Directrices 2/2023 relativas al ámbito de aplicación técnico del artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas (Directiva ePrivacy)

Versión 2.0

Adoptado el 7 de octubre de 2024

Historial de versiones

Versión 1.0	14 de noviembre de 2023	Adopción de las Directrices para consulta pública
Versión 2.0	7 de octubre de 2024	Adopción de las Directrices tras la consulta pública

Resumen Ejecutivo

En las presentes Directrices, el CEPD aborda la aplicabilidad del artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas a diferentes soluciones técnicas (Directiva ePrivacy). Las presentes Directrices amplían el Dictamen 9/2014 del Grupo de Trabajo del Artículo 29 sobre la aplicación de la Directiva ePrivacy a la toma de impresiones dactilares mediante dispositivos y tienen por objeto describir de forma clara las operaciones técnicas contempladas en el artículo 5, apartado 3, de la Directiva ePrivacy.

La aparición de nuevos métodos de rastreo para sustituir las herramientas de rastreo existentes hasta la fecha (por ejemplo, las *cookies*, debido a que algunos navegadores han dejado de ser compatibles con las *cookies* de terceros) y para crear nuevos modelos de negocio se ha convertido en un motivo de preocupación primordial en lo que a la protección de datos se refiere. Si bien la aplicabilidad del artículo 5, apartado 3, de la Directiva ePrivacy está bien establecida y este se aplica a algunas tecnologías de rastreo, como las *cookies*, es necesario abordar las ambigüedades relacionadas con la aplicación de dicha disposición a las herramientas de rastreo emergentes.

Las Directrices establecen tres elementos clave para la aplicabilidad del artículo 5, apartado 3, de la Directiva ePrivacy (sección 2.1), a saber, la «información», el «equipo terminal de un abonado o usuario» y la «obtención de acceso a información almacenada o el almacenamiento de información». Además, las Directrices proporcionan un análisis detallado de cada elemento (secciones 2.2-2.6).

En la sección 3, dicho análisis se aplica a una lista no exhaustiva de casos de uso que representan técnicas comunes, a saber:

- Las URL y el rastreo mediante píxeles
- El tratamiento local
- El rastreo basado únicamente en la dirección IP
- La información intermitente y mediada del Internet de las Cosas (IdC)
- Los identificadores únicos

Índice

El Comité Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra e), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, «el RGPD»),

Visto el Acuerdo sobre el Espacio Económico Europeo y, en particular, su anexo XI y su Protocolo 37, modificado por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[1],

Visto el artículo 15, apartado 3, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la privacidad en el sector de las comunicaciones electrónicas, modificada por la Directiva 2009/136/CE (en lo sucesivo, «la Directiva sobre la privacidad y las comunicaciones electrónicas» o «la Directiva ePrivacy»),

Vistos los artículos 12 y 22 de su Reglamento interno,

HA ADOPTADO LAS SIGUIENTES DIRECTRICES:

1 INTRODUCCIÓN

1. De conformidad con el artículo 5, apartado 3, de la *Directiva ePrivacy, el almacenamiento de información o la obtención de acceso a la información almacenada en el equipo terminal de un abonado o* usuario solo se permite sobre la base del consentimiento o la necesidad para los fines específicos establecidos en dicho artículo. Como se recuerda en el considerando 24 de la Directiva ePrivacy[2], el objetivo de esta disposición es proteger los equipos terminales de los usuarios, ya que forman parte de la esfera privada de los usuarios. De la redacción del propio artículo se desprende que el artículo 5, apartado 3, de la Directiva ePrivacy no se aplica exclusivamente a las *cookies*, sino también a las tecnologías similares. Sin embargo, actualmente no existe una lista exhaustiva de las operaciones técnicas cubiertas por el artículo 5, apartado 3, de la Directiva ePrivacy.

2. El Dictamen 9/2014 del Grupo de Trabajo del Artículo 29 (en lo sucesivo, «el GT29») sobre la aplicación de la Directiva ePrivacy a la toma de impresiones dactilares mediante dispositivos (en lo sucesivo, «el Dictamen 9/2014 del GT29») ya aclaró que la toma de impresiones dactilares entra dentro del ámbito de aplicación técnico del artículo 5, apartado 3, de la Directiva ePrivacy[3]; no obstante, debido a los nuevos avances tecnológicos, es necesaria una mayor orientación con respecto a las técnicas de

[1] Las referencias a «los Estados miembros» realizadas en el presente documento deben entenderse como referencias a «los Estados miembros del EEE».

[2] «Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Los denominados «programas espía» (*spyware*), *web bugs*, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios. Solo debe permitirse la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados.»

[3] Dictamen 9/2014 del GT29, p. 11.

rastreo que se observan actualmente. El panorama técnico ha ido evolucionando durante la última década, con un uso creciente de identificadores integrados en los sistemas operativos, así como la creación de nuevas herramientas que permiten almacenar información en los equipos terminales.

