Consejo de la Unión Europea

Bruselas, 16 de enero de 2017
(OR. en)

5358/17

Expediente interinstitucional: 2017/0003 (COD)

TELECOM 12
COMPET 32
MI 45
DATAPROTECT 4
CONSOM 19
JAI 40
DIGIT 10
FREMP 3
CYBER 10
IA 12
CODEC 52

PROPUESTA

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	12 de enero de 2017
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2017) 10 final
Asunto:	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)

Adjunto se remite a las Delegaciones el documento – COM(2017) 10 final.

Adj.: COM(2017) 10 final

COMISIÓN
EUROPEA

Bruselas, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

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)

(Texto pertinente a efectos del EEE)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

EXPOSICIÓN DE MOTIVOS

1. CONTEXTO DE LA PROPUESTA

1.1. Razones y objetivos de la propuesta

Uno de los objetivos de la Estrategia para el Mercado Único Digital (en lo sucesivo, «**Estrategia MUD** »)[1] es aumentar la seguridad de los servicios digitales y la confianza que los ciudadanos depositan en ellos. Un paso esencial en este sentido lo constituyó la reforma del marco de protección de datos, y en particular la adopción del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en lo sucesivo, «**RGPD**»)[2]. La Estrategia MUD también anunciaba la revisión de la Directiva 2002/58/CE (en lo sucesivo, «**Directiva sobre privacidad y comunicaciones electrónicas**»)[3] con el fin de garantizar un elevado nivel de protección de la intimidad a los usuarios de servicios de comunicaciones electrónicas y condiciones de competencia equitativas para todos los agentes del mercado. La presente propuesta revisa la Directiva sobre privacidad y comunicaciones electrónicas, abundando en los objetivos de la Estrategia MUD y velando por la coherencia con el RGPD.

La Directiva sobre privacidad y comunicaciones electrónicas garantiza la protección de los derechos y libertades fundamentales, en particular el respeto de la vida privada, la confidencialidad de las comunicaciones y la protección de los datos personales en el sector de las comunicaciones electrónicas. También garantiza la libre circulación de datos, equipos y servicios de comunicaciones electrónicas en la Unión. Incorpora en el Derecho derivado de la Unión el derecho fundamental al respeto de la vida privada en el sector de las comunicaciones, establecido en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «**la Carta**»).

En consonancia con los requisitos de la estrategia «Legislar mejor», la Comisión efectuó una evaluación *a posteriori* en el marco del programa de adecuación y eficacia de la reglamentación (conocido por su sigla en inglés «**REFIT**») de la Directiva sobre privacidad y comunicaciones electrónicas. De la evaluación se desprende que los objetivos y principios del marco actual siguen siendo válidos. Con todo, desde la última revisión de dicha Directiva en 2009 se han producido en el mercado importantes cambios de índole tecnológica y económica. Los consumidores y las empresas recurren cada vez más a los nuevos servicios basados en Internet que hacen posibles comunicaciones interpersonales tales como servicios de voz sobre IP, servicios de mensajería instantánea y servicios de correo electrónico basados en la web, en lugar de utilizar los servicios de comunicación tradicionales. Por lo general, estos servicios de transmisión libre (denominados en inglés «*Over-the-Top*» y conocidos por su sigla en inglés «**OTT**») no están regulados por el marco vigente de las comunicaciones

---

1 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Una Estrategia para el Mercado Único Digital de Europa* [COM(2015) 192 final].

2 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, pp. 1-88).

3 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, p. 37).

electrónicas de la Unión, en particular por la Directiva sobre privacidad y comunicaciones electrónicas. Dicha Directiva no ha seguido, pues, el ritmo de la evolución tecnológica, por lo que las comunicaciones transmitidas a través de los nuevos servicios están desprovistas de protección.

1.2. Coherencia con las disposiciones existentes en la misma política sectorial

La presente propuesta 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. Todas las cuestiones relacionadas con el tratamiento de datos personales que no se contemplan específicamente en la propuesta quedan amparadas por el RGPD. La adaptación al RGPD ha obligado a derogar algunas disposiciones, como las obligaciones de seguridad establecidas en el artículo 4 de la Directiva sobre privacidad y comunicaciones electrónicas.

