



17/ES

WP 247

**Dictamen 01/2017 sobre
la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas
(2002/58/CE)**

Adoptado el 4 de abril de 2017

El Grupo de Trabajo se creó de conformidad con el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos y privacidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

De su secretaría se ocupa la Dirección C (Derechos Fundamentales y Estado de Derecho) de la Dirección General de Justicia y Consumidores de la Comisión Europea, B-1049, Bruselas, Bélgica, Oficina n.º MO-59 05/035

Sitio web: http://ec.europa.eu/justice/data-protection/index_en.htm

EL GRUPO DE TRABAJO SOBREPROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

Vistos los artículos 29 y 30 de dicha Directiva,

Visto su Reglamento interno,

HA ADOPTADO EL PRESENTE DICTAMEN:

SINOPSIS

El Grupo de Trabajo acoge con satisfacción la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas de la Comisión Europea de 10 de enero de 2017, y celebra que se haya **optado por un reglamento** como instrumento normativo. De esta forma se garantiza que las normas son uniformes en toda la UE y se ofrece claridad a las autoridades de control y a las organizaciones por igual. Asimismo, se contribuye a asegurar la coherencia con el Reglamento general de protección de datos (en adelante «RGPD»). Dicha coherencia está respaldada asimismo por la decisión de que **la misma autoridad encargada de velar por el cumplimiento del RGPD** sea responsable del cumplimiento de las normas sobre privacidad y comunicaciones electrónicas.

Al mismo tiempo, la elección (mantenimiento) de un **instrumento jurídico complementario** es positiva. La protección de la comunicación confidencial y los equipos terminales presenta una serie de características particulares que no aborda el RGPD. Por consiguiente, son necesarias disposiciones complementarias en relación con estos tipos de servicio, a fin de garantizar una protección adecuada del derecho fundamental a la privacidad y la confidencialidad de las comunicaciones, incluida la confidencialidad de los equipos terminales. A este respecto, el Grupo de Trabajo apoya firmemente el **enfoque basado en principios** por el que se ha optado en la propuesta de Reglamento de **prohibiciones generales y excepciones concretas**, así como la **aplicación específica del concepto de «consentimiento»**.

El Grupo de Trabajo acoge favorablemente la ampliación del ámbito de aplicación de la propuesta de Reglamento a fin de **incluir a los proveedores de servicios de transmisión libre** (denominados en inglés, «Over-The-Top» y conocidos por sus siglas «OTT»), servicios funcionalmente equivalentes a los medios de comunicación más tradicionales y, por tanto, igualmente susceptibles de repercutir en la privacidad y el derecho al secreto de las comunicaciones de los ciudadanos de la UE. Resulta positivo asimismo que la propuesta de Reglamento abarque claramente **el contenido y los metadatos correspondientes** y reconozca que los **metadatos pueden revelar datos muy sensibles**.

No obstante, el Grupo de Trabajo señala también cuatro aspectos que suscitan **grave preocupación**. Por lo que respecta al **seguimiento de la localización de los equipos terminales; las condiciones en las que se permite el análisis del contenido y los metadatos; los ajustes por defecto de los equipos terminales y programas informáticos y por lo que respecta a los muros de seguimiento**, la propuesta de Reglamento reduciría el nivel de protección que garantiza el RGPD. En el presente Dictamen, el Grupo de Trabajo formula sugerencias específicas para velar por que el Reglamento sobre la privacidad y las comunicaciones electrónicas garantice el mismo nivel de protección, o un nivel superior que se adecúe al carácter sensible de los datos de comunicaciones (tanto por lo que respecta al contenido como a los metadatos).

En lo que atañe al **seguimiento por wifi**, en función de las circunstancias y los fines de la recogida de datos, con arreglo al RGPD dicho seguimiento es susceptible de estar sujeto a consentimiento o de que solo pueda llevarse a cabo si los datos personales recogidos se anonimizan. En este último caso, han de cumplirse las cuatro condiciones siguientes: la finalidad de la recogida de datos de equipos terminales se limita 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 eliminarán o anonimizarán inmediatamente después y existen posibilidades efectivas de exclusión voluntaria. Se invita a la Comisión Europea a promover una norma técnica para que los dispositivos móviles notifiquen automáticamente una objeción a dicho seguimiento.

En relación con el **análisis del contenido y los metadatos**, el punto de partida debería ser la prohibición de tratar los datos de comunicaciones sin el consentimiento de todos los usuarios finales (emisores y destinatarios). Para permitir que los proveedores presten servicios solicitados expresamente por el usuario, como por ejemplo la funcionalidad de búsqueda e indexación, o servicios de conversión de texto a voz, debería contemplarse una excepción doméstica para el tratamiento de contenido y metadatos para el uso puramente personal del propio usuario.

Por lo que respecta al **consentimiento del seguimiento**, el Grupo de Trabajo pide que se prohíban expresamente los muros de seguimiento, esto es, opciones «lo tomas o lo dejas» que fuerzan a los usuarios a dar su consentimiento al seguimiento si desean acceder al servicio.

Por último, el Grupo de Trabajo recomienda que los equipos terminales y los programas informáticos deban **ofrecer por defecto ajustes de protección de la privacidad**, y ofrecer opciones claras a los usuarios para confirmar o modificar estos ajustes por defecto durante la instalación. Los ajustes deben ser de fácil acceso durante la utilización. Los usuarios deben poder indicar el consentimiento específico a través de los ajustes de su navegador. Las preferencias de privacidad no deben limitarse a la interferencia por terceros ni a las *cookies*. El Grupo de Trabajo recomienda encarecidamente hacer obligatorio el cumplimiento de la norma «no realizar seguimiento» («Do Not Track»).

El Grupo de Trabajo ha identificado asimismo otros puntos de interés relacionados, por ejemplo, con el alcance, la protección de los equipos terminales y la mercadotecnia directa. Por último, el Grupo de Trabajo ha identificado cuestiones que merecen una aclaración, a fin de proteger mejor a los usuarios finales y para introducir mayor seguridad jurídica para todas las partes interesadas afectadas.

ÍNDICE

1. INTRODUCCIÓN.....	6
2. ASPECTOS POSITIVOS DE LA PROPUESTA DE REGLAMENTO	6
<i>Armonización a escala de la UE, aproximación de las multas y aplicación exclusiva por parte de las autoridades de protección de datos</i>	<i>6</i>
<i>Ampliación del ámbito de aplicación en comparación con la Directiva sobre la privacidad y las comunicaciones electrónicas</i>	<i>8</i>
<i>Aplicación específica del concepto de consentimiento</i>	<i>11</i>
3. PUNTOS QUE PLANTEAN GRAVES PREOCUPACIONES.....	11
<i>La protección otorgada por el RGPD se ve mermada por la propuesta de Reglamento</i>	<i>11</i>
4. OTROS ASPECTOS QUE PLANTEAN PREOCUPACIONES	19
<i>Es preciso ampliar el alcance territorial y material.....</i>	<i>19</i>
<i>Debe reforzarse la protección de los equipos terminales.....</i>	<i>20</i>
<i>Mercadotecnia directa.....</i>	<i>24</i>
<i>Calendario</i>	<i>27</i>
<i>Otras preocupaciones.....</i>	<i>27</i>
5. SUGERENCIAS DE ACLARACIÓN PARA GARANTIZAR LA SEGURIDAD JURÍDICA	31
<i>Aclaraciones sobre el ámbito de aplicación.....</i>	<i>31</i>
<i>Aclaraciones en cuanto al concepto y la aplicación del consentimiento.....</i>	<i>34</i>
<i>Aclaraciones en cuanto a la localización y otros metadatos.....</i>	<i>35</i>
<i>Aclaraciones con respecto a las comunicaciones no solicitadas.....</i>	<i>37</i>
<i>Aclaraciones con respecto a la aplicación de instrumentos en materia de derechos fundamentales</i>	<i>38</i>
<i>Otras aclaraciones.....</i>	<i>39</i>

1. INTRODUCCIÓN

1. El Grupo de Trabajo sobre protección de datos del artículo 29 (en adelante, «el Grupo de Trabajo» o «GT29») acoge con satisfacción la propuesta de la Comisión Europea relativa al Reglamento sobre la privacidad y las comunicaciones electrónicas (en adelante, «la propuesta de Reglamento») ¹, concebido para sustituir a la Directiva sobre la privacidad y las comunicaciones electrónicas².
2. Numerosos aspectos de la propuesta de Reglamento son positivos, y la Comisión Europea ha dado un paso importante con su introducción. No obstante, la propuesta objeto de examen es susceptible de ser mejorada. Con ello no solo se protegería mejor a los usuarios finales, sino que también se introduciría mayor seguridad jurídica para todas las partes interesadas afectadas.
3. Así, el Grupo de Trabajo ha identificado varios puntos de interés y plantea recomendaciones de aclaraciones que habrán de abordar el Parlamento Europeo y el Consejo de Ministros en su debate sobre la propuesta de Reglamento. En primer lugar, el presente Dictamen examinará los aspectos positivos de la propuesta de Reglamento para resaltar, a continuación, las cuestiones que suscitan preocupación y los aspectos que requieren aclaraciones.

2. ASPECTOS POSITIVOS DE LA PROPUESTA DE REGLAMENTO

ARMONIZACIÓN A ESCALA DE LA UE, APROXIMACIÓN DE LAS MULTAS Y APLICACIÓN EXCLUSIVA POR PARTE DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

4. El Grupo de Trabajo celebra que se haya **optado por un reglamento como instrumento normativo**. Ello garantiza que las normas sean uniformes en toda la UE (con ciertas excepciones que se tratarán más adelante) y ofrece claridad tanto a las autoridades de control como a las organizaciones; además, dado el papel fundamental que desempeña el RGPD³ en la propuesta de Reglamento, esto contribuye a garantizar la coherencia entre ambos instrumentos. Al mismo tiempo, **la elección (mantenimiento) de un instrumento jurídico complementario** es positiva. La

¹ Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), 2017/0003 (COD), url: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=ES>.

² 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 intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, pp. 37-47), url: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32002L0058>.

³ 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 (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, p. 1-88), url: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>.

protección de la comunicación confidencial y los equipos terminales presenta una serie de características particulares que el RGPD no aborda. Por consiguiente, son necesarias disposiciones complementarias en relación con este tipo de servicios, a fin de garantizar una protección adecuada de este derecho fundamental. En este contexto, el Grupo de Trabajo también **apoya el enfoque basado en principios por el que se ha optado en la propuesta de Reglamento de prohibiciones generales y excepciones concretas**, y considera que debe evitarse la introducción de excepciones abiertas como las previstas en el artículo 6 del RGPD, y en particular en su letra f) (satisfacción de intereses legítimos).

5. **El control del cumplimiento de estas normas por parte de la misma autoridad responsable de velar por el cumplimiento del RGPD** respaldará aún más la coherencia entre ambos instrumentos. Dado al vínculo entre la protección de los datos de carácter personal y la protección de la comunicación confidencial y los equipos terminales, resulta de utilidad que el control del cumplimiento de las disposiciones recogidas en la propuesta de Reglamento se confíe a la misma autoridad de control encargada de velar por la aplicación del RGPD (considerando 38 y artículo 18 de la propuesta de Reglamento). Por otro lado, la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE)⁴ confirma que resulta fundamental que la autoridad de control sea independiente, tal como prescribe el artículo 7 de la Carta. No obstante, desde el punto de vista práctico, esto significaría una cantidad considerable de trabajo adicional para las autoridades de protección de datos, sin garantía de que puedan cumplir su cometido si no se obtiene un incremento presupuestario. Por tanto, las autoridades de protección de datos acogen con agrado el considerando 38 de la propuesta de Reglamento, que pone de relieve que todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras adicionales necesarios para el ejercicio efectivo de las tareas que les impone el nuevo Reglamento. Les complace asimismo que el artículo 18, apartado 2, establezca la base jurídica para la cooperación entre las autoridades de control de la propuesta de Reglamento y las autoridades nacionales de reglamentación de la propuesta de Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas («CECE»)⁵.
6. Dada la estrecha relación entre la propuesta de Reglamento y el RGPD, también debemos acoger con satisfacción **la armonización de las multas contempladas en uno y otro**. Las actividades comprendidas en el ámbito de aplicación de la propuesta de Reglamento tienen un carácter bastante delicado e implican, entre otras cosas, la interferencia en las comunicaciones confidenciales y los equipos terminales. El nivel de las multas debe ser proporcional al carácter sensible del contexto. Este contexto es asimismo el motivo por el que la armonización en toda la UE es importante, a fin de conceder el mismo nivel de protección en todo su territorio. El artículo 23 de la

⁴ Véase, por ejemplo, TJUE 6 de octubre de 2015, C-362/14 (Safe Harbour), apartado 41 y TJUE 21 de diciembre de 2016, C-203/15 y C-698/15 (Tele2/Watson), apartado 123.

⁵ Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece el Código Europeo de las Comunicaciones Electrónicas (Refundición), 2016/0288 (COD), 12.10.2016, url: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=comnat:COM_2016_0590_FIN.

propuesta de Reglamento contempla multas efectivas por infringir el Reglamento, de nivel similar al de las multas fijadas por violación de las normas del RGPD, salvo en algunos puntos (véase la observación 38).

7. Asimismo, resulta positiva la **eliminación de las normas específicas sobre la notificación de una violación de la seguridad de los datos** de este instrumento jurídico, a fin de evitar solapamientos innecesarios con los requisitos en materia de violación de la seguridad de los datos del RGPD.
8. También es de **agradecer que la atención se centre ahora en conceder el mismo nivel de protección a todos los usuarios finales**, ya que la propuesta de Reglamento ha prescindido del concepto de diferenciación entre «abonados» y otros usuarios de servicios de comunicaciones electrónicas.