3. Las ambigüedades relativas al ámbito de aplicación del artículo 5, apartado 3, de la Directiva ePrivacy han incentivado la aplicación de soluciones alternativas para el rastreo de los usuarios de internet y han dado lugar a una tendencia a eludir las obligaciones legales previstas en el artículo 5, apartado 3, de la Directiva ePrivacy. Todas estas situaciones suscitan preocupación y requieren un análisis adicional para complementar las orientaciones publicadas anteriormente por el CEPD.

4. El objetivo de las presentes Directrices es llevar a cabo un análisis técnico sobre el ámbito de aplicación del artículo 5, apartado 3, de la Directiva ePrivacy, concretamente para aclarar qué abarca técnicamente la expresión «*con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario*». Las presentes Directrices no abordan las circunstancias en las que una operación de tratamiento puede acogerse a las exenciones del requisito de consentimiento previstas en la Directiva ePrivacy[4], ya que estas circunstancias deben analizarse caso por caso teniendo en cuenta la transposición o transposiciones pertinentes del Estado miembro y las orientaciones emitidas por las autoridades nacionales competentes.

5. En la parte final de las presentes Directrices se analizará una lista no exhaustiva de casos de uso específicos.

2 ANÁLISIS

2.1 Elementos clave para la aplicabilidad del artículo 5, apartado 3, de la Directiva ePrivacy

6. El artículo 5, apartado 3, de la Directiva ePrivacy es aplicable si:

   a. **CRITERIO A:** las operaciones realizadas se refieren a la «*información*». Cabe señalar que el término utilizado no es «datos personales», sino «información».

   b. **CRITERIO B:** las operaciones realizadas implican un «*equipo terminal*» de un abonado o usuario (B.1), lo que supone la necesidad de evaluar el concepto *de «red pública de comunicaciones*» (B.2).

   c. **CRITERIO C:** las operaciones efectuadas constituyen efectivamente un «*almacenamiento*» (C.1) o una «*obtención de acceso*» (C.2). Estos dos conceptos pueden estudiarse de forma independiente, como se recuerda en el Dictamen 9/2014 del GT29: *«El uso de la expresión "almacenamiento o acceso" indica que no es necesario que el almacenamiento y el acceso se produzcan dentro de la misma comunicación ni que sean realizados por la misma parte»*[5].

   En aras de la legibilidad, en lo sucesivo se hará referencia a la entidad que obtiene acceso a la información almacenada en el equipo terminal del usuario como «la entidad que accede».

[4] Tal como se establece en el artículo 5, apartado 3, de la Directiva ePrivacy: «*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.*»

[5] Dictamen 9/2014 del GT29, p. 8.

2.2 Concepto de «información»: criterio A

7. Tal como se expresa en el CRITERIO A, en esta sección se detalla lo que abarca el concepto de «información». La elección del término «información», que comprende una categoría más amplia que la mera noción de datos personales, está relacionada con el ámbito de aplicación de la Directiva ePrivacy.

8. El objetivo del artículo 5, apartado 3, de la Directiva ePrivacy es proteger la esfera privada de los usuarios, como se indica en su considerando 24: «*Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales*». También está protegida por el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea.

9. De hecho, las hipótesis que interfieren efectivamente con esta esfera privada, incluso sin implicar ningún dato personal, están explícitamente contempladas en la formulación del artículo 5, apartado 3, y el considerando 24 de la Directiva ePrivacy, por ejemplo, el almacenamiento de virus en el equipo terminal del usuario. Esto demuestra que la definición del término «información» no debe limitarse a la característica de estar relacionada con una persona física identificada o identificable.

10. Así lo ha confirmado el Tribunal de Justicia de la UE: «*Esta protección se aplica a toda información almacenada en dicho equipo, con independencia de si se trata de datos personales o no, y tiene como finalidad, en particular, según se desprende de ese mismo considerando, proteger a los usuarios contra el riesgo de que identificadores ocultos u otros dispositivos similares puedan introducirse en el equipo terminal del usuario sin su conocimiento.*»[6].

11. Ya se habían aclarado previamente las preguntas sobre si el origen de esta información y los motivos por los que se almacena en el equipo terminal deben tenerse en cuenta a la hora de evaluar la aplicabilidad del artículo 5, apartado 3, de la Directiva ePrivacy. Por ejemplo, en el Dictamen 9/2014 del GT29: «*No es correcto interpretarlo en el sentido de que el tercero no necesita el consentimiento para acceder a esta información simplemente porque no la ha almacenado. El requisito del consentimiento también se aplica cuando se accede a un valor de solo lectura (por ejemplo, cuando se solicita la dirección MAC de una interfaz de red a través de la API del sistema operativo)*»[7].

12. En conclusión, el concepto de información incluye los datos tanto no personales como personales, independientemente de cómo hayan sido almacenados y por quién, es decir, si fueron almacenados por una entidad externa (incluidas también otras entidades distintas de la que tiene acceso a los datos), por el usuario, por un fabricante o cualquier otra hipótesis.