1.3. Coherencia con otras políticas de la Unión

La Directiva sobre privacidad y comunicaciones electrónicas forma parte del marco regulador de las comunicaciones electrónicas. En 2016, la Comisión adoptó una propuesta de Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas (en lo sucesivo, «**CECE**»)[4], que revisa ese marco. Aun cuando no forme parte integrante del CECE, la presente propuesta se basa en parte en las definiciones que en él figuran, entre ellas la de «servicios de comunicaciones electrónicas». Al igual que el CECE, esta propuesta también incluye a los proveedores OTT en su ámbito de aplicación a fin de reflejar la realidad del mercado. Además, el CECE complementa la presente propuesta garantizando la seguridad de los servicios de comunicaciones electrónicas.

La Directiva 2014/53/UE sobre equipos radioeléctricos[5] garantiza un mercado único para dichos equipos. Establece, en particular, que, antes de ser comercializados, los equipos radioeléctricos han de incorporar salvaguardias para garantizar la protección de la intimidad y los datos personales del usuario. En virtud de la Directiva sobre equipos radioeléctricos y del Reglamento (UE) n.º 1025/2012[6] sobre la normalización europea, la Comisión está facultada para adoptar medidas. La presente propuesta no afecta a la Directiva sobre equipos radioeléctricos.

La propuesta no contiene disposiciones específicas en materia de conservación de datos. Mantiene el contenido del artículo 15 de la Directiva sobre privacidad y comunicaciones electrónicas y lo adapta a la formulación específica del artículo 23 del RGPD, que permite a los Estados miembros restringir el alcance de los derechos y obligaciones en artículos

---

4 Propuesta de la Comisión relativa a una Directiva del Parlamento Europeo y del Consejo por la que se establece el Código Europeo de las Comunicaciones Electrónicas (refundición) [COM/2016/0590 final - 2016/0288 (COD)].

5 Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE (DO L 153 de 22.5.2014, pp. 62-106).

6 Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión n.º 1673/2006/CE del Parlamento Europeo y del Consejo (DO L 316 de 14.11.2012, pp. 12-33).

específicos de la Directiva sobre privacidad y comunicaciones electrónicas. Por consiguiente, los Estados miembros pueden mantener o crear marcos nacionales de conservación de datos que prevean, en particular, medidas de conservación específicas, siempre y cuando tales marcos sean conformes al Derecho de la Unión, habida cuenta de la jurisprudencia del Tribunal de Justicia sobre la interpretación de la Directiva sobre privacidad y comunicaciones electrónicas y de la Carta de los Derechos Fundamentales[7].

Por último, la propuesta no es aplicable a las actividades de las instituciones, órganos y organismos de la Unión. No obstante, sus principios y obligaciones pertinentes en cuanto al derecho al respeto de la vida privada y las comunicaciones en relación con el tratamiento de datos de comunicaciones electrónicas se han incluido en la propuesta de Reglamento por el que se deroga el Reglamento (CE) n.º 45/2001[8].

2. BASE JURÍDICA, SUBSIDIARIEDAD Y PROPORCIONALIDAD

2.1. Base jurídica

El artículo 16 y el artículo 114 del Tratado de Funcionamiento de la Unión Europea (en lo sucesivo, «**TFUE**») constituyen las bases jurídicas pertinentes de la propuesta.

El artículo 16 del TFUE establece una base jurídica específica para la adopción de normas sobre la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por las instituciones de la Unión y por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. Dado que, en general, se considera que los datos de una comunicación electrónica en que interviene una persona física constituyen datos personales, la protección de las personas físicas en lo que respecta a la privacidad de las comunicaciones y el tratamiento de tales datos debe basarse en el artículo 16.

La propuesta aspira, además, a proteger las comunicaciones y los intereses legítimos correspondientes de las personas jurídicas. De conformidad con el artículo 52, apartado 3, de la Carta, el sentido y el alcance de los derechos conferidos por su artículo 7 han de ser iguales a los establecidos en el artículo 8, apartado 1, del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en lo sucesivo, «**CEDH**»). Por lo que se refiere al alcance del artículo 7 de la Carta, la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «**TJUE**»)[9] y del Tribunal Europeo de Derechos Humanos[10] confirma que las actividades profesionales de las personas jurídicas no pueden quedar

---

7 Véanse asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y otros*, ECLI:EU:C:2014:238; asuntos acumulados C-203/15 y C-698/15, *Tele2 Sverige AB y Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

8 Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, pp. 1-22).

9 Véase el asunto C-450/06, *Varec SA*, ECLI:EU:C:2008:91, apartado 48.

10 Véanse, en particular, las sentencias del Tribunal Europeo de Derechos Humanos (TEDH), en los asuntos *Niemietz/Alemania*, de 16 de diciembre de 1992, serie A, n.º 251-B, apartado 29; *Société Colas Est y otros/Francia*, n.º 37971/97, apartado 41; TEDH 2002-III; *Peck/Reino Unido*, nº 44647/98, apartado 57, TEDH 2003-I; y también *Vinci Construction y GTM Génie Civil et Services/Francia*, n.os 63629/10 y 60567/10, apartado 63, 2 de abril de 2015.

excluidas de la protección de derechos garantizada por el artículo 7 de la Carta y el artículo 8 del CEDH.