AMPLIACIÓN DEL ÁMBITO DE APLICACIÓN EN COMPARACIÓN CON LA DIRECTIVA SOBRE LA PRIVACIDAD Y LAS COMUNICACIONES ELECTRÓNICAS

9. El Grupo de Trabajo acoge con satisfacción la **ampliación del ámbito de aplicación de la propuesta de Reglamento a fin de incluir a los proveedores de servicios de transmisión libre (OTT«)**, servicios funcionalmente equivalentes a los medios de comunicación más tradicionales y, por tanto, igualmente susceptibles de repercutir en la privacidad y el derecho al secreto de las comunicaciones de los ciudadanos de la UE. El Grupo de Trabajo se muestra especialmente satisfecho de que todas las categorías de OTT (OTT0, OTT1 y algunos OTT2)⁶ ahora estén incluidas en el ámbito de aplicación del Reglamento, ya que no solo abarca los medios de comunicación tradicionales (OTT0), sino también los servicios funcionalmente equivalentes (OTT1), tal como se menciona en el artículo 8, apartado 1, letra c), de la propuesta de Reglamento. También es positivo que, además de las definiciones contempladas en el CECE, algunos OTT2 se incluyan cuando proporcionen comunicación interpersonal e interactiva secundaria que vaya intrínsecamente unida a su servicio, como en el caso de juegos, aplicaciones de citas o sitios de reseñas (artículo 4, apartado 2, de la propuesta de Reglamento). De igual forma, también es bien recibida la **aclaración de que la protección también se extiende a la interacción de máquina a máquina**. El considerando 12 deja claro que los dispositivos que se comunican entre sí están dentro del alcance de la protección otorgada por la propuesta de Reglamento. Este hecho es conveniente, ya que frecuentemente este tipo de comunicaciones contiene información protegida por derechos de privacidad. No obstante, la aplicabilidad podría ser objeto de aclaración [véase la observación 40, letra h)].

⁶ Véase una explicación más detallada de estos términos en ORECE, *Report on OTT Services*, BoR (16) 35, 29 de enero de 2016, pp. 15 y 16, url: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services. Nótese asimismo la observación que figura en el informe de que las categorías están pensadas como conceptos a utilizar en el debate sobre la revisión y no como conceptos jurídicos.

10. Asimismo, es positivo que **la propuesta de Reglamento abarque claramente el contenido y los metadatos correspondientes**. El considerando 14 deja claro que la definición de «datos de comunicaciones electrónicas» contemplada en el artículo 4, apartado 3, letra a), está pensada para ser lo suficientemente amplia como para incluir *todo* el contenido así como los metadatos correspondientes, independientemente, por ejemplo, de los medios de transporte de las señales. No obstante, el Grupo de Trabajo señala como aspecto preocupante en la observación 39 que esta definición actual de «datos de comunicaciones electrónicas» aún es objeto de debate. En consonancia con esta ampliación del ámbito de aplicación, el Grupo de Trabajo considera **el reconocimiento de que los metadatos pueden revelar datos muy sensibles** (véase el apartado 2.2 de la exposición de motivos; considerando 2) una adición fundamental. El Grupo de Trabajo acoge con agrado el hecho de que la Comisión Europea, de esta forma, incorpore las consideraciones del TJUE en los asuntos Digital Rights Ireland y Tele2/Watson. Asimismo, valora que se **reconozca que el análisis de contenido es un tratamiento de alto riesgo**. El considerando 19 y el artículo 6, apartado 3, letra b), establecen la presunción legal lógica de que el análisis de contenido es un tratamiento de alto riesgo con arreglo al artículo 35 del RGPD y, aparentemente con independencia de la existencia de un alto riesgo residual, siempre requiere consultar previamente a la autoridad (principal) de protección de datos. Al mismo tiempo, al Grupo de Trabajo le preocupa el alcance de la definición de «metadatos» y el hecho de que el análisis de metadatos no esté sujeto al mismo requisito obligatorio de evaluación de impacto relativa a la protección de datos (véanse las observaciones 33 y 46).
11. También cabe celebrar **el reconocimiento continuado de la importancia de la anonimización**. En la Directiva sobre la privacidad y las comunicaciones electrónicas, las medidas de anonimización ya desempeñaban un papel a la hora de garantizar la compatibilidad (por ejemplo, el artículo 6, apartado 1, de dicha Directiva, que dispone que los datos de tráfico deben eliminarse o hacerse anónimos cuando ya no sean necesarios a los efectos de la transmisión de una comunicación). En el artículo 6, apartado 2, letra c), y apartado 3, letra b), de la propuesta de Reglamento, se permite una excepción a la prohibición de tratamiento de los metadatos y el contenido sobre la base del consentimiento, siempre que el fin o los fines específicos «no puedan alcanzarse mediante el tratamiento de información anonimizada». Requerir tales medidas de protección de la privacidad además de solicitar el consentimiento de los usuarios los protege de un tratamiento injustificado. No obstante, el Grupo de Trabajo se muestra al mismo tiempo profundamente preocupado de que la adopción de tales técnicas de anonimización no se requiera cuando se realice un seguimiento de la localización de los usuarios a través de sus equipos móviles (véase la observación 17). Por otro lado, incluso cuando han de aplicarse medidas de anonimización, los proveedores siempre deberían llevar a cabo una evaluación de impacto relativa a la protección de datos (en adelante «EIPD»)(véanse las observaciones 33 y 46), y el Grupo de Trabajo pide que se introduzca la obligación adicional de hacer pública la forma en que los datos se anonimizan y agregan [véase la observación 42, letra b)].
12. Otro aspecto positivo es la **formulación genérica de la protección de los equipos terminales**. El considerando 20 y el artículo 8 establecen que las tecnologías

utilizadas para acceder a los equipos terminales no son relevantes: toda interferencia en los equipos terminales, incluida la utilización de sus capacidades de tratamiento, requiere el consentimiento del usuario final (con determinadas excepciones). La Comisión Europea ahora ha confirmado convenientemente que la «huella digital de dispositivo» está comprendida en esta disposición. Por otro lado, el Grupo de Trabajo celebra que la negativa de un tercero a respetar las preferencias expresadas en la **configuración del navegador de un usuario sea oponible**, tal como se describe en el considerando 22. Este aspecto resulta útil en aquellas situaciones en que un tercero (p. ej., una red publicitaria) no respete tal configuración. No obstante, debería contemplarse también en una disposición pertinente de la propuesta de Reglamento.

13. Por último, resulta positivo la **inclusión permanente de las personas jurídicas en el ámbito de aplicación de la propuesta de Reglamento** [véase el apartado 2.2 de la exposición de motivos; considerandos 3, 33 y 42; artículos 1 y 15 y artículo 16, apartado 5]. Esta situación ya se contempla en la Directiva sobre la privacidad y las comunicaciones electrónicas, pero ya que las autoridades de protección de datos tendrán el cometido de hacer respetar las nuevas normas, resulta de utilidad subrayarlo específicamente. Esto permite que las autoridades de protección de datos puedan emprender acciones cuando las personas jurídicas sean víctimas de una infracción, por ejemplo cuando las empresas reciben correo basura o sus comunicaciones son monitorizadas de forma subrepticia. No obstante, el Grupo de Trabajo también señala como aspectos preocupantes el hecho de que la aplicación del consentimiento a las personas jurídicas no queda claro [véase la observación 41, letra a)] y que resulta confuso qué se entiende por «interés legítimo» de las personas jurídicas en el caso de la mercadotecnia directa [véase la observación 43, letra c)].

14. El Grupo de Trabajo acoge con satisfacción otra categoría de mejoras en relación con la aplicación e interpretación del concepto de consentimiento. En primer lugar, se agradece **la aclaración de que el acceso a internet y la telefonía (móvil) son servicios esenciales y los proveedores de estos servicios no pueden «forzar» a sus clientes a dar su consentimiento a cualquier tratamiento de datos que no sea necesario para la prestación del servicio esencial en sí.** Concretamente, en el considerando 18 se señala que los servicios de acceso a la internet de banda ancha básica y de comunicaciones de voz han de considerarse servicios esenciales, lo que implica, habida cuenta de la dependencia de las personas del acceso a estos servicios, que el consentimiento para el tratamiento de sus datos de comunicaciones con tales fines adicionales (p. ej., tratamiento con fines publicitarios o de mercadotecnia) no puede ser válido. Al mismo tiempo, al Grupo de Trabajo le preocupa que esta aclaración sea demasiado limitada. Los servicios de determinados proveedores OTT también pueden considerarse servicios esenciales, por lo que el Reglamento sobre la privacidad y las comunicaciones electrónicas también debería prohibir expresamente las opciones de «todo o nada» en otras circunstancias (véase la observación 20).
15. Por otro lado, resulta positivo **que se armonice el requisito de obtener el consentimiento para la inclusión de datos personales de personas físicas en guías.** Con arreglo al artículo 15 de la propuesta de Reglamento, el tratamiento de datos en guías accesibles al público solo se permite con el consentimiento de las personas físicas y la posibilidad de oponerse en el caso de las personas jurídicas. Esto se desarrolla con más detalle en el considerando 31, que señala que este consentimiento debe ser específico con respecto a las categorías específicas de datos personales que se vayan a incluir en la guía. No obstante, el Grupo de Trabajo señala como motivo de preocupación que la propuesta de Reglamento podría ser más clara en relación con que se requerirá consentimiento independiente específico para la búsqueda y la búsqueda inversa (véase la observación 37).
16. También es bienvenida **la nueva excepción específica para la interferencia no intrusiva en equipos terminales.** El Grupo de Trabajo considera de utilidad que la propuesta de Reglamento aclare que la prohibición no se aplica a la medición del tráfico en un sitio web [conforme a la excepción específica de que tal medición la lleve a cabo el proveedor del servicio de la sociedad de la información solicitado por el usuario final; véase el artículo 8, apartado 1, letra d), de la propuesta de Reglamento]. Véase asimismo el considerando 21. No obstante, el Grupo de Trabajo sugiere que se utilice una definición más neutra desde el punto de vista tecnológico y que se aclare la aplicabilidad de esta excepción (véase la observación 25).

3. PUNTOS QUE PLANTEAN GRAVES PREOCUPACIONES

LA PROTECCIÓN OTORGADA POR EL RGPD SE VE MERMADA POR LA PROPUESTA DE REGLAMENTO

Como ya se ha mencionado anteriormente, la propuesta de Reglamento presenta una serie de mejoras clave. Con todo, también presenta varios puntos que plantean preocupaciones

de distinta gravedad. En la presente sección, el Grupo de Trabajo trata las cuatro cuestiones que **más le preocupan**. Se trata de disposiciones que **merman el nivel de protección otorgado por el RGPD**.

17. Las obligaciones contenidas en el Reglamento de cara al seguimiento de la localización de los equipos terminales deberían respetar los requisitos del RGPD.

El artículo 8, apartado 2, letra b), de la propuesta de Reglamento simplemente requiere que se muestre una advertencia y la aplicación de medidas de seguridad para la recopilación de la información emitida por los equipos terminales. Dicha disposición señala asimismo que la persona responsable de dicha recopilación debe indicar las medidas que los usuarios finales pueden adoptar para interrumpir o reducir al mínimo la recopilación. De esta manera, el artículo 8, apartado 2, letra b), da la impresión de que las organizaciones podrán recopilar información emitida por los equipos terminales para rastrear los movimientos físicos de las personas (como por ejemplo «seguimiento por wifi» o «seguimiento por Bluetooth») sin el consentimiento del individuo afectado. Parece que la parte que recopila tales datos podría demostrar el cumplimiento mediante una advertencia que informe a los usuarios de que apaguen sus dispositivos cuando no deseen ser rastreados. Este planteamiento sería contrario al objetivo básico de la política de telecomunicaciones de la Comisión Europea de ofrecer conectividad a internet móvil de alta velocidad, con una protección elevada de la privacidad y a bajo coste, a todos los europeos y trascendiendo las fronteras. Por otro lado, la propuesta de Reglamento no impone ninguna limitación clara por lo que respecta al alcance de la recogida de datos o las actividades de tratamiento ulteriores. En este contexto, cabe señalar que estas direcciones MAC constituyen datos personales, incluso después de aplicar medidas de seguridad como el uso de la función *hash*. Al no imponer más requisitos o limitaciones, el nivel de protección de estos datos personales al amparo de la propuesta de Reglamento es considerablemente menor al otorgado por el RGPD, con arreglo al cual este tipo de seguimiento ha de ser leal, lícito y transparente. Asimismo, el considerando 25 señala, de manera poco útil, que algunas de las funcionalidades del seguimiento por wifi no entrañan graves riesgos para la privacidad, mientras que otras —como el seguimiento de las personas a lo largo del tiempo— sí. Si bien el Grupo de Trabajo valora que se reconozcan los graves riesgos de privacidad que estas últimas plantean, no es de utilidad decidir ya de antemano que otras funcionalidades no lo hacen, sin evaluar en mayor profundidad las circunstancias y la proporcionalidad del tratamiento. Tal evaluación debería llevarse a cabo teniendo en cuenta las condiciones que se exponen a continuación en relación con el seguimiento por wifi sin anonimizar.

En función de las circunstancias y la finalidad de la recogida de datos, con arreglo al RGPD, el seguimiento es susceptible de estar sujeto a consentimiento o de que solo pueda llevarse a cabo si los datos personales recogidos se anonimizan. Lo ideal es que esta anonimización se realice justo después de la recogida. Si la anonimización inmediata no es posible habida cuenta de la finalidad con la que se recogen los datos, estos datos podrán ser tratados durante un periodo en el que no estén anonimizados únicamente en las siguientes condiciones: i) la finalidad de la recogida de datos de equipos terminales debe limitarse al mero recuento estadístico (véanse los ejemplos que figuran a continuación); ii) el seguimiento se limita en el tiempo y el espacio en la medida estrictamente necesaria para tal fin; iii) los datos se eliminan o anonimizan inmediatamente después; y iv) existe la posibilidad efectiva de exclusión voluntaria. Obviamente, los responsables del tratamiento han de cumplir la obligación de facilitar información adecuada en todas las circunstancias.

Al Grupo de Trabajo le preocupa que la posible oferta de una exclusión voluntaria individual por organización que recoja dichos datos impondría una carga inaceptable sobre los ciudadanos, dado el incremento del despliegue de este tipo de tecnologías de seguimiento por parte de organizaciones privadas y del sector público. Por consiguiente, el Grupo de Trabajo insta al legislador europeo a que promueva el desarrollo de normas técnicas para que los dispositivos indiquen automáticamente la objeción a dicho seguimiento, y para garantizar que el respeto a dicha indicación sea exigible.

