya que se agrupa a varios usuarios/abonados bajo la misma dirección IP pública.

- **Información generada vía dispositivos IOT**

El EDPB expone que los dispositivos IoT (Internet de las cosas) producen información de forma continua a lo largo del tiempo, por ejemplo a través de sensores integrados en el dispositivo. La información puede ser preprocesada localmente o no. Algunos dispositivos IoT tienen una conexión directa a una red de comunicación pública, por ejemplo mediante el uso de WIFI o de una tarjeta SIM. Estos dispositivos podrían recibir instrucciones del fabricante para transmitir la información recopilada, aunque almacenan localmente la información en caché hasta que, por ejemplo, haya una conexión disponible. Otros dispositivos IoT no tienen una conexión directa a una red de comunicación pública y pueden recibir instrucciones para transmitir información a otro dispositivo a través de una conexión punto a punto (por ejemplo, a través de Bluetooth). El otro dispositivo suele ser un smartphone que puede, o no, preprocesar la información antes de enviarla al servidor. En el primer caso, el dispositivo IoT, cuando está conectado a una red

pública de comunicaciones, se consideraría en sí mismo un terminal. El hecho de que la información se transmita o se almacene en caché para su presentación no cambia la naturaleza de dicha información.

En ambas situaciones sería de aplicación el artículo 5.3 de la Directiva ePrivacy, ya que, mediante la instrucción del dispositivo IOT de enviar los datos almacenados se produce una "obtención de acceso". En el caso de dispositivos IoT conectados a la red a través de un dispositivo de transmisión (un smartphone, hub dedicado, etc.) con una conexión puramente punto a punto entre el dispositivo IoT y el dispositivo de transmisión, la transmisión de datos al dispositivo de transmisión podría quedar fuera del ámbito del artículo5.3, ya que la comunicación no tiene lugar en una red de comunicación pública. Sin embargo, la información recibida por el dispositivo de transmisión se consideraría almacenada por un terminal y, por tanto, se aplicaría el artículo 5.3 en cuanto se ordenara a ese dispositivo de transmisión el envío de esa información a un servidor remoto.

- **Identificadores Únicos.**

El EDPB expone que una herramienta común utilizada por las empresas de publicidad es la noción de "identificadores únicos" o "identificadores persistentes". Estos identificadores suelen derivarse de datos personales persistentes (nombre y apellidos, correo electrónico, número de teléfono, etc.), que se codifican en el dispositivo del usuario, se recopilan y se comparten entre varias entidades para así identificar de forma exclusiva a una persona en diferentes conjuntos de datos (datos de uso recopilados mediante el uso de un sitio web o una aplicación, datos de gestión de relaciones con los clientes-CRM-,relacionados con la compra o suscripciones online u offline etc.) En los sitios web, los datos personales persistentes se obtienen generalmente en el contexto de la autenticación o la suscripción a newsletters.

El EDPB expone que, el hecho de que la información sea aportada por el usuario no impediría la aplicación del artículo 5.3 de la Directiva ePrivacy en lo que respecta al almacenamiento, ya que esta información se almacena temporalmente en el terminal antes de ser recopilada. Así, la recogida de "identificadores únicos" en páginas web o aplicaciones móviles se encontraría dentro del ámbito de aplicación del artículo 5.3 ya que se está produciendo una "obtención de acceso" cuando la entidad que recoge los datos está dando instrucciones al navegador (mediante la distribución de código client-side) para que envíe esa información.