Dado que la iniciativa persigue un doble objetivo y que el componente relativo a la protección de las comunicaciones de las personas jurídicas y el objetivo de implantar el mercado interior de esas comunicaciones electrónicas y garantizar su funcionamiento a este respecto no pueden considerarse meramente accesorios, la iniciativa debe, por tanto, basarse también en el artículo 114 del TFUE.

2.2. Subsidiariedad

El respeto de las comunicaciones es un derecho fundamental reconocido en la Carta. El contenido de las comunicaciones electrónicas puede desvelar información muy delicada acerca de los usuarios finales que intervienen en ellas. Del mismo modo, los metadatos derivados de las comunicaciones electrónicas pueden también revelar información muy delicada y de carácter personal, como reconoció expresamente el TJUE[11]. La mayoría de los Estados miembros reconoce también la necesidad de que la protección de las comunicaciones constituya un derecho constitucional diferenciado. Los Estados miembros podrían adoptar políticas que garantizaran el respeto de ese derecho, si bien este objetivo no se alcanzaría de manera uniforme a falta de normas de la Unión y se crearían restricciones de los flujos transfronterizos de datos personales y no personales relacionados con la utilización de los servicios de comunicaciones electrónicas. Por último, para mantener la coherencia con el RGPD, es necesario revisar la Directiva sobre privacidad y comunicaciones electrónicas y adoptar medidas para armonizar ambos instrumentos.

Los avances tecnológicos y las ambiciones de la Estrategia MUD han reafirmado la necesidad de actuar a escala de la Unión. El éxito de la Estrategia MUD de la UE depende del grado en que la UE logre eliminar los compartimentos y barreras nacionales para aprovechar las ventajas y las economías que comporta un mercado único digital europeo. Por otra parte, dado que Internet y las tecnologías digitales no conocen fronteras, la dimensión del problema va más allá del territorio de un solo Estado miembro. En la situación actual, los Estados miembros no pueden resolver eficazmente los problemas. El correcto funcionamiento del mercado único digital requiere condiciones de competencia justas para los operadores económicos que prestan servicios sustituibles y una protección equitativa de los usuarios finales a escala de la Unión.

2.3. Proporcionalidad

Para garantizar la protección jurídica efectiva del respeto de la privacidad y las comunicaciones, es preciso ampliar el ámbito de aplicación a los proveedores de servicios OTT. Aunque varios proveedores populares de servicios OTT cumplan ya total o parcialmente el principio de confidencialidad de las comunicaciones, la autorregulación por parte del sector no basta para garantizar la protección de los derechos fundamentales. Asimismo, cobra cada vez mayor importancia la protección efectiva de la privacidad de los equipos terminales, que actualmente son indispensables en la vida personal y profesional para el almacenamiento de información delicada. La aplicación de la Directiva sobre privacidad y comunicaciones electrónicas no ha resultado eficaz para capacitar a los usuarios finales en este ámbito. Por consiguiente, a fin de alcanzar ese objetivo, es necesario aplicar el principio centralizando el consentimiento en los programas informáticos y facilitando a los usuarios

[11] Véase la nota a pie de página n.º 7.

información sobre las opciones de privacidad que ofrecen. En la aplicación del presente Reglamento desempeñarán un papel esencial las autoridades de control y el mecanismo de coherencia del RGPD. Además, la propuesta permite a los Estados miembros implantar excepciones nacionales para determinados fines legítimos. Así pues, la propuesta no va más allá de lo necesario para alcanzar sus objetivos y respeta el principio de proporcionalidad enunciado en el artículo 5 del Tratado de la Unión Europea. Las obligaciones impuestas a los servicios afectados se mantienen en el nivel más bajo posible, sin vulnerar los derechos fundamentales considerados.

2.4. Elección del instrumento

La Comisión presenta una propuesta de Reglamento a fin de garantizar la coherencia con el RGPD y ofrecer seguridad jurídica a usuarios y empresas evitando interpretaciones divergentes en los Estados miembros. Un Reglamento puede garantizar un nivel uniforme de protección de los usuarios en toda la Unión y abaratar los costes de conformidad de las empresas que desarrollan actividades transfronterizas.