Por ejemplo, con arreglo al RGPD probablemente se requeriría consentimiento cuando un responsable del tratamiento de datos recoge y almacena direcciones MAC indirectamente identificables (por wifi o Bluetooth) de dispositivos y calcula la localización del usuario, a fin de rastrear la localización del usuario a lo largo del tiempo, por ejemplo, en múltiples tiendas. Este es especialmente el caso cuando este seguimiento se produce en zonas públicas, donde los usuarios tienen la expectativa legítima de no ser identificados o rastreados y, aun así, se recogen las direcciones MAC de los viandantes. Este consentimiento podría obtenerse, por ejemplo, a través de una aplicación que invite a los usuarios a permitir el seguimiento de su localización en zonas específicas a cambio de ofertas comerciales, u ofreciendo puntos de registro dentro de ubicaciones específicas o a través de un módulo de consentimiento en los punto de acceso inalámbrico.

Solo en un número limitado de circunstancias debería permitirse que los responsables del tratamiento de datos traten la información emitida por los equipos terminales a efectos de rastrear sus movimientos físicos sin el consentimiento del individuo afectado. Por ejemplo, este podría ser el caso cuando se lleva a cabo un recuento de los clientes dentro de una ubicación específica, o cuando se recopilan los datos emitidos a ambos lados de un control de seguridad para mostrar el tiempo de espera. No obstante, en ambas situaciones habría que suprimir o anonimizar los datos una vez cumplida la finalidad estadística. Esto implica que las direcciones MAC de los dispositivos de los visitantes dentro de una ubicación específica, como una tienda, han de anonimizarse inmediatamente tras la recogida, sin que haya un almacenamiento permanente de las direcciones MAC y de tal forma que volver a identificarlos esté técnicamente excluido. En el caso del cálculo del tiempo de espera, las direcciones MAC deberían ser suprimidas o anonimizadas en cuanto los datos ya no sean pertinentes para calcular el tiempo de espera (por ejemplo, porque el visitante ha alcanzado el otro lado del control de seguridad o porque ha abandonado la cola). Por otro lado, el responsable del tratamiento habría de cumplir los requisitos de minimización de datos (por ejemplo, no realizar un seguimiento 24 horas al día, 7 días a la semana cuando la finalidad se limita al horario comercial de la tienda o al muestreo a intervalos). Asimismo, los responsables del tratamiento deben adoptar otras medidas de mitigación para garantizar que el impacto sobre los derechos a la privacidad de los usuarios es mínimo o nulo, por ejemplo para proteger la privacidad de las personas que viven cerca de los puntos de recogida.

Llama especialmente la atención que en el artículo 8, apartado 2, de la propuesta de Reglamento, se haya optado por requerir una mera advertencia, habida cuenta de la

conclusión del considerando 20 de que también es posible recopilar a distancia información relacionada con el dispositivo del usuario final a efectos de identificación y seguimiento, y que este tratamiento, conforme a la propuesta de Reglamento, puede suponer una grave intromisión en la vida privada de ese usuario final. Por otro lado, la obligación no va más allá de la obligación de información ya prevista en los artículos 13 y 14 del RGPD. La grave intromisión en la vida privada mediante el seguimiento se ve agudizada con la posibilidad de que otros accedan a los datos recogidos, como por ejemplo la posibilidad de que las fuerzas o cuerpos de seguridad identifiquen a los usuarios finales a partir de la dirección o direcciones MAC almacenadas emitidas por sus dispositivos móviles.

18. Deben elaborarse las condiciones en las que se permite el análisis del contenido y los metadatos.

El artículo 6 de la propuesta de Reglamento otorga un nivel de protección diferente a los metadatos y al contenido. El Grupo de Trabajo no respalda esta distinción: ambas categorías de datos son altamente sensibles. Por ello, los metadatos y el contenido deben recibir el mismo nivel de protección. Así, el punto de partida debería ser la prohibición del tratamiento de metadatos y del contenido sin el consentimiento de todos los usuarios finales (es decir, el emisor y el destinatario).

No obstante, en función del fin de que se trate, podría permitirse determinado tratamiento sin consentimiento, de ser estrictamente necesario para el fin perseguido:

- Los proveedores pueden tratar los datos de comunicaciones electrónicas para las finalidades mencionadas en el artículo 6, apartado 1, letras a) y b), y apartado 2, letras a) y b), de la propuesta de Reglamento⁷.
- Debería precisarse que determinadas técnicas de detección/filtrado de correo basura y mitigación de redes zombi también podrían considerarse estrictamente necesarias para detectar o impedir la utilización abusiva de servicios de comunicaciones electrónicas [artículo 6, apartado 2, letra b)]. Con respecto al filtrado del correo basura, deberían ofrecerse a los usuarios finales que reciban este tipo de correo, siempre que sea técnicamente viable, opciones de exclusión voluntaria pormenorizadas.
- Debería aclararse que el análisis de los datos de comunicaciones electrónicas a efectos de prestar un servicio al cliente también podría enmarcarse en la excepción de necesidad «para proceder a la facturación» [véase el artículo 6, apartado 2, letra b)]. Los metadatos correspondientes pueden conservarse hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago con arreglo a la legislación nacional. Los datos pertinentes (como por ejemplos los de la URL) solo podrán conservarse a

⁷ Con respecto a la necesidad de cumplir los requisitos obligatorios de calidad del servicio esbozados en el artículo 6, apartado 2, letra a), de la propuesta de Reglamento, los proveedores deberían tener en cuenta las condiciones descritas en el Reglamento (UE) 2015/2120, concretamente en el artículo 3 y los considerandos 10 y 13 a 15. Sobre la base de esta disposición, podría requerirse a los proveedores que tratan los datos de comunicaciones que detectaran y filtraran programas maliciosos y programas espía, y podría permitírseles comprimir datos.

petición del usuario final y, aun así, únicamente durante el tiempo que sea estrictamente necesario para resolver la controversia por la facturación (lo que implica que el artículo 7, apartado 3, debe modificarse en consecuencia).

- Debería contemplarse la posibilidad de tratar datos de comunicaciones electrónicas a efectos de prestar servicios solicitados expresamente por un usuario final, como la funcionalidad de búsqueda o de indexación de palabras clave, asistentes virtuales, motores de conversión de texto a voz y servicios de traducción. Esto requiere la introducción de una excepción para el análisis de tales datos para uso (doméstico) puramente individual, así como para uso individual profesional⁸. Así, ello sería posible sin el consentimiento de todos los usuarios finales, aunque podría producirse únicamente con el consentimiento del usuario final que solicita el servicio. Tal consentimiento específico también evitaría que el proveedor utilizara estos datos para otros fines.

Esto implica que el análisis del contenido y/o los metadatos a cualquier otro efecto, como la realización de análisis, elaboración de perfiles, publicidad comportamental u otros fines que redunden en el beneficio (comercial) del proveedor requiere el consentimiento de todos los usuarios finales cuyos datos se tratarían. Por lo que respecta a tales situaciones, la propuesta de Reglamento debería explicar que el mero acto de enviar un correo electrónico u otro tipo de comunicación personal desde otro servicio a un usuario final que haya dado personalmente el consentimiento para que su contenido y metadatos sean tratados (por ejemplo, durante la suscripción a un servicio de correspondencia) no constituye un consentimiento válido del remitente.

Por último, debería aclararse que el tratamiento de datos de personas distintas de los usuarios finales implicados (p. ej., la imagen o descripción de un tercero en un intercambio entre dos personas) también ha de cumplir todas las disposiciones pertinentes del RGPD.

19. **Los equipos terminales y los programas informáticos deben desincentivar, impedir y prohibir por defecto toda interferencia ilícita en los mismos y facilitar información sobre las posibilidades al respecto.** Si bien la propuesta de Reglamento obliga a los proveedores de programas informáticos que permiten comunicaciones electrónicas a «ofrecer la posibilidad» de evitar una forma limitada de interferencia en los equipos terminales y, al iniciarse la instalación, obliga a los proveedores de programas informáticos a solicitar el consentimiento del usuario final respecto de una configuración determinada (artículo 10, apartados 1 y 2), esta opción no es equiparable a la *privacidad por defecto*. Por otro lado, la «posibilidad» de evitar determinada interferencia ya existe en la actualidad, y hasta la fecha no ha conseguido que se ataje suficientemente el problema del seguimiento injustificado. Es

⁸ Si bien el considerando 13 de la propuesta de Reglamento excluye expresamente del ámbito de aplicación del Reglamento a las redes corporativas, esta nueva excepción de utilización individual también debería abordar el uso de servicios en la nube por parte de los empleados en el contexto laboral, como por ejemplo la búsqueda en su correo electrónico.

precisamente este el motivo por el que en el RGPD se ha tomado la decisión política consciente de introducir los principios de protección de los datos y de privacidad desde el diseño y por defecto (artículo 25 del citado Reglamento). La propuesta de Reglamento socava estos principios por lo que respecta a los datos de las comunicaciones y los dispositivos. Entre tanto, la Directiva 2014/53/UE sobre equipos radioeléctricos⁹ (mencionada en el considerando 10) solo contempla una obligación de seguridad muy limitada, requiriendo que los equipos radioeléctricos contengan «salvaguardias que garanticen la protección de los datos personales y la privacidad del usuario y del abonado» [artículo 3, apartad 3, letra e)]. Esto no puede sustituir a la configuración específica de privacidad por defecto en la propuesta de Reglamento. A este respecto, cabe mencionar asimismo que la encuesta Eurobarómetro sobre privacidad y comunicaciones electrónicas, publicada en diciembre de 2016, señala que «casi siete de cada diez personas (69 %) se muestran totalmente de acuerdo con que la configuración por defecto de su navegador impida que su información sea compartida»¹⁰. El Grupo de Trabajo encuentra otros aspectos preocupantes con respecto a la configuración del navegador y la definición de «terceros». Véase la observación 24. Por otro lado, debería tenerse en cuenta que esta disposición no solo atañe a los navegadores utilizados en los ordenadores, sino que también se hace extensiva a otros tipos de programas informáticos que permiten la comunicación (incluidos sistemas operativos, aplicaciones e interfaces informáticas para dispositivos conectados al internet de las cosas). En resumen, los equipos terminales y los programas informáticos deben ofrecer *por defecto* configuraciones de protección de la privacidad y guiar a los usuarios a través del menú de configuración para cambiar estos ajustes por defecto en el momento de la instalación. Dicho menú de configuración debería ser siempre de fácil acceso durante la utilización. El Grupo de Trabajo anima a los legisladores europeos a aclarar el alcance del artículo 10 a tales efectos.

- 20. El Reglamento sobre la privacidad y las comunicaciones electrónicas debería prohibir explícitamente los muros de seguimiento**, esto es, la práctica por la cual se deniega el acceso a un sitio web o servicio a menos que los usuarios acepten ser rastreados en otros sitios web o servicios. Como ya se ha señalado en dictámenes anteriores del Grupo de Trabajo en relación con la Directiva sobre la privacidad y las comunicaciones electrónicas¹¹, estos planteamientos de «lo tomas o lo dejas» rara vez son legítimos¹². Cuando el uso de las capacidades de tratamiento y almacenamiento de los equipos terminales o la recopilación de información de los equipos terminales de los usuarios finales permite el rastreo de las actividades del usuario a lo largo del tiempo, o transversalmente entre servicios (p. ej., distintos sitios web o aplicaciones),

⁹ Directiva 2014/53/UE sobre equipos radioeléctricos.

¹⁰ Véase el Eurobarómetro Flash 443, Informe sobre privacidad y comunicaciones electrónicas (publicado en diciembre de 2016), p. 5.

¹¹ Véase, por ejemplo, WP240 (revisión de la Directiva sobre la privacidad y las comunicaciones electrónicas), p. 16; WP 208 (excepción relativa al consentimiento), p. 5.

¹² Esta posición debe entenderse sin perjuicio del artículo 7, apartado 4, del RGPD, que también podría excluir las opciones de «lo tomas o lo dejas» en otros casos en que resulte apropiado.

dichas actividades de tratamiento podrían suponer una grave intromisión en la vida privada de esos usuarios. Dada la importancia fundamental de internet a la hora de permitir el derecho fundamental de libertad de expresión, incluido el derecho de acceso a la información, la capacidad de los usuarios para acceder a contenidos en línea no debería depender de la aceptación del seguimiento de sus actividades en diferentes dispositivos y sitios web/aplicaciones. Por consiguiente, el futuro Reglamento sobre la privacidad y las comunicaciones electrónicas debería especificar que el acceso a contenidos, por ejemplo, en sitios web y aplicaciones no puede supeditarse a la aceptación de dichas actividades de seguimiento intrusivas, independientemente de la tecnología de seguimiento empleada, tales como *cookies*, huella digital de dispositivo, utilización de identificadores únicos u otras técnicas de seguimiento. La necesidad de esta prohibición se hace más patente con la encuesta Eurobarómetro sobre privacidad y comunicaciones electrónicas publicada recientemente, en la que se señala que casi dos tercios de los encuestados indican que «es inaceptable que se monitoricen sus actividades en línea a cambio de poder acceder sin restricciones a determinado sitio web (64 %)».