2.3 Concepto de «equipo terminal de un abonado o usuario»: criterio B.1

13. Esta sección se basa en la definición utilizada en la Directiva 2008/63/CE y en la referencia a esta contenida en el artículo 2 de la Directiva (UE) 2018/1972, en la que «equipo terminal» se define como: «*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*

[6] Sentencia del Tribunal de Justicia de 1 de octubre de 2019, Planet 49, asunto C-673/17, ECLI:EU:C:2019:801, apartado 70.
[7] Dictamen 9/2014 del GT29, p. 8.

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;»[8].

14. El considerando 24 de la Directiva ePrivacy ofrece una descripción clara de la función de los equipos terminales para la protección brindada por el artículo 5, apartado 3, de la Directiva ePrivacy. La Directiva ePrivacy protege la privacidad de los usuarios no solo en relación con la confidencialidad de su información, sino también salvaguardando la integridad del equipo terminal del usuario. La interpretación del concepto de equipo terminal a lo largo de las presentes Directrices se guiará por este principio.

15. El artículo 3 de la Directiva ePrivacy establece que, para que dicha directiva sea aplicable, el tratamiento de datos personales debe llevarse a cabo en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en redes públicas de comunicaciones. Esto implica que un dispositivo debe ser utilizable en relación con dicho servicio y que, para ser calificado como equipo terminal, debe estar conectado o ser conectable[9] a la interfaz de una red pública de comunicaciones. El CEPD observa que las modificaciones introducidas en 2009[10] en el texto del artículo 5, apartado 3, de la Directiva ePrivacy ampliaron la protección de los equipos terminales suprimiendo la referencia al «uso de la red de comunicaciones electrónicas» como medio para almacenar información o acceder a la información almacenada en los equipos terminales. Por lo tanto, siempre que un dispositivo cuente con una interfaz de red que lo haga apto para la conexión (aunque dicha conexión no esté activada), el artículo 5, apartado 3, de la Directiva ePrivacy se aplicará a toda entidad que almacene información y obtenga acceso a información ya almacenada en el equipo terminal, independientemente del medio de acceso al equipo terminal y de si está conectado o desconectado de una red.

16. Los equipos que forman parte de la propia red pública de comunicaciones electrónicas no se considerarían equipos terminales con arreglo al artículo 5, apartado 3, de la Directiva ePrivacy[11].

17. Un equipo terminal puede estar compuesto por cualquier número de piezas individuales de *hardware*, que juntas constituyen el equipo terminal. Este puede o no adoptar la forma de un dispositivo físicamente cerrado que aloja todos los componentes de la pantalla, de tratamiento, de almacenamiento y del *hardware* periférico (por ejemplo, *smartphones*, ordenadores portátiles, dispositivos de almacenamiento conectados a la red, coches o televisores conectados, gafas inteligentes, etc.).

[8] Directiva 2008/63/CE de la Comisión, de 20 de junio de 2008, relativa a la competencia en los mercados de equipos terminales de telecomunicaciones (Versión codificada), artículo 1, apartado 1.

[9] Es decir, disponer de las capacidades técnicas necesarias para conectarse a la red, aun cuando dicha conexión no esté activada actualmente.

[10] Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n.º 2006/2004 sobre la cooperación entre autoridades nacionales responsables de la aplicación de las leyes en materia de protección de los consumidores (Texto pertinente a efectos del EEE), DO L 337, 18.12.2009, artículo 2, apartado 5, y considerando 65.

[11] Para conocer los límites de la red en diferentes contextos, consulte las Directrices del ORECE sobre enfoques comunes para la identificación del punto de terminación de la red en diferentes topologías de red [*BEREC Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies*, BoR (20) 46, documento disponible en inglés].

18. La Directiva ePrivacy reconoce que la protección de la confidencialidad de la información almacenada en el equipo terminal de un usuario y de la integridad del equipo terminal del usuario no se limita a la protección de la esfera privada de las personas físicas, sino que también se refiere al derecho al respeto de su correspondencia o a los intereses legítimos de las personas jurídicas[12]. Como tal, un equipo terminal que permita llevar a cabo esta correspondencia y defender los intereses legítimos de las personas jurídicas está protegido en virtud del artículo 5, apartado 3, de la Directiva ePrivacy.

19. El usuario o abonado puede tener en propiedad o alquilar, u obtener de alguna otra forma, el equipo terminal. Varios usuarios o abonados pueden compartir el mismo equipo terminal.

20. Esta protección está garantizada por la Directiva ePrivacy para el equipo terminal asociado al usuario o abonado, y no depende de si el usuario ha establecido los medios de acceso (por ejemplo, si ha iniciado la comunicación electrónica) o tan siquiera de si el usuario tiene conocimiento de dichos medios de acceso.

2.4 Concepto de «red pública de comunicaciones»: criterio B.2

21. Dado que la situación regulada por la Directiva ePrivacy se refiere a «*la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad*»[13], y dado que la definición de un equipo terminal menciona específicamente el concepto de «*red pública de comunicaciones*», es fundamental aclarar este concepto para determinar el contexto en el que se aplica el artículo 5, apartado 3, de la Directiva ePrivacy.