3. RESULTADOS DE LAS EVALUACIONES *EX POST*, DE LAS CONSULTAS CON LAS PARTES INTERESADAS Y DE LAS EVALUACIONES DE IMPACTO

3.1. Evaluaciones *ex post* / control de calidad de la legislación existente

En la evaluación REFIT se examinó si la Directiva sobre privacidad y comunicaciones electrónicas ha contribuido eficazmente a una protección adecuada del respeto de la vida privada y la confidencialidad de las comunicaciones en la UE. También se procuró detectar posibles solapamientos.

La evaluación REFIT llega a la conclusión de que los mencionados objetivos de la Directiva siguen siendo **pertinentes**. El RGPD garantiza la protección de los datos personales, mientras que la Directiva sobre privacidad y comunicaciones electrónicas garantiza la confidencialidad de las comunicaciones, que también pueden contener datos de carácter no personal y datos relacionados con personas jurídicas. Por consiguiente, es preciso un instrumento independiente para garantizar la protección efectiva del derecho contemplado en el artículo 7 de la Carta. Se ha comprobado que también siguen siendo pertinentes otras disposiciones tales como las normas sobre el envío de comunicaciones comerciales no solicitadas.

En términos de **eficacia y eficiencia**, la evaluación REFIT llega a la conclusión de que la Directiva no ha alcanzado plenamente sus objetivos. La imprecisa redacción de determinadas disposiciones y la ambigüedad de los conceptos jurídicos han puesto en peligro la armonización, ocasionando dificultades a las empresas a la hora de desarrollar actividades transfronterizas. La evaluación también pone de manifiesto que algunas disposiciones han impuesto una carga innecesaria a empresas y consumidores. Así, por ejemplo, la norma relativa al consentimiento, destinada a proteger la confidencialidad de los equipos terminales, no ha logrado alcanzar sus objetivos por cuanto los usuarios finales pueden acceder a que se les instalen *cookies* de rastreo sin comprender lo que ello significa y, en algunos casos, se ven incluso expuestos a *cookies* instaladas sin su consentimiento. La norma relativa al consentimiento tiene un alcance a veces demasiado amplio, pues también engloba prácticas que no afectan a la privacidad, y a veces demasiado limitado, ya que no abarca claramente algunas técnicas de seguimiento (por ejemplo, la huella digital de dispositivo) que pueden no

entrañar el acceso o almacenamiento en el dispositivo. Por último, su aplicación puede resultar onerosa para las empresas.

La evaluación llega a la conclusión de que las normas sobre privacidad y comunicaciones electrónicas siguen presentando **valor añadido europeo** para alcanzar mejor el objetivo de garantizar la protección de la vida privada en línea en un mercado de las comunicaciones electrónicas de carácter cada vez más transnacional. También demuestra que, en general, las normas son **coherentes** con otras normativas pertinentes, a pesar de que se hayan detectado algunas repeticiones innecesarias en relación con el nuevo RGPD (véase la sección 1.2).

3.2. Consultas con las partes interesadas

La Comisión organizó una consulta pública, que tuvo lugar entre el 12 de abril y el 5 de julio de 2016 y en la que se recibieron 421 respuestas[12]. Las principales conclusiones son las siguientes[13]:

– **Necesidad de normas específicas para el sector de las comunicaciones electrónicas en materia de confidencialidad de las comunicaciones electrónicas**: el 83,4 % de los ciudadanos, las organizaciones de consumidores y de la sociedad civil y el 88,9 % de las administraciones públicas que participaron en la consulta reconocían esta necesidad, mientras que el 63,4 % de los participantes del sector no lo hacían.

– **Ampliación del ámbito de aplicación a nuevos servicios de comunicaciones (OTT)**: el 76 % de los ciudadanos y de la sociedad civil y el 93,1 % de las administraciones públicas estaban a favor de la ampliación, porcentajes que se reducían al 36,2 % en el caso de los participantes del sector.

– **Modificación de las excepciones con respecto al consentimiento para el tratamiento de datos de tráfico y localización**: el 49,1 % de los ciudadanos y organizaciones de consumidores y de la sociedad civil y el 36 % de las administraciones públicas preferían no ampliar las excepciones, mientras que, en el sector, el 36 % de los participantes estaba a favor de ampliar las excepciones y dos terceras partes abogaban por la mera derogación de las disposiciones.

– **Apoyo a las soluciones propuestas para la cuestión del consentimiento del uso de *cookies***: el 81,2 % de los ciudadanos y el 63 % de las administraciones públicas abogan por que se imponga a los fabricantes de equipos terminales la obligación de comercializar productos con las opciones de privacidad predeterminadas activadas, mientras que el 58,3 % del sector opta por respaldar la autorregulación o la corregulación.