21. En resumen, por lo que respecta a los cuatro aspectos mencionados, **la propuesta de Reglamento debería cumplir su promesa de ofrecer un nivel de protección igual o superior al del RGPD**. En el considerando 5 se afirma sin rodeos que la propuesta de Reglamento no reduce el nivel de protección que depara el RGPD. No obstante, ateniéndose a la forma actual de la propuesta de Reglamento, esta afirmación es incorrecta, en particular por lo que respecta al seguimiento de los dispositivos (observación 17), la ausencia del principio de privacidad por defecto (observación 19) y el consentimiento (observación 18). Esto es especialmente pertinente ya que en el mismo considerando se señala que la propuesta de Reglamento «constituye una *lex specialis* en relación con el RGPD, precisándolo y completándolo en lo que respecta a los datos de comunicaciones electrónicas que se consideran datos personales». El Grupo de Trabajo sugiere que, como mínimo, el texto del Reglamento sobre la privacidad y las comunicaciones electrónicas aclare que:

- i) las prohibiciones contenidas en la propuesta de Reglamento gozan de prioridad sobre los permisos recogidos en el RGPD [p. ej., la prohibición de interferencia recogida en el artículo 5 de la propuesta de Reglamento goza de prioridad sobre los derechos de los proveedores de servicios de comunicaciones electrónicas de tratar ulteriormente datos personales con arreglo al artículo 5, apartado 1, letra b), y al artículo 6, apartado 4, del RGPD];
- ii) cuando se permita el tratamiento al amparo de cualquier excepción (también en relación con el consentimiento) a las prohibiciones recogidas en el Reglamento sobre la privacidad y las comunicaciones electrónicas, dicho tratamiento, cuando afecte a datos personales, aún debe respetar todas las disposiciones pertinentes del RGPD;
- iii) cuando se permita el tratamiento al amparo de cualquier excepción a las prohibiciones recogidas en el Reglamento sobre la privacidad y las comunicaciones electrónicas, se prohibirá cualquier otro tratamiento sobre la base del RGPD, incluido el tratamiento para otros fines con arreglo al artículo 6, apartado 4, del RGPD. Ello no sería óbice para que los responsables del tratamiento soliciten un consentimiento adicional para las nuevas operaciones

de tratamiento. Tampoco impediría que los legisladores contemplasen excepciones adicionales, limitadas y específicas en el Reglamento sobre la privacidad y las comunicaciones electrónicas, por ejemplo, para permitir el tratamiento con fines científicos o estadísticos con arreglo al artículo 89 del RGPD, o para proteger «intereses vitales» de las personas físicas conforme al artículo 6, apartado 1, letra d), del RGPD.

Por otro lado, el Reglamento sobre la privacidad y las comunicaciones electrónicas debería interpretarse de tal forma que se garantice que conceda un nivel de protección igual o, en su caso, superior, al del RGPD.

4. OTROS ASPECTOS QUE PLANTEAN PREOCUPACIONES

Además de los aspectos mencionados anteriormente, el Grupo de Trabajo del Artículo 29 se muestra **preocupado** por lo siguiente.

ES PRECISO AMPLIAR EL ALCANCE TERRITORIAL Y MATERIAL

22. **La definición del término «metadatos» es excesivamente restrictiva.** Actualmente el término se define en el artículo 4, letra c), como los «datos tratados en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas (el énfasis es nuestro). El uso de la palabra «red» parece sugerir que solo los datos generados en el transcurso de la prestación de los servicios en la capa «inferior» de la red se considerarían «metadatos». Esto podría implicar que los datos generados en el transcurso de la prestación de un servicio OTT quedarían excluidos de este ámbito de aplicación, lo que no resultaría deseable, y probablemente tampoco se pretende, dada la intención de ampliar el ámbito de aplicación de la propuesta de Reglamento a los proveedores de servicios OTT. Para abordar esta cuestión, la definición de «metadatos de comunicaciones electrónicas» debería modificarse para incluir todos los datos tratados con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas.

23. Por otro lado, también es motivo de preocupación que **el ámbito de aplicación territorial de la propuesta de Reglamento con respecto a las organizaciones sin establecimiento en la UE solo abarque a los proveedores de servicios de comunicaciones electrónicas.** A tenor de lo dispuesto en la propuesta de Reglamento, el proveedor de un servicio de comunicaciones electrónicas que no esté establecido en la Unión deberá designar por escrito a un representante en la Unión (artículo 3, apartado 2). También se menciona en el considerando 9 que el Reglamento será de aplicación al tratamiento por parte de proveedores de servicios de comunicaciones electrónicas, independientemente del lugar en que se efectúe el tratamiento. El Grupo de Trabajo acoge con satisfacción esta aclaración. No obstante, puesto que la redacción se limita a los proveedores de servicios de comunicaciones electrónicas, no queda claro en qué medida este alcance territorial se aplica a otra clase de partes [por ejemplo, partes que interfieran con información emitida por los equipos terminales de los usuarios finales o que la recopilen; véase el artículo 3, apartado 1, letra c), junto con el artículo 8 de la propuesta de Reglamento]. Por consiguiente, el Grupo de Trabajo sugiere que se modifique el artículo 3, apartados 2

y 5, para incluir a los proveedores de guías accesibles al público, los proveedores de programas informáticos que permiten comunicaciones electrónicas y las personas que envían comunicaciones comerciales de mercadotecnia directa o recopilan (otra) información relativa a los usuarios finales o que está almacenada en sus equipos terminales, siempre que sus actividades estén dirigidas a usuarios en la UE (véase el considerando 8 de la propuesta de Reglamento)¹³.

DEBE REFORZARSE LA PROTECCIÓN DE LOS EQUIPOS TERMINALES

Otro tipo de inquietudes tienen que ver con la insuficiente protección de los equipos terminales en la propuesta de Reglamento.

24. En primer lugar, **la propuesta de Reglamento sugiere erróneamente que es posible otorgar un consentimiento válido a través de configuraciones no específicas del navegador**. El Grupo de Trabajo reconoce que actualmente los usuarios finales se ven desbordados por las solicitudes de consentimiento (considerando 22). La configuración de los navegadores (y de los programas informáticos comparables tienen un papel que desempeñar en la resolución de este problema. No obstante, ya que la configuración general de los navegadores no está concebida para aplicarse al uso de una tecnología de seguimiento en un caso en concreto, no es idónea para otorgar consentimiento con arreglo al artículo 7 y el considerando 32 del RGPD (puesto que el consentimiento no está suficientemente fundamentado ni es específico).

El usuario final debe estar en condiciones de dar un consentimiento individual al seguimiento para cada sitio web o aplicación con diferentes finalidades (como por ejemplo el intercambio en redes sociales o la publicidad). Un responsable del tratamiento a cargo de varios sitios web o aplicaciones también podría solicitar el consentimiento para todos los sitios o aplicaciones bajo su control, siempre que esta solicitud de consentimiento se presente por separado.

Por otro lado, el responsable del tratamiento debe cumplir todas las demás obligaciones relativas al consentimiento, incluida la obligación de facilitar a los usuarios información adecuada. Tanto en el caso de los navegadores como en el de los responsables del tratamiento, esto implica que no sería válido que solo ofreciesen una opción de «aceptar todas las *cookies*», puesto que esto no permitiría a los usuarios dar el consentimiento pormenorizado requerido. Sin embargo, debería ser posible que los navegadores permitiesen a los usuarios adoptar la decisión fundamentada y consciente de aceptar todas las *cookies*, evitando así que en el futuro reciban solicitudes de consentimiento específicas de los sitios web que visiten.

El Grupo de Trabajo recomienda encarecidamente que el Reglamento sobre la privacidad y las comunicaciones electrónicas haga obligatorio que los navegadores

¹³ Véase el artículo 3, apartado 2, del RGPD: «*El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión*». Esta obligación podría incluir asimismo excepciones similares a las establecidas en el artículo 27, apartado 2, del RGPD.

apliquen mecanismos técnicos, como la norma *Do Not Track*, para garantizar que los usuarios tienen verdadera capacidad de elección y control sobre la interferencia con sus dispositivos¹⁴.

Más importante aún, el Reglamento sobre la privacidad y las comunicaciones electrónicas debe garantizar que todos los responsables del tratamiento aceptan como indicación jurídicamente vinculante del consentimiento o la denegación tanto la elección con respecto al almacenamiento de información en el dispositivo como un indicativo DNT del navegador. Esto debe entenderse sin perjuicio de una posterior orientación del Grupo de Trabajo respecto de la conformidad de la norma DNT, entre otros, con el principio de limitación de la finalidad, una vez concluida la norma (prevista para finales de 2017).

Los tipos de «consentimiento» implícitos, como hacer clic en el sitio web o desplazarse por la página, no pueden invalidar las opciones con respecto al almacenamiento y el indicativo DNT. Una ventaja importante de la utilización de esta norma es que no se limita a la tecnología de rastreo de *cookies*, sino que también se extiende a otros tipos de seguimiento, como la huella digital de dispositivo.

Hacer legalmente obligatorio el cumplimiento de esta norma también resolverá el problema que plantea el uso actual del término «terceros» en el artículo 10. Por lo general, una página web o aplicación contiene numerosos elementos, tanto del propio sitio web como elementos externos. También es posible que un código externo se ejecute en el contexto del sitio web visitado, al tiempo que envía información a un servidor de un tercero. Una primera parte puede suministrar una *cookie* de rastreo cuando un usuario visita, por ejemplo, un sitio de redes sociales, que, a su vez, también puede ser un tercero, cuando el mismo usuario visita otro sitio web que incluye interacción con dicho sitio de redes sociales. En todos estos casos, independientemente de que se trate de «acceso» a la información del dispositivo del usuario final o de «almacenamiento» de información en el mismo, esto constituye una interferencia en el dispositivo, para la cual se requiere consentimiento (a menos que sea de aplicación una de las excepciones). En la norma DNT, esta situación se aborda utilizando los términos «en todo el sitio» y «en todo internet». Por consiguiente, para mejorar la seguridad jurídica de todas las partes interesadas, debe reformularse la referencia a «terceros» incluida en el Reglamento sobre la privacidad y las comunicaciones electrónicas para que abarque a todas las entidades con las que interactúa un dispositivo (porque almacenan información en el dispositivo o acceden a la información que este contiene).

A fin de que la norma *Do Not Track* sea compatible con el elevado nivel de protección de la confidencialidad de las comunicaciones y la protección de datos amparados por la Carta, el Reglamento sobre la privacidad y las comunicaciones electrónicas debería especificar que las solicitudes de seguimiento a escala de internet, a diferencia del seguimiento a escala de sitio, deben presentarse de manera independiente y los usuarios deberían ser libres de aceptar o rechazar tales solicitudes. Por otro lado, con el fin de proteger a los usuarios frente a solicitudes de

¹⁴ Véase la URL: <https://www.w3.org/TR/tracking-compliance/>. El apartado 7 explica el modelo de excepción y la distinción entre excepciones a escala de sitio y de web. El apartado 6 contiene la información legible por máquina que los responsables del tratamiento pueden facilitar por lo que respecta al requisito de información para obtener el consentimiento.

consentimiento frecuentes, el Reglamento sobre la privacidad y las comunicaciones electrónicas debería garantizar que la negativa a aceptar un seguimiento a escala de internet por parte de una organización específica (a través de la norma *Do Not Track* o de una lista negra independiente) implique que dicha organización no pueda realizar futuras solicitudes de consentimiento durante al menos seis meses. Esta norma no es óbice para que dicha organización, cuando reciba la visita directa del usuario (es decir, en calidad de primera parte), solicite el consentimiento en su propio sitio web (es decir, una solicitud de consentimiento a escala de sitio). En la práctica esto implica que, por ejemplo, un sitio de emisión de vídeo en tiempo real que suministre *cookies* de rastreo podrá solicitar el consentimiento cuando este usuario visite el sitio de emisión de vídeo en tiempo real, pero no podrá volver a solicitar el consentimiento por un periodo de seis meses cuando el usuario haya denegado su consentimiento y visite otros sitios web que contengan vídeos suministrados por el sitio web de emisión en tiempo real.

25. Por otro lado, **la redacción de la excepción aplicable a la «medición de la audiencia en la web» es imprecisa.** El artículo 8, apartado 1, letra d), de la propuesta de Reglamento contempla una excepción para la medición de la audiencia en la web. El primer punto de preocupación es que este término es impreciso y podría confundirse con la elaboración de perfiles de usuario. La definición debería dejar claro que no se puede recurrir a esta excepción con fines de elaboración de perfiles. La excepción debería aplicarse exclusivamente a la analítica del uso necesaria para analizar el rendimiento del servicio solicitado por el usuario, pero no a la analítica de usuarios (es decir, el análisis del comportamiento de usuarios identificables de un sitio web, una aplicación o un dispositivo). Por consiguiente, no se puede recurrir a esta excepción en circunstancias en que los datos puedan vincularse a datos de usuarios identificables tratados por el proveedor u otros responsables de tratamiento. Por otro lado, su descripción sugiere una aplicación muy específica desde el punto de vista tecnológico. Por lo tanto, el término «medición de la audiencia en la web» debería reformularse de una manera tecnológicamente neutral para incluir también la información analítica de uso similar obtenida de aplicaciones, tecnología adherible al cuerpo y dispositivos del internet de las cosas.

El Grupo de Trabajo sugiere tomar como inspiración la excepción prevista en la legislación neerlandesa, que se aplica si es estrictamente necesario para obtener información sobre la calidad técnica o la eficacia de un servicio de la sociedad de la información prestado y tiene un impacto mínimo o nulo en la privacidad del abonado o usuario final afectado [véase el artículo 11.7 *bis*, apartado 3, letra b), de la Ley de telecomunicaciones neerlandesa]. Esta excepción tiene en cuenta el hecho de que la mayor parte de los datos recopilados a partir de los análisis web o de aplicaciones siguen siendo datos personales. Esto implica que el tratamiento de estos datos también está sujeto al RGPD y que, por ejemplo, la analítica del uso también puede ser llevada a cabo por una organización externa, pero solo si:

- i) dicha organización actúa como encargada del tratamiento de datos;
- ii) se celebra un acuerdo de encargado del tratamiento conforme con el RGPD;
- iii) la tecnología de análisis utilizada evita la reidentificación, incluida, por ejemplo, la anonimización de las direcciones IP de los usuarios;

- iv) las *cookies* u otros datos específicos utilizados para el análisis solo se pueden usar para el sitio, aplicación o tecnología adherible al cuerpo de que se trate y no pueden vincularse a otros datos identificables;
- v) los usuarios tienen el derecho de exclusión voluntaria (véanse asimismo las observaciones 17 y 50 del presente Dictamen).

Aunque si se cumplen estas condiciones no se requeriría consentimiento, aun así los responsables del tratamiento deben facilitar información adecuada a los usuarios, por ejemplo a través de los campos de representación del estado de seguimiento de la norma *Do Not Track*¹⁵.