22. El concepto de red de comunicaciones electrónicas no se define en la propia Directiva. Este concepto fue mencionado inicialmente en la Directiva 2002/21/CE (Directiva marco), relativa a un marco regulador común para las redes y los servicios de comunicaciones electrónicas[14], sustituida posteriormente por el artículo 2, apartado 1, de la Directiva 2018/1972 (Código Europeo de las Comunicaciones Electrónicas). Actualmente establece lo siguiente:

> *«"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 cable, radio, 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»*[15].

23. Esta definición es neutra con respecto a las tecnologías de transmisión. 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.

---

[12] De hecho, como se recuerda en el artículo 2, apartado 13, de la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas, el usuario puede ser una persona física o jurídica.

[13] Artículo 3 de la Directiva ePrivacy.

[14] Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco).

[15] Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (versión refundida) (Texto pertinente a efectos del EEE).

24. El concepto de red de comunicaciones electrónicas en virtud de la Directiva (UE) 2018/1972 no depende del carácter público o privado de la infraestructura, ni de la manera en que se implante o gestione la red («*se basen o no en una infraestructura permanente o en una capacidad de administración centralizada*»[16]). Por tanto, la definición de red de comunicaciones electrónicas que figura en el artículo 2 de la Directiva (UE) 2018/1972 es lo suficientemente amplia como para abarcar cualquier tipo de infraestructura. 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 unirse dinámicamente a una malla de otros equipos terminales, o abandonarla, utilizando protocolos de transmisión de corto alcance.

25. Esta definición de red no establece ninguna limitación en cuanto al número de equipos terminales presentes en la red en cualquier momento. Algunos sistemas de creación de redes se basan en nodos que transmiten información de manera *ad hoc* a nodos conectados en ese momento[17], de manera que en algún momento podrían contar con tan solo dos nodos comunicados entre sí. Estos casos estarían dentro del ámbito general de aplicación de la Directiva ePrivacy, siempre que el protocolo de red permita la inclusión de otros nodos adicionales.

26. La disponibilidad pública de la red de comunicación es necesaria para que el producto se considere un equipo terminal y, por tanto, para la aplicabilidad del artículo 5, apartado 3, de la Directiva ePrivacy. Cabe señalar que el hecho de que la red se ponga a disposición de un subconjunto limitado del público (por ejemplo, abonados, sean o no de pago, sujetos a condiciones de admisibilidad) no hace que dicha red sea privada[18].

2.5 Concepto de «obtención de acceso»: criterio C.1

27. Para contextualizar correctamente el concepto de «obtención de acceso», es importante tener en cuenta el ámbito de aplicación de la Directiva ePrivacy, establecido en su artículo 1: «*garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la privacidad, 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*».

28. En pocas palabras, la Directiva ePrivacy es un instrumento jurídico de preservación de la privacidad cuyo objetivo es proteger la confidencialidad de las comunicaciones y la integridad de los dispositivos. En el considerando 24 de la Directiva ePrivacy se aclara que, en el caso de las personas físicas, el equipo terminal del usuario forma parte de la esfera privada de este, y que el acceso a la información almacenada en el equipo sin su conocimiento puede interferir gravemente en su privacidad.

[16] Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (versión refundida) (Texto pertinente a efectos del EEE).

[17] Por ejemplo, en el contexto de un sistema de red tolerante al retardo que aplica «técnicas de almacenamiento y reenvío», como el proyecto de código abierto Briar.

[18] Para un análisis más detallado sobre la identificación de las redes públicas de comunicaciones, véanse las Directrices del ORECE sobre la aplicación del Reglamento relativo al acceso a una internet abierta [*BEREC Guidelines on the Implementation of the Open Internet Regulation*, BoR (20) 112, documento disponible en inglés].

29. Las personas jurídicas también están protegidas por la Directiva ePrivacy[19]. En consecuencia, el concepto de «obtener acceso» a que se refiere el artículo 5, apartado 3, de la Directiva ePrivacy debe interpretarse de manera que se salvaguarden esos derechos frente a la violación por parte de terceros.

30. El almacenamiento de información o la obtención de acceso a información almacenada pueden ser operaciones independientes y realizadas por entidades independientes. El almacenamiento de información y el acceso a la información ya almacenada no tienen por qué darse para que se aplique el artículo 5, apartado 3, de la Directiva ePrivacy.

31. Como se señala en el Dictamen 9/2014 del GT29: «*El uso de la expresión "almacenamiento o acceso" indica que no es necesario que el almacenamiento y el acceso se produzcan dentro de la misma comunicación ni que sean realizados por la misma parte. Por lo tanto, la información almacenada por una parte (entre ella, la información almacenada por el usuario o el fabricante del dispositivo) a la que posteriormente acceda otra parte entra en el ámbito de aplicación del artículo 5, apartado 3*»[20]. Por consiguiente, no existen restricciones en cuanto al origen de la información presente en el equipo terminal para que se aplique el concepto de acceso.