Además, la Comisión Europea organizó dos reuniones de trabajo en abril de 2016, una destinada a todas las partes interesadas y otra a las administraciones nacionales competentes,

[12] 162 contribuciones de ciudadanos, 33 de organizaciones de consumidores y de la sociedad civil, 186 del sector y 40 de administraciones públicas, incluidas las autoridades competentes encargadas de la aplicación de la Directiva sobre privacidad y comunicaciones electrónicas.

[13] El informe completo puede consultarse en: https://ec.europa.eu/digital-single-market/news-redirect/37204.

en las que se examinaron las principales cuestiones de las consultas públicas. Los puntos de vista expresados durante dichas reuniones reflejaban los resultados de la consulta pública.

Con el fin de conocer la opinión de los ciudadanos, se realizó en toda la UE una encuesta del Eurobarómetro sobre la privacidad en las comunicaciones electrónicas[14]. Las principales conclusiones son las siguientes[15]:

– El 78 % de los encuestados considera muy importante que para acceder a la información de carácter personal almacenada en su ordenador, móvil o tableta sea necesaria su autorización.

– El 72 % señala que es muy importante que esté garantizada la confidencialidad de sus mensajes electrónicos y de la mensajería instantánea en línea.

– El 89 % está de acuerdo con la opción propuesta de que la configuración predeterminada de su navegador deje de compartir su información.

3.3. Obtención y uso de asesoramiento especializado

La Comisión se basó en el siguiente asesoramiento externo:

– Consultas específicas a grupos de expertos de la UE: dictamen del Grupo de Trabajo del artículo 29; dictamen del SEPD; dictamen de la plataforma REFIT; opinión del ORECE; opinión de la ENISA y de los miembros de la Red de Cooperación para la Protección del Consumidor.

– Asesoramiento externo, en particular los dos estudios siguientes:

  – Estudio *ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation* [«Directiva sobre privacidad y comunicaciones electrónicas: evaluación de la transposición, eficacia y compatibilidad con la propuesta de Reglamento sobre protección de datos», documento no disponible en lengua española] (SMART 2013/007116).

  – Estudio *Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector* [«Evaluación y revisión de la Directiva 2002/58 sobre la privacidad y el sector de las comunicaciones electrónicas», documento no disponible en lengua española] (SMART 2016/0080).

3.4. Evaluación de impacto

Se realizó una evaluación de impacto de esta propuesta, sobre la que el Comité de Control Reglamentario emitió un dictamen favorable el 28 de septiembre de 2016[16]. Atendiendo a las recomendaciones del Consejo, la evaluación de impacto explica más exhaustivamente el alcance de la iniciativa, su coherencia con otros instrumentos jurídicos (RGPD, CECE, Directiva sobre equipos radioeléctricos) y la necesidad de contar con un instrumento independiente. La hipótesis de referencia se amplía y aclara. El análisis de los efectos se

14 Encuesta del Eurobarómetro (EB) n.º 443 sobre la privacidad en las comunicaciones electrónicas (SMART 2016/079).

15 El informe completo puede consultarse en: https://ec.europa.eu/digital-single-market/news-redirect/37205.

16 http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

refuerza y hace más equilibrado, aclarando y ampliando la descripción de los costes y beneficios previstos.

Se examinaron las siguientes opciones de actuación en función de los criterios de eficacia, eficiencia y coherencia:

– **Opción 1:** Medidas de Derecho indicativo (no vinculantes)

– **Opción 2:** Refuerzo limitado de la privacidad/confidencialidad y simplificación

– **Opción 3:** Refuerzo moderado de la privacidad/confidencialidad y simplificación

– **Opción 4:** Mayor refuerzo de la privacidad/confidencialidad y simplificación

– **Opción 5:** Derogación de la Directiva sobre privacidad y comunicaciones electrónicas.

La opción 3 destacó en muchos aspectos como **opción preferida** para alcanzar los objetivos fijados, teniendo en cuenta al mismo tiempo su eficiencia y coherencia. Sus principales ventajas son las siguientes:

– Aumenta la protección de la confidencialidad de las comunicaciones electrónicas ampliando el ámbito de aplicación del instrumento jurídico para incluir en él nuevos servicios de comunicaciones electrónicas equivalentes desde el punto de vista funcional. Además, el Reglamento ofrece al usuario final mayores posibilidades de control al aclarar que el consentimiento puede expresarse mediante los oportunos parámetros técnicos.