26. El Reglamento sobre la privacidad y las comunicaciones electrónicas **debería garantizar que las excepciones relativas al requisito de consentimiento sean restrictivas y estén formuladas con precisión**. La redacción de la excepción al requisito de consentimiento para la interferencia en dispositivos contemplada en el artículo 8, apartado 1, letra c), es prácticamente idéntica a la redacción actual recogida en el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas («en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario»), pero se ha omitido sin explicación la palabra fundamental «estrictamente». Esto suscita preocupación por dos motivos: por un lado, la disposición de la Directiva sobre la privacidad y las comunicaciones electrónicas ya ha generado un amplio debate en cuanto a su alcance entre las autoridades de control y las organizaciones, y la supresión de la palabra «estrictamente» no hará sino aportar menos seguridad jurídica. Resulta preocupante también porque el Grupo de Trabajo ya ha ofrecido orientación en cuanto a la interpretación del término «estrictamente» en este contexto. El Grupo de Trabajo sugirió la siguiente aclaración en su Dictamen sobre la excepción al consentimiento de las *cookies* (WP 194):

«Una cookie es estrictamente necesaria para prestar una funcionalidad específica al usuario (o abonado): si las cookies no funcionan, la funcionalidad no se prestará y dicha funcionalidad ha sido solicitada explícitamente por el usuario (o abonado), como parte de un servicio de la sociedad de la información.»¹⁶

Por otro lado, el Grupo de Trabajo aclaró que:

«las "cookies de terceros" no suelen ser "estrictamente necesarias" para el usuario que visita un sitio web, ya que suelen estar generalmente vinculadas a un servicio distinto del servicio "solicitado específicamente" por el usuario»¹⁷.

¹⁵ Véase: Tracking Preference Expression (DNT), borrador del editor, 7 de marzo de 2016.

¹⁶ Grupo de Trabajo del Artículo 29, WP 294, Dictamen 04/2012 sobre la exención del requisito de consentimiento de *cookies*, adoptado el 7 de junio de 2012, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_es.pdf.

¹⁷ *Ibidem*.

El Grupo de Trabajo añadió que el uso de módulos de complementos de contenidos sociales destinados a personas que no sean usuarios de una plataforma o sitio web tampoco se consideraría estrictamente necesario.

Asimismo, aunque el artículo 6, apartado 1, letra b), de la propuesta de Reglamento permite el tratamiento de datos de comunicaciones electrónicas «cuando sea necesario» por motivos de seguridad, el considerando 49 del RGPD exige que esto sea en la medida estrictamente necesaria. Es posible que la omisión de la palabra «estrictamente» no haya sido intencionada, puesto que el considerando 21 de la propuesta de Reglamento sí menciona que no ha de solicitarse consentimiento para interferir cuando sea «estrictamente» necesario. No obstante, la propuesta de Reglamento brinda la oportunidad de aclarar aún más que la prueba de necesidad en el contexto del Reglamento debe interpretarse restrictivamente con respecto a todas las excepciones. Por consiguiente, el Grupo de Trabajo sugiere que, en relación con todas las excepciones contempladas en el artículo 6 y el artículo 8, apartado 1, de la propuesta de Reglamento, se añada la palabra «estrictamente» antes de «necesario».

Por otro lado, el Reglamento sobre la privacidad y las comunicaciones electrónicas debería permitir explícitamente interferir en los equipos para instalar actualizaciones de seguridad. El envío de actualizaciones de seguridad a través de internet es el método preferido para instalar dichas actualizaciones en la mayoría de los dispositivos de los usuarios finales. La instalación de actualizaciones se considera una interferencia en los equipos terminales. Existe un interés legítimo en garantizar que la seguridad de estos dispositivos está actualizada. Por consiguiente, los proveedores de parches de seguridad deberían poder, en general, instalar las actualizaciones de seguridad estrictamente necesarias sin el consentimiento del usuario final. No obstante, no está claro si esta interferencia puede acogerse a la excepción a la prohibición de interferencia relativa a la «sociedad de la información» [artículo 8, apartado 1, letra c)]. Debería aclararse que la instalación de actualizaciones de seguridad está permitida al amparo de esta excepción, pero únicamente en la medida en que: i) las actualizaciones de seguridad vengan en paquetes discretos y no alteren en forma alguna la funcionalidad de los programas informáticos del equipo (incluida la interacción con otros programas o configuraciones elegidos por el usuario); ii) se informe de antemano al usuario final cada vez que se instale una actualización; y iii) el usuario final tenga la posibilidad de desactivar la instalación automática de estas actualizaciones.

MERCADOTECNIA DIRECTA

Otros temas de preocupación están relacionados con la insuficiente protección frente a la mercadotecnia directa.

27. En primer lugar, resulta preocupante que **el ámbito de la mercadotecnia directa sea demasiado limitado**. El artículo 4, apartado 3, letra f), de la propuesta de Reglamento define «comunicaciones de mercadotecnia directa» como «toda forma de publicidad, oral o escrita, enviada a uno o varios usuarios finales identificados o identificables de servicios de comunicaciones electrónicas». El uso de la palabra

«enviada» implica la utilización de medios de comunicación tecnológicos que conllevan necesariamente el transporte de una comunicación, mientras que la mayor parte de la publicidad en la web (a través de plataformas de redes sociales o en sitios web) no conllevaría el «envío» de anuncios en sentido estricto. Este hecho también se confirma con los ejemplos que se dan a continuación en la definición (SMS, correo electrónico) y en el considerando 33. Todos ellos se refieren a formas bastante tradicionales de comunicación con fines de mercadotecnia, y, aun así, el uso de sistemas de llamada —bastante tradicionales— presumiblemente queda excluido del ámbito de aplicación. El artículo y el considerando deberían modificarse para incluir toda la publicidad «enviada, dirigida o presentada» a uno o varios usuarios identificados o identificables. Por otro lado, debe garantizarse asimismo que la publicidad comportamental (basada en los perfiles de usuarios finales) también se considera comunicaciones de mercadotecnia directa dirigida a «uno o varios usuarios finales identificados o identificables» (puesto que este tipo de publicidad está destinada a usuarios específicos e identificables).

Por otro lado, de acuerdo con el ámbito de aplicación propuesto de las «comunicaciones de mercadotecnia directa», la protección otorgada por el artículo 16, apartado 1, se limitaría a los mensajes que contengan material publicitario y no protegería a las personas de otros mensajes enviados, dirigidos o presentados con fines de mercadotecnia (como por ejemplo mensajes de generación de oportunidades de venta que persiguen el consentimiento, promoción de ideas políticas o preferencias de voto, promoción de asociaciones benéficas u otras organizaciones sin ánimo de lucro o de desarrollo general de marca de una organización). Asimismo, aunque no se mencionan en la definición, siguen utilizándose aparatos de fax como método de mercadotecnia directa. El artículo 4, apartado 3, letra f), debería incluir, por tanto, toda forma de publicidad, propaganda o promoción, también en el caso de las organizaciones sin ánimo de lucro, y debería incluir explícitamente los aparatos de fax junto al correo electrónico y los SMS [véase asimismo la sugerencia de aclaración de la observación 43, letra a)]. Por último, el considerando 32 establece que la mercadotecnia directa incluye los mensajes enviados por los partidos políticos con fines de propaganda política. Debe actualizarse la redacción para incluir a los políticos y a los candidatos electorales que hacen propaganda de su candidatura.

28. En segundo lugar, **la retirada del consentimiento para la mercadotecnia directa no es gratuita y no es tan fácil como su concesión**. La posibilidad de retirar el consentimiento con arreglo a la propuesta de Reglamento debe aclararse para garantizar la coherencia y mejorar la protección de los destinatarios. El artículo 16, apartado 6, de la propuesta de Reglamento prevé actualmente que se debe comunicar a los destinatarios de mercadotecnia directa «la información necesaria [...] para que estos puedan ejercer fácilmente su derecho a retirar su consentimiento para recibir nuevas comunicaciones de mercadotecnia» (el énfasis es nuestro). Este hecho se confirma en el considerando 34. No obstante, del considerando 70 del RGPD se desprende que, con arreglo a dicho Reglamento, los interesados no solo deben tener derecho a oponerse al tratamiento con fines de mercadotecnia directa de manera sencilla, sino a hacerlo también «sin coste alguno». Este término también se utiliza en el artículo 16, apartado 2, de la propuesta de Reglamento, pero únicamente en

relación con la exclusión voluntaria de la mercadotecnia directa a partir de los datos de contacto obtenidos en el contexto de una venta.

El artículo 7, apartado 3, del RGPD prevé que será tan fácil retirar el consentimiento como darlo, y que los interesados deben tener derecho a retirar su consentimiento en cualquier momento. Por otro lado, en su Dictamen 04/2010 sobre la FEDMA (WP174), el Grupo de Trabajo ya reconoció la importancia de ofrecer «un método sencillo, efectivo, gratuito, directo y de fácil acceso para dejar de recibir» mercadotecnia directa¹⁸. Esta norma para la retirada del consentimiento debería incorporarse en las disposiciones aplicables a la mercadotecnia directa en la propuesta de Reglamento. Lo mismo es de aplicación para el requisito recogido en el artículo 7, apartado 3, del RGPD de que debe ser tan fácil retirar el consentimiento como darlo en cualquier momento.

29. En relación con esto, **debería aclararse la forma de retirar el consentimiento o excluirse voluntariamente de las llamadas con fines de mercadotecnia**. Sobre la base del artículo 16, apartado 4, los Estados miembros pueden decantarse por un sistema de exclusión voluntaria para las llamadas de voz a voz con fines de mercadotecnia. El Reglamento sobre la privacidad y las comunicaciones electrónicas debería especificar el procedimiento para la retirada del consentimiento y para excluirse voluntariamente de las llamadas con fines de mercadotecnia. El considerando 36 especifica que conviene que los Estados miembros «puedan» establecer o mantener sistemas nacionales de exclusión voluntaria. Sobre la base de esta disposición, los Estados miembros, por tanto, podrían permitir una situación en la que un usuario tuviese que excluirse voluntariamente ante cada proveedor de comunicaciones. Tal aplicación no protege a los usuarios frente a las molestias de una comunicación injustificada¹⁹ ni ofrece un mecanismo conforme con el RGPD para retirar el consentimiento fácilmente y en cualquier momento. Por consiguiente, el Reglamento debería especificar que todos los Estados miembros «deben» crear una Lista Robinson de llamadas. Por otro lado, el Reglamento debería especificar que los destinatarios de llamadas de voz a voz deben disponer de dos opciones para retirar su consentimiento: de cara a futuras llamadas de esa empresa u organización y la posibilidad durante la llamada de inscribirse en una Lista Robinson nacional.
30. Otro aspecto que suscita preocupación es que **el uso de identidades falsas a la hora de enviar comunicaciones de mercadotecnia directa no se prohíbe explícitamente**. En el considerando 34 se señala que se prohíbe «la ocultación de la identidad y el uso de identidades, domicilios o números de contacto falsos a la hora de enviar comunicaciones comerciales no solicitadas para fines de mercadotecnia

18 Grupo de Trabajo del Artículo 29, WP174, Dictamen 04/2010 relativo al «Código de conducta europeo de la FEDMA sobre la utilización de datos personales en la comercialización directa», adoptado el 13 de julio de 2010, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_es.pdf.

19 Por ejemplo, el operador de telecomunicaciones BT registró en el Reino Unido 31 millones de llamadas molestas en una semana. Véase: <http://www.bbc.com/news/business-38635921>.

directa». Sin embargo, en el artículo 16, apartado 6, simplemente se indica que los usuarios finales deberán ser informados de «la identidad de la persona física o jurídica en nombre de la cual se transmite la comunicación». Esta obligación de informar a los destinatarios de la identidad debería complementarse con la prohibición de utilizar domicilios de contacto ocultos o falsos para fines de mercadotecnia directa.

31. Esta cuestión guarda relación con otro motivo de preocupación: **el requisito de prefijo para las llamadas de mercadotecnia directa se presenta como una alternativa al requisito de identificación de la línea de contacto.** Con arreglo al artículo 16, apartado 3, se permiten las llamadas de mercadotecnia directa si la persona que llama i) presenta la identificación de una línea en la que se pueda contactar a la persona física o jurídica que efectúa la llamada [artículo 16, apartado 3, letra a)]; o ii) presenta un código o prefijo específico que permita identificar que se trata de una llamada de mercadotecnia [artículo 16, apartado 3, letra b)]. Aunque el Grupo de Trabajo acoge con satisfacción la obligación contemplada en el artículo 16, apartado 3, letra b), de utilizar un prefijo, opina que este requisito no aborda la misma cuestión que trata la obligación de identificación de una línea de contacto del artículo 16, apartado 3, letra a). Mientras que la finalidad del requisito de prefijo es permitir al destinatario identificar una llamada como llamada con fines de mercadotecnia anticipadamente (y tomar medidas para bloquear estas llamadas), la del requisito de identificación de una línea de contacto es facilitar a los destinatarios (y a las autoridades de control) una serie de medios para identificar al promotor de la mercadotecnia y entrar en contacto con él. Esto es especialmente relevante en el caso de las llamadas automatizadas, que presentan un fuerte desequilibrio entre las posibilidades del responsable de la mercadotecnia para enviar llamadas molestas y las posibilidades del destinatario para evitar tales llamadas. Así, los requisitos no han de ser alternativos, sino complementarios entre sí.

CALENDARIO

32. El Grupo de Trabajo del Artículo 29 alaba a la Comisión Europea por reconocer la necesidad de que la propuesta de Reglamento entre en vigor junto al RGPD en mayo de 2018 para evitar incoherencias entre ambos actos legislativos. No obstante, sigue siendo un motivo de preocupación que se trata de un marco temporal ambicioso que también requiere concluir el proyecto de CECE. Por consiguiente, el Grupo de Trabajo solicita a todas las partes implicadas en el proceso legislativo que se comprometan con el plazo de mayo de 2018.

OTRAS PREOCUPACIONES

En la presente sección se tratarán una serie de preocupaciones adicionales.