32. Siempre que una entidad adopte medidas para obtener acceso a la información almacenada en el equipo terminal, se aplicará el artículo 5, apartado 3, de la Directiva ePrivacy. Normalmente, esto implica que la entidad que realice el acceso envíe de forma proactiva instrucciones específicas a los equipos terminales para recibir la información que se desea obtener. Este es el caso, por ejemplo, de las *cookies*, cuando la entidad que realiza el acceso da instrucciones al equipo terminal para que envíe información de forma proactiva con cada solicitud sucesiva del protocolo de transferencia de hipertexto (HTTP).

33. Lo mismo ocurre cuando la entidad que realiza el acceso distribuye *software* en el equipo terminal del usuario que se almacena y, a continuación, llamará de forma proactiva a la interfaz de programación de aplicaciones (API) a través de la red. Otros ejemplos serían el código JavaScript, en el que la entidad que realiza el acceso da instrucciones al navegador del usuario para que envíe solicitudes asíncronas con la información que se desea obtener. Dicho acceso entra claramente en el ámbito de aplicación del artículo 5, apartado 3, de la Directiva ePrivacy, ya que la entidad que realiza el acceso ordena explícitamente al equipo terminal que envíe la información.

34. En algunos casos, la entidad que ordena al equipo terminal que devuelva los datos que se desea obtener puede no coincidir con la entidad que recibe la información. Esto puede deberse a la provisión y/o el uso de un mecanismo común entre las dos entidades. Dar instrucciones al dispositivo para que envíe información ya almacenada (por ejemplo, usando un protocolo o un kit de desarrollo de software[21], lo que supone el envío proactivo de información por parte del equipo terminal) hace posible una intrusión en el equipo terminal, por lo que dicho acceso conlleva la aplicabilidad del artículo 5, apartado 3, de la Directiva ePrivacy. Como se señala en el Dictamen 09/2014 del GT29, este caso puede darse cuando un sitio web ordena al equipo terminal que envíe información a servicios de publicidad de terceros mediante la inclusión de un píxel de rastreo[22]. Este caso de uso se desarrolla con más detalle en la sección 3.1.

[19] Considerando 26 de la Directiva ePrivacy. Véase el apartado 17 anterior.
[20] Dictamen 9/2014 del GT29, p. 8.
[21] Un «kit de desarrollo de *software*» (*software development kit*, SDK) es un conjunto de herramientas de desarrollo de *software* puestas a disposición para facilitar la creación de programas informáticos de aplicaciones.
[22] Dictamen 9/2014 del GT29, p. 9.

2.6 Conceptos de «almacenamiento de información» y de «información almacenada»: criterio C.2

35. El almacenamiento de información en el sentido del artículo 5, apartado 3, de la Directiva ePrivacy se refiere a la colocación de información en un soporte de almacenamiento electrónico físico que forma parte del equipo terminal de un usuario o abonado[23].

36. Por lo general, la información no se almacena en el equipo terminal de un usuario o abonado mediante el acceso directo a la memoria del dispositivo por otra de las partes, sino transmitiendo instrucciones al *software* presente en el equipo terminal para que genere una información específica. El almacenamiento que se produzca mediante este tipo de instrucciones se considerará iniciado directamente por la otra parte. Esto incluye, entre otras cosas, hacer uso de protocolos establecidos, como el almacenamiento de *cookies* en el navegador, así como de *software* personalizado, independientemente de quién haya creado o instalado los protocolos o el *software* en el equipo terminal.

37. La Directiva ePrivacy no establece ningún límite máximo ni mínimo en cuanto al tiempo que la información debe mantenerse en un soporte de almacenamiento para que se contabilice como almacenada, ni tampoco existe un límite máximo ni mínimo en cuanto a la cantidad de información que debe almacenarse.

38. Del mismo modo, el concepto de almacenamiento no depende del tipo de soporte en el que se almacena la información. Algunos ejemplos típicos son las unidades de disco duro (*hard disk drive*, HDD), las unidades de estado sólido (*solid state drive*, SSD), la memoria solo de lectura, programable y borrable eléctricamente (*electrically-erasable programmable read-only memory*, EEPROM) y la memoria de acceso aleatorio (*random-access memory*, RAM), pero no se excluyen del ámbito de aplicación escenarios menos habituales que impliquen un soporte como una cinta magnética o una unidad central de procesamiento (*central processing unit*, CPU). El soporte de almacenamiento puede estar conectado internamente (por ejemplo, a través de una conexión SATA) o externamente (por ejemplo, a través de una conexión USB)

39. «Información almacenada» se refiere a la información ya existente en el equipo terminal, independientemente de la fuente de origen o de la naturaleza de esta información. Esto incluye, entre otras cosas, cualquier fruto del almacenamiento de información en el sentido del artículo 5, apartado 3, de la Directiva ePrivacy, tal como se ha descrito anteriormente (ya sea por la misma parte que obtendría acceso posteriormente o por un tercero). Además, incluye los resultados de los procesos de almacenamiento de información que escapan al ámbito de aplicación del artículo 5, apartado 3, de la Directiva ePrivacy, como por ejemplo: el almacenamiento en el equipo terminal por el propio usuario o abonado, o por un fabricante de *hardware* (como las direcciones MAC de los controladores de la interfaz de red), los sensores integrados en el equipo terminal o los procesos y programas ejecutados en los equipos terminales, que pueden o no producir información dependiente o derivada de la información almacenada.