– Incrementa la protección contra las comunicaciones no solicitadas, introduciendo la obligación de presentar la identificación de la línea llamante o un prefijo obligatorio para las llamadas comerciales y ofreciendo mayores posibilidades de bloquear las llamadas de números no deseados.

– Simplifica y aclara el marco regulador reduciendo el margen de maniobra de los Estados miembros, derogando disposiciones obsoletas y ampliando las excepciones a las normas de consentimiento.

Se prevé que la incidencia económica de la opción 3 sea globalmente proporcionada a los objetivos de la propuesta. Se abren nuevas perspectivas comerciales relacionadas con el tratamiento de los datos de las comunicaciones para los servicios de comunicaciones electrónicas tradicionales, mientras que los proveedores OTT pasan a estar sujetos a las mismas normas, lo cual les supondrá costes de conformidad adicionales. Con todo, este cambio no afectará sustancialmente a aquellos proveedores OTT que ya operan sobre la base del consentimiento. Por último, el impacto de esta opción no se notará en los Estados miembros que ya han ampliado estas normas a los proveedores OTT.

Con esta opción se centraliza el consentimiento en programas o aplicaciones tales como los navegadores de Internet, se incita a los usuarios a elegir su configuración de privacidad y se amplían las excepciones a la norma de consentimiento del uso de *cookies*, gracias a lo cual es posible que una proporción significativa de empresas suprima los mensajes y anuncios de *cookies*, lo que entrañará ahorros de costes potencialmente considerables y una mayor simplificación. No obstante, a los anunciantes de publicidad personalizada en línea les puede

resultar más difícil obtener el consentimiento si una gran proporción de usuarios opta en su configuración por no aceptar *cookies* de terceros. Al mismo tiempo, centralizar el consentimiento no impide a los operadores de sitios web obtener el consentimiento por medio de solicitudes individuales a los usuarios finales y mantener así su modelo de negocio actual. Ello supondría costes adicionales para algunos proveedores de navegadores o programas similares, que deberían garantizar configuraciones respetuosas de la privacidad.

El estudio externo presentaba tres hipótesis distintas de aplicación de la opción 3 en función de la entidad que vaya a establecer el recuadro de diálogo entre el usuario que haya elegido «rechazar *cookies* de terceros» o «no realizar seguimiento» en su configuración y los sitios web que visita y que quieren que reconsidere su elección. Las entidades que podrían ser responsables de esta labor técnica son las siguientes: 1) programas como los navegadores de Internet; 2) rastreadores de terceros; 3) los sitios web en cuestión (es decir, el servicio de la sociedad de la información solicitado por el usuario). En comparación con la hipótesis de referencia, la opción 3 generaría un ahorro global en términos de costes de conformidad de un 70 % (948,8 millones EUR) en el primer caso (navegadores), aplicado en la presente propuesta. Los ahorros de costes serían inferiores en las demás hipótesis. Dado que el ahorro global se deriva en gran medida de una acusada disminución del número de empresas afectadas, se prevé que el importe de los costes de conformidad con los que deba correr una empresa sea por término medio superior al de hoy en día.

3.5. Adecuación regulatoria y simplificación

Las medidas estratégicas propuestas en la opción preferida persiguen el objetivo de simplificar y reducir la carga administrativa, de acuerdo con los resultados de la evaluación REFIT y el dictamen de la plataforma REFIT[17].

La plataforma REFIT formuló tres series de recomendaciones a la Comisión:

– Debe reforzarse la protección de la vida privada de los ciudadanos adecuando la Directiva sobre privacidad y comunicaciones electrónicas al Reglamento general de protección de datos.

– Debe depararse una protección más eficaz a los ciudadanos contra la publicidad no solicitada añadiendo excepciones a la norma del consentimiento con respecto a las *cookies*.

– La Comisión ha de examinar los problemas de aplicación que surjan a escala nacional y facilitar el intercambio de mejores prácticas entre los Estados miembros.

La propuesta incluye específicamente los siguientes aspectos:

– Uso de definiciones neutras desde el punto de vista tecnológico para integrar nuevos servicios y tecnologías de modo que el Reglamento esté preparado para el futuro.

– Derogación de las normas en materia de seguridad para evitar la doble regulación.

– Aclaración del ámbito de aplicación para contribuir a eliminar o reducir el riesgo de divergencias en la aplicación por los Estados miembros (punto 3 del dictamen).

[17] http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf.

– Clarificación y simplificación de la norma relativa al consentimiento para el uso de *cookies* y otros identificadores, tal como se explica en las secciones 3.1 y 3.4 (punto 2 del dictamen).