33. En primer lugar, al Grupo de Trabajo le preocupa **la insinuación de que las medidas de conservación de datos no específicas son aceptables.** La exposición de motivos señala que, con arreglo a la propuesta de Reglamento, los Estados miembros pueden mantener o crear marcos nacionales de conservación de datos que prevean, en

particular, medidas de conservación específicas (apartado 1.3). Tras la resolución Tele2/Watson²⁰ ha quedado patente que los marcos de conservación que prevean hipótesis que no sean la de conservación específica no están permitidos al amparo de la Carta (y aun así están sujetos a importantes condiciones, como la de supervisión), y que un acceso generalizado a metadatos ha de verse como una violación de la esencia del artículo 7 de la misma manera que un acceso generalizado al contenido de una comunicación electrónica lo es (véase TJUE, Schrems, y considerando 94). La formulación de esta frase sugiere, por tanto, que los Estados miembros gozan de cierto margen de maniobra con respecto a las medidas de conservación de datos, cuando en realidad no es así. En relación con esto, la propuesta de Reglamento **no concede un nivel de protección suficiente de los metadatos**. Como se ha mencionado en la observación 10, el Grupo de Trabajo del Artículo 29 agradece el reconocimiento de que los metadatos pueden revelar datos muy sensibles. No obstante, los metadatos no reciben en la propuesta de Reglamento la protección que cabría esperar tras este reconocimiento. Dado el carácter sensible de los metadatos en particular, previamente a un análisis con arreglo al artículo 6, apartado 2, letra c), debería llevarse a cabo una EIPD (véase asimismo la observación 46).

34. En segundo lugar, **la propuesta de Reglamento ampliaría excesivamente las posibilidades de conservar datos**. El artículo 11 de la propuesta de Reglamento menciona el artículo 23, apartado 1, letras a) a e), del RGPD, a la hora de describir las finalidades por las que los Estados miembros pueden limitar las obligaciones y los derechos contemplados en los artículos 5 a 8 del Reglamento. El RGPD no prevé tales limitaciones con respecto a categorías especiales de datos, en consonancia con los riesgos elevados para los interesados. Aunque el artículo 15 de la Directiva sobre la privacidad y las comunicaciones electrónicas permite actualmente una limitación similar, las finalidades son más reducidas. La nueva propuesta de Reglamento haría posibles nuevas limitaciones con fines de «ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención» [artículo 23, apartado 1, letra d), del RGPD] y «otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social» [artículo 23, apartado 1, letra e), del RGPD]. Estos fines no solo son nuevos en comparación con la Directiva sobre la privacidad y las comunicaciones electrónicas, sino que el último fin contemplado en el artículo 23, apartado 1, letra d), y el fin contemplado en el artículo 23, apartado 1, letra e), están formulados de manera sumamente general. Por consiguiente, se sugiere eliminar la referencia al artículo 23, apartado 1, letras a) a e), del RGPD y, en su lugar, mencionar únicamente los fines contemplados en el artículo 15 de la Directiva sobre la privacidad y las comunicaciones electrónicas.
35. **La obligación de informar a los usuarios sobre los riesgos de seguridad tiene un alcance minimalista**. El Grupo de Trabajo acoge con satisfacción que los proveedores de servicios deban informar a los usuarios de los riesgos de seguridad y las medidas para hacer frente a tales riesgos, como por ejemplo el cifrado (artículo 17

²⁰ ECLI:EU:C:2016:970, URL: <http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203>.

y considerando 37). No obstante, el título de la disposición reza así: «Información sobre los riesgos de seguridad detectados». El hecho de que el título hable de riesgos detectados sugiere que esta disposición únicamente atañe a las (posibles) violaciones de la seguridad, mientras que la redacción de la disposición y el considerando apuntan, más bien, a la educación general de los usuarios finales. Por ejemplo, si un proveedor de servicios detecta que el dispositivo de un usuario está infectado con un programa malicioso y ha pasado a integrar una red zombi, esta disposición parece imponer directamente sobre el proveedor la obligación de informar al usuario de los riesgos resultantes. No obstante, el ámbito de esta disposición podría aclararse y no debería limitarse a esta hipótesis específica. Como mínimo, la disposición debería abarcar los riesgos de seguridad detectados en todos los equipos entregados al usuario final por el proveedor como parte de la suscripción, como por ejemplo enrutadores y dispositivos móviles, e incluir instrucción sobre los riesgos de modificar la configuración establecida para proteger la privacidad de acuerdo con el principio de privacidad desde el diseño.

El Grupo de Trabajo recomienda ampliar el ámbito de aplicación para incluir a los proveedores de programas informáticos que permiten comunicaciones electrónicas (véase el considerando 8) y, posiblemente, a una nueva categoría: proveedores de tecnología esencial para proteger las comunicaciones, que no son proveedores de servicios (p. ej. proveedores de tecnología de cifrado). En el caso de esta última ampliación, debe prestarse atención a que esta obligación no se solape con las obligaciones de notificación de violación de la seguridad contempladas en otros instrumentos como la Directiva sobre la seguridad de las redes y de la información²¹ y otros instrumentos jurídicos relativos a los proveedores de certificados. Puesto que esta última categoría de proveedores de tecnología normalmente no tienen un contacto directo con los usuarios finales, debe explicarse asimismo cómo pueden cumplir su obligación de información conforme a esta disposición.

36. El Grupo de Trabajo acoge con satisfacción las disposiciones de los artículos 2 y 13, que se aplicarán a servicios de comunicaciones interpersonales basados en números. Sin embargo, cuesta entender por qué **los servicios de llamadas OTT funcionalmente equivalentes no habrían de disponer de un nivel similar de protección de la privacidad.**
37. Asimismo, al Grupo de Trabajo le preocupa la **falta de claridad en cuanto al consentimiento pormenorizado en el caso de la búsqueda inversa en guías.** El artículo 15, apartado 2, de la propuesta de Reglamento obliga a los proveedores a obtener el consentimiento de los usuarios finales antes de habilitar funciones de búsqueda en relación con los datos (véase asimismo el considerando 31). El Grupo de Trabajo acoge con satisfacción la armonización del requisito de consentimiento por lo que respecta a la inclusión en guías, pero lamenta la falta de pormenorización en

²¹ Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016, p. 1-30), url: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SPA

relación con las distintos tipos de búsquedas. La actual Directiva sobre la privacidad y las comunicaciones electrónicas permite que los Estados miembros exijan un requisito de consentimiento independiente a efectos de la búsqueda inversa, sobre la base del artículo 12, apartado 3. Dicho artículo afirma que «[lo]s Estados miembros podrán exigir que para cualquier finalidad de una guía pública distinta de la búsqueda de datos de contacto de personas a partir de su nombre y, si resulta necesario, de un mínimo de otros identificadores, se recabe el consentimiento específico de los abonados». Sobre la base de esta disposición, en numerosos Estados miembros se requiere un consentimiento independiente para las funcionalidades de búsqueda inversa, teniendo en cuenta los distintos niveles de identificabilidad y, por ende, de capacidad de intrusión de las dos funcionalidades.

38. Otra cuestión, de carácter más formal, es que **el nivel de las multas no está armonizado para todas las infracciones del Reglamento**. En la propuesta de Reglamento, los Estados miembros establecerán normas sobre las sanciones aplicables a las infracciones de lo dispuesto en el artículo 23, apartados 4 y 6, y el artículo 24 de la propuesta de Reglamento. Lo más coherente sería disponer dichas normas también en el propio Reglamento sobre la privacidad y las comunicaciones electrónicas.
39. Por último, **la propuesta de Reglamento recurre a definiciones que pueden convertirse en «blancos móviles»**. En una serie de conceptos clave, la propuesta de Reglamento remite a otro instrumento jurídico que actualmente se encuentra en fase de proyecto: la propuesta de CECE [véase, por ejemplo, el artículo 4, apartado 1, letra b)]. Dos ejemplos destacados de este hecho son la definición de «usuario final», que actualmente comprende a las personas físicas y jurídicas, y las definiciones de «servicio de comunicaciones electrónicas» y «servicios de comunicaciones interpersonales», que se reflejan en la propuesta de Reglamento en su artículo 4, apartado 1, letra b) y, en el caso de la segunda definición detallada ulteriormente en el artículo 4, apartado 2, para incluir tipos de servicios excluidos específicamente en el CECE²². El presente Dictamen se fundamenta en el estado actual de las definiciones, aunque es bastante probable que la propuesta de CECE o sus conceptos clave cambien. Ello tendría implicaciones inmediatas también para el Reglamento sobre la privacidad y las comunicaciones electrónicas. Lo ideal es que todos los términos que proceden del CECE se definan independientemente en el Reglamento sobre la privacidad y las comunicaciones electrónicas; o, como mínimo, la propuesta de Reglamento debería incluir una aclaración cuando existan términos cuyas definiciones se desvíen de las contempladas en el CECE (p. ej., la inclusión, antes mencionada, de «servicios secundarios» en la definición de «servicio de comunicaciones interpersonales»). No obstante, si esto no fuese posible, el Grupo de Trabajo sugeriría a todas las partes involucradas en el proceso legislativo que velasen

²² Por ejemplo, el artículo 4, apartado 2, de la propuesta de Reglamento afirma que un servicio de comunicaciones electrónicas «englobará los servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio», mientras que el artículo 2, apartado 5, del CECE excluye expresamente este tipo de servicios de la definición. (El CECE incluye el «servicio de comunicaciones interpersonales» dentro de la categoría más amplia de «servicio de comunicaciones electrónicas» en su artículo 2, apartado 4).

por que tanto la propuesta de Reglamento como el CECE se debatieran y votaran simultáneamente, a fin de que todas las partes interesadas puedan evaluar correctamente el alcance y las implicaciones de los nuevos instrumentos.

5. SUGERENCIAS DE ACLARACIÓN PARA GARANTIZAR LA SEGURIDAD JURÍDICA

Además de los aspectos tratados anteriormente, el Grupo de Trabajo también desea destacar algunas disposiciones de la propuesta de Reglamento que se beneficiarían de una aclaración. Tales aclaraciones se consideran necesarias para mejorar la seguridad jurídica de todas las partes interesadas garantizando que el Reglamento sobre la privacidad y las comunicaciones electrónicas se interpretará y aplicará de manera uniforme en toda la UE.

ACLARACIONES SOBRE EL ÁMBITO DE APLICACIÓN

40. Con respecto al ámbito de aplicación de la propuesta de Reglamento, el Grupo de Trabajo sugiere las siguientes aclaraciones:

- a. **El término «usuario final» debería incluir a todos los usuarios particulares.** El artículo 2, apartado 14, del CECE define «usuario final» como el usuario que no suministra redes públicas de comunicaciones o servicios de comunicaciones electrónicas disponibles para el público. Debería aclararse que los particulares que contribuyan a redes —por ejemplo, a redes en malla con sus enrutadores inalámbricos— no están excluidos del alcance de la protección de la propuesta de Reglamento.
- b. **Debería aclararse que el ámbito de aplicación territorial es extensivo a todos los usuarios finales en la Unión.** El artículo 3, apartado 1, letra a), dispone que la propuesta de Reglamento es aplicable a la prestación de servicios de comunicaciones electrónicas a los usuarios finales «en la Unión», mientras que el artículo 3, apartado 1, letra c), dispone que es aplicable a la protección de los equipos terminales de los usuarios finales «situados en la Unión» (el énfasis es nuestro). Esta situación es variable en función de las diversas versiones lingüísticas; la versión alemana no hace esta distinción, mientras que otras, como la francesa, la española o la neerlandesa, sí. Del considerando 9 se desprende claramente que la intención es que el alcance sea amplio, independientemente de que los servicios se presten desde fuera de la Unión o el tratamiento se produzca en la Unión. Por consiguiente, se sugiere eliminar la palabra «situados» del artículo 3, apartado 1, letra c), a fin de hacer hincapié en este alcance amplio.
- c. **La propuesta de Reglamento únicamente parece proteger las comunicaciones confidenciales en «tránsito», y no cuando están «almacenadas».** El planteamiento actual de la propuesta de Reglamento es centrarse en la protección de la transmisión de las comunicaciones. Véase, por ejemplo, el considerando 15, que afirma que la prohibición de la interceptación de datos de comunicaciones ha de ser aplicable durante su transporte, es decir, hasta la recepción del contenido de la comunicación electrónica por el destinatario previsto. El alcance de esta protección se basa en un marco conceptual de las comunicaciones que ha quedado desfasado. La

mayor parte de los datos de comunicaciones permanecen almacenados en los proveedores del servicio, incluso después de la recepción. Debería garantizarse que la confidencialidad de dichos datos sigue estando protegida. Por otro lado, la comunicación entre abonados de los mismos servicios basados en la nube (por ejemplo, proveedores de correo web) frecuentemente solo implicará un transporte muy reducido: el envío de un correo implicaría, sobre todo, reflejar este hecho en la base de datos del proveedor, más que enviar realmente comunicaciones entre dos partes. El argumento de que esto ya estaría cubierto por el RGPD no resulta convincente: la finalidad global de la propuesta de Reglamento es proteger toda comunicación confidencial, independientemente de los medios técnicos de dicha comunicación. Cabe la posibilidad de que se trate de un mero error de redacción, puesto que la prohibición contemplada en el artículo 5 se refiere al «almacenamiento» y al «tratamiento».