3 CASOS DE USO

40. Como se ha señalado en la introducción de las presentes[24]Directrices, estas no analizan la aplicación de las exenciones a la obligación de recabar el consentimiento prevista en el artículo 5, apartado 3, de

[23] Tal como se define en la sección 2.3 de las presentes Directrices.
[24] Véase el apartado 4 anterior.

la Directiva ePrivacy. El CEPD recuerda que, en todos los casos en que se almacene información o se obtenga acceso a información ya almacenada, habría que evaluar si es necesario contar con el consentimiento o si podría aplicarse una exención en virtud del artículo 5, apartado 3, de la Directiva ePrivacy. Por lo tanto, el lector debe tener en cuenta las exenciones en su caso de uso, junto con este análisis técnico.

41. Sin perjuicio del contexto específico en el que pueden utilizarse esas categorías técnicas, que son necesarias para calificar si es aplicable el artículo 5, apartado 3, de la Directiva ePrivacy, es posible determinar, de manera no exhaustiva, categorías generales de identificadores e información que se utilizan ampliamente y que pueden estar sujetas a la aplicabilidad del artículo 5, apartado 3, de la Directiva ePrivacy.

42. La comunicación en red suele basarse en un modelo de distintos niveles que requiere el uso de identificadores para permitir el correcto establecimiento y realización de la comunicación. La comunicación de dichos identificadores a los agentes remotos es transmitida a través de un programa informático siguiendo protocolos de comunicación acordados. Como se ha señalado anteriormente, el hecho de que la entidad receptora pueda no ser la entidad que ordena el envío de información no excluye la aplicación del artículo 5, apartado 3, de la Directiva ePrivacy. Esto podría afectar a los identificadores de encaminamiento, como la dirección MAC o IP del equipo terminal, pero también a los identificadores de sesión (SSRC, identificador WebSocket) o a los *tokens* de autenticación.

43. Del mismo modo, el protocolo de aplicación puede incluir varios mecanismos para proporcionar datos contextuales (como los encabezados HTTP, entre ellos el campo «aceptar» o el agente de usuario), un mecanismo de almacenamiento en caché (como ETag[25]) u otras funcionalidades (entre ellas, las *cookies* o la política de seguridad HSTS[26]). Una vez más, el recurso a estos mecanismos para recopilar información (por ejemplo, en el contexto de la toma de impresiones dactilares[27] o el rastreo de identificadores de recursos) puede dar lugar a la aplicación del artículo 5, apartado 3, de la Directiva ePrivacy.

44. Por otro lado, existen algunos contextos en los que las aplicaciones locales instaladas en el equipo terminal utilizan determinada información estrictamente dentro del terminal, como podría ser el caso de las API del sistema de los *smartphones* (acceso a la cámara, micrófono, sensor GPS, chip acelerador, chip de radio, archivos locales, lista de contactos, identificadores, etc.). Este también podría ser el caso de 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 dicha información por una aplicación no constituiría «obtención de acceso a la información almacenada» en el sentido del artículo 5, apartado 3, de la Directiva ePrivacy, siempre que la información no salga del dispositivo; no obstante, cuando se acceda a esta información o a cualquier derivación de ella, se aplicaría el artículo 5, apartado 3, de la Directiva ePrivacy.

45. Por último, en algunos casos, hay agentes que distribuyen elementos de *software* malicioso, por ejemplo, programas informáticos de minería de criptoactivos o, de forma más general, programas maliciosos (*malware*), aprovechando las capacidades de procesamiento de los equipos terminales en

[25] El HTTP Etag es un identificador que permite realizar una solicitud condicional basada en la validez de los datos del cliente almacenados en la memoria caché.
[26] El HTTP con Seguridad de Transporte Estricta (*HTTP Strict Transport Security*, HSTS) permite a los servidores especificar qué recursos deben solicitarse siempre utilizando conexiones HTTPS.
[27] Como se señala en la introducción, véase el Dictamen 9/2014 del Grupo de Trabajo del Artículo 29 sobre la aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas (Directiva ePrivacy) a la toma de impresiones dactilares con dispositivos

beneficio del agente distribuidor. La distribución de dichos programas informáticos maliciosos en los equipos terminales del usuario constituiría un «almacenamiento» en el sentido del artículo 5, apartado 3, de la Directiva ePrivacy. Además, si el *software* estableciera una conexión de red para enviar información en una fase posterior, constituiría una «obtención de acceso» en el sentido del artículo 5, apartado 3, de la Directiva ePrivacy.