– Atribución de las funciones de control a las autoridades responsables de la aplicación del RGPD y recurso al mecanismo de coherencia del RGPD.

3.6. Impacto en los derechos fundamentales

La propuesta tiene como objetivo incrementar el nivel y la eficacia de protección de la vida privada y de los datos de carácter personal tratados en el contexto de las comunicaciones electrónicas de conformidad con los artículos 7 y 8 de la Carta y garantizar una mayor seguridad jurídica. La propuesta complementa y precisa el RGPD. La protección efectiva de la confidencialidad de las comunicaciones es esencial para ejercer la libertad de expresión y de información y otros derechos afines, tales como el derecho a la protección de los datos personales o la libertad de pensamiento, conciencia y religión.

4. REPERCUSIONES PRESUPUESTARIAS

La propuesta no tiene ninguna incidencia en el presupuesto de la Unión.

5. OTROS ELEMENTOS

5.1. Planes de ejecución y modalidades de seguimiento, evaluación e información

La Comisión supervisará la aplicación del Reglamento y presentará cada tres años un informe sobre su evaluación al Parlamento Europeo y al Consejo, así como al Comité Económico y Social Europeo. Estos informes serán públicos y analizarán la aplicación y el cumplimiento efectivos del presente Reglamento.

5.2. Explicación detallada de las disposiciones específicas de la propuesta

El capítulo I contiene las disposiciones generales: el objeto (artículo 1), el ámbito de aplicación (artículos 2 y 3) y sus definiciones, incluidas las referencias a las definiciones pertinentes de otros instrumentos de la UE como, por ejemplo, el RGPD.

El capítulo II contiene las principales disposiciones para garantizar la confidencialidad de las comunicaciones electrónicas (artículo 5), limita los fines autorizados y establece las condiciones de tratamiento de esos datos de comunicaciones (artículos 6 y 7). También aborda la protección de los equipos terminales i) garantizando la integridad de la información almacenada en ellos, y ii) protegiendo la información emitida por los equipos terminales, ya que puede permitir identificar a sus usuarios finales (artículo 8). Por último, el artículo 9 establece disposiciones con respecto al consentimiento de los usuarios finales —uno de los fundamentos jurídicos esenciales del presente Reglamento—, remitiéndose expresamente a su definición y a las condiciones establecidas en el RGPD, mientras que el artículo 10 impone a los proveedores de programas informáticos que permiten hacer uso de las comunicaciones electrónicas la obligación de ayudar a los usuarios finales a tomar las decisiones adecuadas en materia de configuración de la privacidad. En el artículo 11 se detallan los fines y las condiciones para que los Estados miembros puedan restringir las disposiciones antes mencionadas.

El capítulo III presenta los derechos que asisten a los usuarios finales en materia de control del envío y la recepción de comunicaciones electrónicas a fin de proteger su privacidad: i) derecho de los usuarios finales a impedir la presentación de la identificación de la línea llamante para garantizar el anonimato (artículo 12), con las limitaciones correspondientes (artículo 13); y ii) obligación de los proveedores de servicios de comunicaciones interpersonales basados en números y disponibles al público de prever la posibilidad de limitar la recepción de llamadas no deseadas (artículo 14). Este capítulo también regula las condiciones en que los usuarios finales pueden ser incluidos en guías accesibles al público (artículo 15) y las condiciones en que pueden efectuarse comunicaciones no solicitadas para fines de mercadotecnia directa (artículo 17). Asimismo, contempla los riesgos en materia de seguridad y prevé la obligación por parte de los proveedores de servicios de comunicaciones electrónicas de alertar a los usuarios finales en caso de que surja un riesgo específico que pueda comprometer la seguridad de sus redes y servicios. Las obligaciones en materia de seguridad establecidas en el RGPD y en el CECE se aplicarán a los proveedores de servicios de comunicaciones electrónicas.

El capítulo IV se refiere a la supervisión y ejecución del presente Reglamento, que se confían a las autoridades de control encargadas del RGPD, habida cuenta de las grandes sinergias existentes entre la protección de datos en general y la confidencialidad de las comunicaciones (artículo 18). Las atribuciones del Comité Europeo de Protección de Datos se amplían (artículo 19) y el mecanismo de cooperación y coherencia previsto en el RDPR será aplicable en los asuntos transfronterizos relacionados con el presente Reglamento (artículo 20).

El capítulo V describe las distintas vías de recurso de que disponen los usuarios finales (artículos 21 y 22) y las sanciones que pueden imponerse (artículo 24), en particular las condiciones generales para la imposición de multas administrativas (artículo 23).