- d. **Todos los puntos públicos de acceso inalámbrico a internet deberían estar incluidos en el ámbito de aplicación.** Puesto que el uso de puntos de acceso inalámbrico es común, es lógico que no haya duda alguna en cuanto a la protección de la confidencialidad de las comunicaciones transmitidas a través de dichos puntos de acceso inalámbricos. Sin embargo, el Reglamento fracasa en su intento de aclarar este aspecto, puesto que el ámbito de aplicación solo se extiende a las redes a disposición de un «grupo indefinido de usuarios finales» (considerando 13). Han de definirse los términos «grupo indefinido de usuarios finales» y «grupo cerrado de usuarios finales». En particular, debe aclararse que las redes inalámbricas seguras (es decir, con una contraseña) también están incluidas en el ámbito de aplicación, siempre que esta contraseña se facilite a un grupo de usuarios teóricamente indefinido cuya identidad no pueda determinarse de antemano (p. ej., clientes de una cafetería, visitantes de un aeropuerto). El principio subyacente en este contexto es que, en consonancia con el dictamen previo del Grupo de Trabajo sobre la revisión de la Directiva sobre la privacidad y las comunicaciones electrónicas, únicamente deberían estar exentos del instrumento sobre privacidad y comunicaciones electrónicas los servicios que se produzcan en una situación oficial o de trabajo y exclusivamente para fines laborales u oficiales, o la comunicación técnica entre organismos que no sean públicos u organismos públicos exclusivamente, a fin de controlar procesos de trabajo o empresariales, así como el uso de servicios con fines exclusivamente domésticos. (p. 8).
- e. **Los datos recopilados en el transcurso de una oferta de servicios digitales de radiodifusión deberían estar amparados por la propuesta de Reglamento.** Habida cuenta del carácter delicado de los hábitos de visualización, puesto que revelan características e intereses personales de los usuarios, el Reglamento sobre la privacidad y las comunicaciones electrónicas debería especificar (quizá mediante un considerando) que la exclusión de los servicios que suministren «contenidos transmitidos mediante redes [...] de comunicaciones electrónicas» de la definición de «servicio de comunicaciones electrónicas» no implica que los proveedores de servicios que ofrezcan tanto servicios de comunicaciones electrónicas como servicios de contenidos queden fuera del ámbito de aplicación de las disposiciones de

la propuesta de Reglamento dirigidas a los proveedores de servicios de comunicaciones electrónicas. Esto es de especial relevancia ya que la prestación de servicios que suministren «contenidos transmitidos mediante redes [...] de comunicaciones electrónicas» está excluida de la definición de «servicio de comunicaciones electrónicas» contemplada en la propuesta de CECE (artículo 2, apartado 4).

- f. **Por lo general, los datos de comunicaciones son datos personales.** En el considerando 4 se señala que los datos de comunicaciones pueden incluir datos personales. Sin embargo, la mayoría de los datos de comunicaciones son datos personales²³ y, en gran medida, datos de una naturaleza bastante íntima y sensible, por lo que debería modificarse para afirmar que generalmente los datos de comunicaciones son datos personales.
- g. **La comunicación confidencial incluye los mensajes dentro de plataformas.** El considerando 1 explica que el principio de confidencialidad se aplica a «los medios de comunicación actuales y futuros». El considerando enumera a continuación ejemplos de tales medios, entre los que se incluyen «los mensajes personales transmitidos a través de las redes sociales». Es probable que la finalidad de este ejemplo sea incluir los mensajes privados entre usuarios de una red social (p. ej., Facebook o Twitter) o los mensajes publicados en una cronología que sean accesibles para un número limitado de personas, pero la redacción no es lo suficientemente clara.
- h. **Cómo se aplica el Reglamento sobre la privacidad y las comunicaciones electrónicas a la interacción de máquina a máquina.** Como se mencionó en la observación 9, el Grupo de Trabajo acoge con satisfacción la ampliación de la protección a la interacción de máquina a máquina. Sin embargo, esto solo se menciona en el considerando 12 y no en un artículo correspondiente. Esta protección es conveniente, ya que frecuentemente este tipo de comunicaciones contiene información protegida por derechos de privacidad. Por otro lado, una categoría restringida de comunicación exclusiva de máquina a máquina debería estar exenta si esta no tiene repercusiones ni para la privacidad ni para la confidencialidad de las comunicaciones, como por ejemplo los casos en que dicha comunicación se produce durante la ejecución de un protocolo de transmisión entre componentes de una red (p. ej., servidores, conmutadores) para informar recíprocamente de su estado de actividad.

Un contexto específico en el que la aplicación de la propuesta de Reglamento requiere una aclaración es el ámbito de los sistemas de transporte inteligentes. Se prevé que los vehículos transmitirán por radiofrecuencia de manera ininterrumpida datos que contengan un identificador único. Sin la protección adicional en la propuesta de Reglamento respecto a los datos de comunicaciones, esto podría desembocar en un seguimiento continuado de

²³ Véase por ejemplo TJUE 6 de noviembre de 2003, C-101/01, apartado 4 (con respecto a un número de teléfono), TJUE 19 de octubre de 2016, C-582/14 (Breyer), apartado 49 (con respecto a las direcciones IP dinámicas) y CJUE 8 de abril de 2014, C-239/12 y C-594/12 (Digital Rights Ireland), apartados 26 y 27 (con respecto al carácter delicado de los metadatos).

los hábitos de conducción, los itinerarios y la velocidad de los conductores. No obstante, el artículo 2, apartado 1, del CECE contiene una definición nueva y ampliada de redes de comunicaciones. Estas incluyen los sistemas de transmisión que no cuentan con una capacidad de administración centralizada y que permiten el transporte de señales mediante ondas hertzianas. El considerando 14 de la propuesta de Reglamento especifica que dichos datos son datos de comunicaciones electrónicas. Con arreglo al artículo 5 de la propuesta de Reglamento, se prohíbe todo tipo de interceptación, seguimiento o almacenamiento de estos datos de comunicaciones, a menos que se aplique una de las excepciones. Con todo, reviste interés tratar estos datos que permiten a objetos, como automóviles autónomos y dispositivos, advertirse de su proximidad o de otros riesgos. La cuestión es, por tanto, qué excepción se aplicaría en este caso. El consentimiento de los usuarios finales no es una excepción viable, porque podría acabar siendo necesario poder tratar estos datos siempre. Por consiguiente, los proveedores deberían poder ampararse en una excepción específica que permita a objetos, como automóviles autónomos y dispositivos, advertirse de su proximidad o de otros riesgos.

ACLARACIONES EN CUANTO AL CONCEPTO Y LA APLICACIÓN DEL CONSENTIMIENTO

41. Por lo que respecta al concepto y la aplicación del consentimiento en la actual propuesta de Reglamento, el Grupo de Trabajo sugiere las siguientes aclaraciones:
 - a. **Cómo se aplicará el concepto de consentimiento en el contexto de las personas jurídicas.** El considerando 3 señala que el Reglamento debe garantizar que las disposiciones del RGPD también se aplican a los usuarios finales que sean personas jurídicas. Esto, según el considerando, incluye la definición de consentimiento contemplada en el RGPD (véase asimismo el considerando 18). Como ya se señaló en la observación 13, al Grupo de Trabajo le complace la inclusión explícita de las personas jurídicas en el ámbito de aplicación del Reglamento, aunque no queda claro cómo se va a aplicar este principio en la práctica. La definición de consentimiento contemplada en el RGPD requiere que este sea «informado» y que la voluntad del interesado se manifieste «mediante una declaración o una clara acción afirmativa» (artículo 4, apartado 11, del RGPD). Debe aclararse cuándo puede considerarse de hecho que una persona jurídica está «informada» y cuándo hay una manifestación de tal voluntad por parte de una persona jurídica.
 - b. En este contexto, cabe señalar que un empleador, en la mayoría de las circunstancias, no puede dar su consentimiento en nombre de sus empleados porque cuando un empleador requiere el consentimiento de un empleado, y dado el equilibrio desigual de poder, existe un perjuicio real o potencial derivado de no dar el consentimiento: tal consentimiento no es válido porque

no se da libremente²⁴. En relación con las **empresas que entregan dispositivos o equipos apersonas, la propuesta de Reglamento no incluye una excepción (adecuada)** a la prohibición de interferencia. Un ejemplo de ello es cuando un empleador desea actualizar un teléfono de empresa. Otro ejemplo es cuando un empleador ofrece a los empleados automóviles arrendados y a efectos administrativos permite que un tercero recoja datos sobre la localización a través de la unidad de a bordo del automóvil. En ambos casos el empleador tiene interés en interferir en dichos dispositivos.

La interferencia no puede considerarse necesaria para la prestación de un servicio de la sociedad de la información [artículo 8, apartado 1, letra c)] ni necesaria para medir la audiencia en la web [artículo 8, apartado 1, letra d)]. Esta situación podría resolverse creando una nueva excepción para incluir las circunstancias en que i) el empleador entregue determinados equipos en el contexto de una relación laboral; ii) el empleado sea el usuario de dichos equipos; y iii) la interferencia sea estrictamente necesaria para que el empleado haga funcionar los equipos (lo que implica la aplicación de los principios de proporcionalidad y subsidiariedad por lo que respecta a la recogida de datos). El empleador solo podría interferir con el dispositivo de los usuarios finales cuando se cumpliesen estas condiciones.

- c. **Mejora de los controles para detener las llamadas desviadas automáticamente.** El artículo 14 ofrece un control importante para que los usuarios finales detengan el desvío automático de llamadas por un tercero. Esta protección puede mejorarse aún más requiriendo también el consentimiento del usuario final para iniciar el desvío de llamadas en primer lugar.

ACLARACIONES EN CUANTO A LA LOCALIZACIÓN Y OTROS METADATOS

- 42. El Grupo de Trabajo sugiere aclarar los siguientes puntos por lo que respecta a los datos de localización y otros metadatos:

- a. El significado de «**datos de localización que se generen en un contexto distinto al de la prestación de servicios de comunicaciones electrónicas**», **dentro del considerando 17, debería aclararse.** No queda claro si esto se refiere a los datos de localización recogidos a través de, por ejemplo, aplicaciones que utilizan los datos de la funcionalidad GPS de los dispositivos inteligentes y/o generan datos de localización a partir de enrutadores inalámbricos cercanos, o a los datos de localización recogidos mediante asistentes de navegación de abordó u otras formas de generar datos de localización. Esta falta de claridad crea inseguridad jurídica en cuanto al alcance de la obligación. En cualquier caso, los datos de localización del equipo terminal de una persona física se consideran datos personales y, por ende, el tratamiento de dichos datos está sujeto a las obligaciones del RGPD.

²⁴ Véase el Dictamen 15/2011 sobre la definición de consentimiento (WP 187), el Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral (WP48) y el nuevo Dictamen sobre el tratamiento de datos en el trabajo (adoptado al mismo tiempo que el presente Dictamen).

- b. Debería aclararse que **la mayor parte del tratamiento lícito de datos de localización y otros metadatos no requiere un identificador único**. El considerando 17 menciona los mapas térmicos como ejemplo de usos comerciales de metadatos de comunicaciones electrónicas por parte de los proveedores de servicios de comunicaciones electrónicas. No obstante, para crear un mapa térmico básico no hacen falta identificadores únicos, basta con un simple recuento estadístico. Otro ejemplo mencionado en el considerando, el uso de las estructuras y la presión ejercida sobre ellas, también puede registrarse mediante determinados puntos de medición, por ejemplo creando estadísticas agregadas sobre el uso de torres de control del tráfico para obtener una estimación de la presión sobre una ubicación en un momento dado, sin que sea necesario conocer también la identidad de las personas conectadas.

Además, el considerando menciona como ejemplo mostrar los movimientos del tráfico en ciertas direcciones durante un determinado período de tiempo, para lo cual sería necesario un identificador único que relacione las posiciones de las personas en determinados intervalos de tiempo. Con este ejemplo, el considerando parece legitimar el tratamiento ulterior de estos datos en apoyo de los análisis de «macrodatos». La única condición con arreglo a la propuesta de Reglamento para este tipo de tratamiento es la obligación de llevar a cabo una evaluación de impacto relativa a la protección de datos cuando «sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas». Esta condición resulta insuficiente. Por otro lado, contraviene la obligación recogida en el artículo 6 de que este tipo de tratamiento solo podrá efectuarse con el consentimiento de los usuarios, y únicamente si los datos no pueden anonimizarse, es decir, sin ningún tipo de identificador único. Frecuentemente los usuarios no pueden negarse a que los proveedores de servicios de comunicaciones electrónicas recopilen los datos de su geolocalización, cuando dicha recopilación es técnicamente necesaria para transmitir la comunicación al usuario o cuando dicho tratamiento es necesario para prestar el servicio solicitado (p. ej., navegación). En dictámenes previos, el Grupo de Trabajo ha concluido que los datos de localización de este tipo de dispositivos inteligentes son datos personales de naturaleza sensible, y que los beneficios de analizar estos datos no prevalecen sobre los derechos de los usuarios a la protección de la confidencialidad de los metadatos de sus comunicaciones, ni tampoco prevalecen sobre sus derechos generales a la protección de datos al amparo del RGPD. Por consiguiente, el considerando debe, como mínimo, especificar que los proveedores deben cumplir las obligaciones que se desprenden del artículo 25 del RGPD en caso de tratamiento ulterior de los datos de localización u otros metadatos. Esto implica que, como mínimo, han de adoptarse las siguientes medidas:

- i) el uso de seudónimos temporales;
- ii) la eliminación de toda tabla de búsqueda inversa entre estos seudónimos y los datos de identificación originales;
- iii) la agregación hasta un nivel tal que los usuarios individuales ya no puedan ser identificados a través de sus itinerarios específicos; y

iv) la eliminación de valores atípicos con respecto a los cuales la identificación seguiría siendo posible (todas estas medidas han de aplicarse a la vez).

Por último, el Reglamento sobre la privacidad y las comunicaciones electrónicas debe obligar a las partes que participen en el tratamiento de los datos de localización y otros metadatos a que hagan públicos sus métodos de anonimización y agregación ulterior, sin perjuicio de la confidencialidad salvaguardada por la legislación. Así sería posible que tanto las autoridades de control como el público en general verificasen fácilmente si el método elegido es apropiado.