46. A continuación, se ofrece un análisis específico para un subconjunto de estas categorías que presentan un interés particular, ya sea por su uso generalizado o porque está justificado un estudio específico en relación con las circunstancias de su uso.

3.1 Las URL y el rastreo mediante píxeles

47. Un píxel de rastreo es un hipervínculo a un recurso, normalmente un archivo de imagen, incrustado en una pieza de contenido como un sitio web o un correo electrónico. Este píxel no suele tener ningún propósito finalidad relacionado con el contenido solicitado en sí, sino que su única finalidad es establecer automáticamente una comunicación por parte del cliente con el anfitrión del píxel, que de lo contrario no se habría producido. Sin embargo, esta situación no se da de forma sistemática y los píxeles de rastreo también pueden crearse añadiendo información adicional a las imágenes de carga de hipervínculos que sean pertinentes para el contenido mostrado al usuario. El establecimiento de la comunicación transmite diversa información al host del píxel, dependiendo del caso de uso específico.

48. En el caso de un correo electrónico, el remitente puede incluir un píxel de rastreo para detectar cuándo el receptor lee el correo electrónico. Los píxeles de rastreo de los sitios web pueden enlazar con una entidad que recopile muchas de estas solicitudes y, de este modo, son capaces de rastrear el comportamiento de los usuarios. Estos píxeles de rastreo también pueden contener identificadores, metadatos o contenidos adicionales como parte del enlace. Estos punteros de datos pueden ser añadidos por el propietario del sitio web, posiblemente relacionándolos con la actividad del usuario en dicho sitio web, de modo que puedan generarse informes analíticos de uso. También pueden generarse de forma dinámica mediante una lógica de aplicación del lado del cliente proporcionada por la entidad.

49. Los enlaces de rastreo pueden funcionar de la misma manera, pero el identificador se añade a la dirección del sitio web. Cuando el usuario visita la URL (*uniform resource locator*, localizador uniforme de recursos), el sitio web en cuestión carga el recurso solicitado, pero también recoge un identificador que no es pertinente en términos de identificación de recursos. Los sitios web de comercio electrónico utilizan estos identificadores con mucha frecuencia para determinar el origen de su fuente de tráfico entrante. Por ejemplo, este tipo de sitios web puede proporcionar enlaces con función de rastreo a socios para que los utilicen en su dominio, de modo que el sitio web de comercio electrónico sepa cuál de sus socios es responsable de una determinada venta y pueda pagarle una comisión, una práctica conocida como *marketing* de afiliados.

50. Tanto los enlaces de rastreo como los píxeles de rastreo pueden distribuirse a través de una gran variedad de canales, por ejemplo, a través de correos electrónicos, sitios web o incluso, en el caso de los enlaces de rastreo, a través de cualquier tipo de sistema de mensajería de texto. Esta distribución a los equipos terminales del usuario constituye efectivamente un almacenamiento, al menos a través del mecanismo de memoria caché del *software* del cliente. Como tal, el artículo 5, apartado 3, de la Directiva ePrivacy es aplicable aunque este almacenamiento no sea permanente.

51. La adición de información de rastreo a las URL o imágenes (píxeles) enviadas al usuario constituye una instrucción al equipo terminal para que responda enviando la información que se desea obtener (el identificador especificado). En el caso de los píxeles de rastreo construidos de forma dinámica, es la

distribución de la lógica de aplicación (normalmente, un código JavaScript) la que imparte la instrucción. Por tanto, puede considerarse que la recopilación de identificadores facilitada mediante tales mecanismos de rastreo constituye una «obtención de acceso» en el sentido del artículo 5, apartado 3, de la Directiva ePrivacy, por lo que también se aplica a esa etapa.

3.2 El tratamiento local

52. Algunas tecnologías se basan en el tratamiento local instruido mediante *software* distribuido en los equipos terminales de los usuarios, donde la información producida por el procesamiento local se pone posteriormente a disposición de agentes seleccionados a través de API del lado del cliente. Este puede ser el caso, por ejemplo, de una API proporcionada por el navegador web, que permite acceder de forma remota a los resultados generados localmente.

53. Si en algún punto —por ejemplo, en el código del lado del cliente— la información procesada se pone a disposición de un tercero, por ejemplo, enviándola a través de la red a un servidor, tal operación (cuyas instrucciones ha transmitido la entidad que produce el código del lado del cliente distribuido en el equipo terminal del usuario) constituiría una «obtención de acceso a información almacenada». El hecho de que esta información se produzca a nivel local no excluye la aplicación del artículo 5, apartado 3, de la Directiva ePrivacy.

3.3 El rastreo basado únicamente en la dirección IP

54. Algunos proveedores están desarrollando soluciones basadas únicamente en la recopilación de un componente, a saber, la dirección IP, para rastrear la navegación[28] del usuario, en algunos casos a través de múltiples dominios. En este contexto, el artículo 5, apartado 3, de la Directiva ePrivacy podría aplicarse, aunque la instrucción de facilitar la dirección IP haya sido emitida por una entidad distinta de la receptora.

55. Sin embargo, obtener acceso a las direcciones IP solo activaría la aplicación del artículo 5, apartado 3, de la Directiva ePrivacy en los casos en que esta información proceda del equipo terminal de un abonado o usuario. Aunque esto no se da de forma sistemática (por ejemplo, cuando se activa la técnica CGNAT[29]), la IPv4 estática saliente procedente del rúter del usuario se ajustaría a ese caso, así como las direcciones IPV6, ya que están parcialmente definidas por el anfitrión. A menos que la entidad pueda garantizar que la dirección IP no procede del equipo terminal de un usuario o abonado, deberá adoptar todas las medidas previstas en el artículo 5, apartado 3, de la Directiva ePrivacy.

56. Aunque las presentes directrices no analizan la aplicación de las excepciones a la obligación de recabar el consentimiento previstas en el artículo 5, apartado 3, de la Directiva ePrivacy, es importante recordar una vez más que la aplicabilidad de este artículo no significa sistemáticamente que sea necesario recabar el consentimiento. Así pues, el CEPD recuerda que en cada caso habría que evaluar si es necesaria una autorización o si pudiera aplicarse una exención en virtud del artículo 5, apartado 3, de la Directiva ePrivacy[30].

[28] Esto es complementario e independiente del uso y la función de una dirección IP para el establecimiento y la transmisión de las comunicaciones técnicas subyacentes, o del hecho de que puede tratarse o no de datos personales (en lo que respecta al análisis de la privacidad y las comunicaciones electrónicas, se trata de «información»).

[29] Los proveedores de servicios de internet utilizan la técnica Carrier-Grade NAT (CGNAT) para maximizar el uso de un espacio limitado de las direcciones IP. Agrupa a varios abonados bajo una misma dirección IP pública.

[30] El Dictamen 9/2014 del GT29 establece algunos ejemplos en los que podría no necesitarse el consentimiento.

3.4 Información intermitente y mediada sobre el Internet de las Cosas (IdC)

57. Los dispositivos del IdC producen información de forma continua a lo largo del tiempo, por ejemplo, a través de sensores integrados en el dispositivo, que pueden ser o no preprocesados localmente. En muchos casos, la información se pone a disposición de un servidor remoto, pero las modalidades de dicha recopilación pueden variar.

58. Algunos dispositivos del IdC poseen una conexión directa a una red pública de comunicaciones con una tarjeta SIM para móvil. Otros pueden tener una conexión indirecta a una red pública de comunicaciones, por ejemplo, mediante el uso de una red wifi o la retransmisión de información a otro dispositivo a través de una conexión de extremo a extremo (por ejemplo, a través de Bluetooth). El otro dispositivo puede ser, por ejemplo, un *smartphone* o una pasarela específica que puede o no preprocesar la información antes de enviarla al servidor.

59. Los dispositivos del IdC pueden recibir instrucciones del fabricante de transmitir siempre la información recogida y, sin embargo, seguir guardando primero la información en la memoria caché local, por ejemplo, hasta que se disponga de conexión.

60. En cualquier caso, cuando esté conectado (directa o indirectamente) a una red pública de comunicaciones, el dispositivo del IdC se consideraría en sí mismo un equipo terminal. El hecho de que la información se transmita o se almacene en la memoria caché para la elaboración de informes intermitentes no cambia la naturaleza de esa información. En ambas situaciones, se aplicaría el artículo 5, apartado 3, de la Directiva ePrivacy, ya que existe, a través de la instrucción de código en el dispositivo del IdC para enviar los datos almacenados dinámicamente al servidor remoto, una «obtención de acceso».

3.5 Los identificadores únicos

61. Una herramienta común utilizada por las empresas es el concepto de «identificadores únicos» o «identificadores persistentes». Dichos identificadores pueden derivarse de datos personales persistentes (nombre y apellidos, correo electrónico, número de teléfono, etc.), a los que se les aplica la función hash en el dispositivo del usuario, se recopilan y se comparten entre varios controladores para identificar de forma univoca 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 suscripción en línea o sin conexión, etc.). En los sitios web, los datos personales persistentes se obtienen generalmente en el contexto de la autenticación o la suscripción a boletines informativos.

62. Como se ha señalado anteriormente, el hecho de que la información sea introducida por el usuario no excluiría la aplicación del artículo 5, apartado 3, de la Directiva ePrivacy en lo que respecta al almacenamiento, ya que esta información se almacena temporalmente en el equipo terminal antes de su recopilación.

63. En el contexto de la recopilación de un «identificador único» en sitios web o aplicaciones para dispositivos móviles, la entidad que recopila la información da instrucciones al navegador (mediante la distribución del código del lado del cliente) para que envíe dicha información. Como tal, esta circunstancia supone una «obtención de acceso», por lo que se aplica el artículo 5, apartado 3, de la Directiva ePrivacy.