ACLARACIONES CON RESPECTO A LAS COMUNICACIONES NO SOLICITADAS

43. El Grupo de Trabajo sugiere aclarar los siguientes puntos por lo que respecta a las comunicaciones no solicitadas:

- a. **La formulación de la prohibición de la mercadotecnia directa sin consentimiento.** Actualmente, el artículo 16, apartado 1, de la propuesta de Reglamento señala que los servicios de comunicaciones electrónicas «podrán» utilizarse para el envío de comunicaciones de mercadotecnia directa (con consentimiento), pero no contiene explícitamente la prohibición de enviar (dirigir o presentar) mercadotecnia directa sin consentimiento. Esta situación contrasta con el planteamiento de otras disposiciones, en las que primero se formula una prohibición para a continuación enumerar determinadas excepciones específicas. La redacción actual sugiere un planteamiento más permisivo (que seguramente no sea el que se pretende). El Grupo de Trabajo sugiere modificar ligeramente la redacción del actual artículo 13, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas: «la utilización por parte de personas físicas o jurídicas de servicios de comunicaciones electrónicas, incluidas llamadas de voz a voz, sistemas de llamada automática y comunicación, incluidos los sistemas semiautomáticos que conectan a la persona que recibe la llamada con otra persona, fax, correo electrónico u otro uso de servicios de comunicaciones electrónicas con fines de presentar comunicaciones de venta directa a usuarios finales solo se podrá autorizar respecto de aquellos usuarios finales que hayan dado su consentimiento previo».
- b. **El alcance de las disposiciones sobre las comunicaciones y llamadas de mercadotecnia a los contactos existentes.** El artículo 16, apartado 2, prevé que cuando una persona obtenga la dirección de correo electrónico de un cliente existente, esta podrá utilizar esos datos de contacto para la comercialización directa ulterior de sus propios productos y servicios cuando ofrezca de manera clara la oportunidad de oponerse de manera sencilla y gratuita en el momento de la recopilación y cada vez que se envíe un mensaje. Este supuesto se limita actualmente a los contactos comerciales obtenidos «en el contexto de la venta de un producto o servicio» y para una comercialización ulterior de sus propios productos o servicios similares. Habida cuenta de que las disposiciones sobre la mercadotecnia directa se

aplican igualmente a las actividades promocionales sin fines comerciales (p. ej., de asociaciones benéficas o partidos políticos), esta disposición debería modificarse para que fuese igualmente de aplicación a las organizaciones sin fines comerciales que contacten a simpatizantes previos cuando promuevan sus propios objetivos o ideales similares y el mismo derecho de oposición debería aplicarse a las llamadas de mercadotecnia directa. Por otro lado, debería fijarse un plazo de validez de los «contactos de clientes existentes» en las comunicaciones electrónicas con fines comerciales, políticos o de beneficencia, y este plazo debería aplicarse también a las llamadas de mercadotecnia directa. Cuando los Estados miembros hayan optado por un sistema de oposición a las llamadas de mercadotecnia de voz a voz, la existencia de una relación de «contacto de cliente existente» invalidará la inscripción en una Lista Robinson. En tales circunstancias, los usuarios finales no disponen de una opción efectiva para evitar las llamadas molestas de empresas u organizaciones con las que hayan entrado en contacto alguna vez pero con las que ya no deseen mantener una relación. Por consiguiente, como norma general, el Reglamento debería especificar una validez para esta excepción del «cliente existente», por ejemplo uno o dos años, en relación con las expectativas legítimas de los usuarios finales afectados.

- c. **La aplicación de las normas sobre mercadotecnia directa a las personas jurídicas.** El artículo 16, apartado 5, de la propuesta de Reglamento prevé que los Estados miembros velarán por que el interés legítimo de los usuarios finales que sean personas jurídicas esté suficientemente protegido en lo que se refiere a las comunicaciones no solicitadas. El artículo 13, apartado 5, de la Directiva sobre la privacidad y las comunicaciones electrónicas en vigor describe los intereses legítimos de los abonados distintos de las personas físicas. No quedan claras las implicaciones de esta modificación de la redacción. Debería aclararse en los considerandos que esta modificación no es reflejo de la intención de ofrecer un nivel de protección menor. En relación con este aspecto, la prohibición en materia de mercadotecnia directa sin consentimiento atañe a «los usuarios finales que sean personas físicas y hayan dado su consentimiento» (el énfasis es nuestro). Debería aclararse que también se incluyen las personas físicas «que trabajen para» personas jurídicas. Por otro lado, no se requeriría consentimiento para ponerse en contacto con personas jurídicas a través de información de contacto genérica que hayan hecho pública a tales efectos (p. ej., «info@companyname.eu»).
- d. **La aplicación de las normas sobre mercadotecnia directa a aquellos que actúan en calidad de representante (político):** tal como está redactado, el artículo 16 podría impedir que se envíen a representantes electos ciertas comunicaciones en las que se esbocen inquietudes o intereses comerciales. Debería aclararse que el Reglamento no impide este tipo de comunicaciones.

44. Debería aclararse en más detalle **la aplicación de la Carta y el CEDH a la legislación nacional de conservación de datos**. El considerando 26 contempla que cualquier medida tomada por los Estados miembros para proteger el interés público, como las medidas legales de interceptación, ha de ser conforme con la Carta (además de con el CEDH), lo que resulta conveniente, ya que se ajusta al razonamiento en Tele2/Watson de que cualquier excepción nacional a las protecciones en materia de tratamiento de datos del Derecho de la UE está supeditada a la Carta (y las infracciones a través de las legislaciones nacionales pueden, por tanto, llevarse ante el Tribunal de Justicia de la UE). Sin embargo, el artículo 11 de la propuesta de Reglamento simplemente señala que las limitaciones del ámbito de aplicación de los artículos 5 a 8 de la propuesta de Reglamento deben respetar en lo esencial los derechos y libertades fundamentales y ser una medida necesaria y proporcionada. También debería incluirse una referencia explícita a la Carta y al CEDH en este punto.
45. **El hecho de que la confidencialidad de las comunicaciones también está protegida en virtud del artículo 8 del CEDH**. En el apartado 1.1 de la exposición de motivos, así como en el considerando 1, se explica que la propuesta de Reglamento aplica el artículo 7 de la Carta. Este hecho se repite en el considerando 19. Sin embargo, el derecho fundamental a las comunicaciones confidenciales no solo está protegido en la disposición citada, sino también por el artículo 8 del CEDH. La inclusión de una referencia explícita en uno de los artículos de la propuesta de Reglamento vendría a confirmar asimismo que cualquier jurisprudencia pertinente del Tribunal Europeo de Derechos Humanos habrá de tenerse en cuenta también a la hora de evaluar el Reglamento (final). Referencia que, por cierto, ya se incluye en los considerandos 20 (en relación con los equipos terminales) y 26 (en relación con la interceptación ilícita), y se respalda asimismo en las consideraciones del apartado 2.1 de la exposición de motivos (sobre la relación entre la Carta y el CEDH en el contexto de las personas jurídicas), pero no en ninguno de los artículos pertinentes, como el artículo 11, apartado 1.

OTRAS ACLARACIONES

46. Debería aclararse que **las obligaciones con arreglo al RGPD, como por ejemplo en relación con el régimen aplicable a la violación de la seguridad de los datos y la evaluación de impacto relativa a la protección de datos, siguen siendo de aplicación** cuando las partes traten datos personales en el contexto de los datos de comunicaciones electrónicas. Ya que se menciona en el considerando 5 que la propuesta de Reglamento constituye una *lex specialis* en relación con el RGPD y que el tratamiento de datos de comunicaciones electrónicas solo debe permitirse con arreglo a la propuesta de Reglamento, cabría preguntarse si determinadas obligaciones contempladas en el RGPD también se aplican en el contexto de la propuesta de Reglamento. Esto es así especialmente cuando podría interpretarse que la propuesta de Reglamento dispone determinada obligación también cubierta por el RGPD. He aquí algunos ejemplos ilustrativos:
- i) la propuesta de Reglamento obliga a notificar determinados riesgos de seguridad «detectados» (artículo 17) (véase asimismo la observación 35),

pero el RGPD incluye un régimen de notificación de las violaciones de la seguridad de los datos (artículos 33 y 34);

- ii) la propuesta de Reglamento menciona que la realización de una EIPD y la consulta con la autoridad de control en consonancia con el RGPD son obligatorias en determinadas circunstancias [considerandos 17 y 19; y artículo 6, apartado 3, letra b)], al tiempo que el RGPD ya establece cuándo ha de realizarse una EIPD y cuándo se requiere la consulta (artículos 5 y 36); y
- iii) no se menciona expresamente que, aunque se cumplan las condiciones necesarias de una excepción a la prohibición de tratamiento con arreglo al artículo 5 de la propuesta de Reglamento, sigue siendo necesario cumplir todas las obligaciones pertinentes recogidas en el RGPD por lo que respecta al tratamiento de datos personales y se prohíbe cualquier otro tratamiento con arreglo al RGPD. Debería aclararse que, por consiguiente, la prueba de compatibilidad establecida en el artículo 6, apartado 4, del RGPD no es de aplicación.
- iv) La propuesta de Reglamento no prevé mecanismos de certificación similares a los contemplados en los artículos 42 y 43 del RGPD. Puesto que el ámbito de aplicación del artículo 42 del RGPD se limita, en sentido estricto, a la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el RGPD, debería examinarse la pertinencia de introducir una disposición comparable para permitir la certificación de la conformidad de operaciones de tratamiento, normas, productos o servicios con el Reglamento sobre la privacidad y las comunicaciones electrónicas.

Para garantizar que esta falta de claridad no se utilice como argumento para disminuir el nivel de protección otorgado por la propuesta de Reglamento, debería dejarse claro que los responsables del tratamiento también deben cumplir el RGPD en todos los casos.

- 47. Por otro lado, debería aclararse que **el requisito para la retirada del consentimiento también se aplica en el contexto de la interferencia en equipos terminales**. El artículo 8, apartado 1, letra b), de la propuesta de Reglamento prevé la posibilidad de interferir en los equipos terminales de los usuarios finales cuando estos hayan dado su consentimiento. El artículo 9, apartado 3, exige que se ofrezca a los usuarios finales la posibilidad de retirar su consentimiento en cualquier momento, pero esto solo se aplica al consentimiento para el análisis de los metadatos y el contenido. Debería aclararse que esta obligación es extensiva a la interferencia en los equipos terminales.
- 48. En relación con esta cuestión, debería aclararse que **el recordatorio de la posibilidad de retirar el consentimiento también se aplica al consentimiento dado a través de la configuración del navegador**. El artículo 9, apartado 3, exige que se recuerde a los usuarios finales la posibilidad de retirar su consentimiento en cualquier momento a intervalos regulares de seis meses. Aunque el Grupo de Trabajo cree que la configuración general de los navegadores y demás programas informáticos, como los sistemas operativos, las aplicaciones y las interfaces informáticas para los dispositivos conectados a la internet de las cosas (es decir, sin partir de controles pormenorizados específicos) no pueden constituir una medida válida para dar el

consentimiento, ya que la configuración general no es apropiada para dar consentimiento específico ante una situación específica (véase la observación 24), los ajustes por defecto deberían ser intuitivos (véase la observación 19). Si esto se mantiene en la propuesta de Reglamento, las configuraciones deben ser lo suficientemente pormenorizadas como para controlar todo tratamiento de datos que el usuario consienta y abarcar cada una de las funcionalidades del equipo que pueda traducirse en un tratamiento de datos. Por otro lado, el usuario final debería recibir un recordatorio de la posibilidad de cambiar estos ajustes como mínimo a intervalos regulares de seis meses.

49. Es bien recibido que la propuesta de Reglamento exija que los programas informáticos ya comercializados informen al usuario final de sus opciones de configuración de confidencialidad (artículo 10). **No obstante, no queda claro cómo aplicar efectivamente este aspecto a los productos antiguos** y a otros que ya no son compatibles. Además, debería aclararse cómo se va a aplicar esta obligación en el caso de los programas informáticos de código abierto que se desarrollan de manera abierta y descentralizada.
50. Debería aclararse que **el ofrecimiento de la posibilidad de bloquear las cookies (de terceros) con arreglo al artículo 10 de la propuesta de Reglamento prevalece sobre la excepción para la medición de la audiencia en web** del artículo 8, apartado 1, letra d). En otras palabras: aunque un sitio web pueda emplear métodos analíticos para la medición de la audiencia en la web con arreglo al artículo 8, apartado 1, letra d), los usuarios deberían seguir teniendo el derecho de bloquear tales tecnologías de seguimiento en su navegador.
51. La **definición de sistemas (semi)automatizados de llamada y comunicación debería aclararse**. La definición de este término en el artículo 4, apartado 3, letra h), de la propuesta de Reglamento contiene una referencia al propio término en la segunda parte de la frase («incluidas las llamadas efectuadas mediante sistemas automatizados de llamada y comunicación que conectan a la persona llamada a otra persona»). Se sugiere eliminar esta última frase de la definición y modificar la definición del artículo 4, apartado 3, letra g), para incluir las llamadas efectuadas con la ayuda de sistemas de comunicación semiautomatizados, como por ejemplo marcadores automáticos, que conectan a la persona llamada a otra persona.
52. **Debería aclararse la información que «forma parte de la suscripción a un servicio»**. En el considerando 14 se menciona que los metadatos de comunicaciones electrónicas «pueden incluir información que forme parte de la suscripción al servicio cuando esa información se trata para transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas». No queda clara cuál es la intención de esta formulación.
53. Debería aclararse **la aplicabilidad de los mecanismos de coherencia y cooperación**. En el considerando 38 se señala que la propuesta de Reglamento se basa en el mecanismo de coherencia del RGPD. Además, el artículo 18, apartado 1, prevé que los capítulos VI y VII del RGPD serán de aplicación *mutatis mutandis*. En el artículo 19 se señala asimismo que el Comité Europeo de Protección de Datos («CEPD»)

ejercerá las funciones previstas en el artículo 70 del RGPD. Aunque la aplicación de estas disposiciones está relativamente clara, no puede descartarse que surjan cuestiones de interpretación con respecto a los conceptos clave de los mecanismos de coherencia y cooperación del RGPD. Por ejemplo, el mecanismo de la autoridad principal se aplica a aquellos casos en que exista «tratamiento transfronterizo» (artículo 56, apartado 1, del RGPD): no queda claro cómo se aplica en caso de interferencia de equipos terminales o análisis de contenido o metadatos con arreglo a la propuesta de Reglamento. Por ello, conviene aclarar la aplicación de estos conceptos clave en un considerando y hacer hincapié en que cualquier cuestión pendiente en cuanto a la aplicabilidad de dichos capítulos del RGPD, en el contexto de la propuesta de Reglamento, se resolverá interpretando las disposiciones de estos capítulos en consonancia con su intención. Por otro lado, resultaría recomendable aclarar que el artículo 70 se aplica *mutatis mutandis* al Comité Europeo de Protección de Datos en el contexto de la propuesta de Reglamento (aspecto que actualmente no figura en el considerando).

* * *