El capítulo VI trata la adopción de actos delegados y actos de ejecución con arreglo a lo dispuesto en los artículos 290 y 291 del Tratado.

Por último, el capítulo VII contiene las disposiciones finales del presente Reglamento: la derogación de la Directiva sobre privacidad y comunicaciones electrónicas, la supervisión y la evaluación, la entrada en vigor y la aplicación. En lo que respecta a la evaluación, la Comisión tiene la intención de evaluar, en particular, si sigue siendo necesario un acto jurídico separado a la vista de la evolución jurídica, técnica o económica y teniendo en cuenta la primera evaluación del Reglamento (UE) 2016/679, prevista para el 25 de mayo de 2020.

2017/0003 (COD)

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)

(Texto pertinente a efectos del EEE)

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular sus artículos 16 y 114,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo[1],

Visto el dictamen del Comité de las Regiones[2],

Visto el dictamen del Supervisor Europeo de Protección de Datos[3],

De conformidad con el procedimiento legislativo ordinario,

Considerando lo siguiente:

(1) El artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «la Carta») ampara el derecho fundamental de toda persona al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. El respeto de la privacidad de las comunicaciones personales constituye una dimensión esencial de este derecho. La confidencialidad de las comunicaciones electrónicas garantiza que la información intercambiada entre las partes y los elementos externos de la comunicación, incluyendo el momento en que se ha remitido la información, el lugar desde el que se ha enviado y su destinatario, no se revelará a partes distintas de las que intervienen en la comunicación. El principio de confidencialidad debe aplicarse a los medios de comunicación actuales y futuros, entre ellos las llamadas telefónicas, el acceso a Internet, las aplicaciones de mensajería instantánea, el correo electrónico, las

[1] DO C […] de […], p. […].
[2] DO C […] de […], p. […].
[3] DO C […] de […], p. […].

llamadas telefónicas por Internet y los mensajes personales transmitidos a través de las redes sociales.

(2) El contenido de las comunicaciones electrónicas puede desvelar información muy delicada sobre las personas físicas que participan en ellas, tales como experiencias personales y emociones, problemas de salud, preferencias sexuales y opiniones políticas, cuya divulgación podría causar daños personales y sociales, pérdidas económicas o situaciones embarazosas. Del mismo modo, los metadatos derivados de las comunicaciones electrónicas también pueden desvelar información muy delicada y de carácter personal. Entre esos metadatos figuran los números a los que se ha llamado, los sitios web visitados, la localización geográfica o la hora, la fecha y la duración de una llamada, información que permite extraer conclusiones precisas sobre la vida privada de las personas participantes en la comunicación electrónica tales como sus relaciones sociales, sus costumbres y actividades de la vida cotidiana, sus intereses, sus preferencias, etc.

(3) Los datos de las comunicaciones electrónicas también pueden revelar información relativa a las personas jurídicas, como secretos comerciales u otro tipo de información confidencial que tiene valor económico. Por consiguiente, las disposiciones del presente Reglamento deben aplicarse tanto a las personas físicas como a las personas jurídicas. Por otra parte, el presente Reglamento debe garantizar que las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[4] sean también aplicables a los usuarios finales que son personas jurídicas. Ello incluye la definición de consentimiento con arreglo al Reglamento (UE) 2016/679. Cuando se haga referencia al consentimiento de un usuario final, incluidas las personas jurídicas, debe aplicarse esa definición. Además, las personas jurídicas deben tener los mismos derechos que los usuarios finales que son personas físicas en lo que se refiere a las autoridades de control; por otra parte, las autoridades de control en el marco del presente Reglamento también han de ser responsables de supervisar su aplicación por lo que se refiere a las personas jurídicas.

(4) Con arreglo al artículo 8, apartado 1, de la Carta y al artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea, toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. El Reglamento (UE) 2016/679 establece normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y normas relativas a la libre circulación de tales datos. Los datos de las comunicaciones electrónicas pueden incluir datos personales a tenor del Reglamento (UE) nº 2016/679.

(5) Las disposiciones del presente Reglamento precisan y complementan las normas generales sobre la protección de datos personales establecidas en el Reglamento (UE) 2016/679 en lo que respecta a los datos de comunicaciones electrónicas que pueden considerarse datos personales. Por consiguiente, el presente Reglamento no reduce el nivel de protección que depara a las personas físicas el Reglamento (UE) 2016/679. El tratamiento de datos de comunicaciones electrónicas por parte de los proveedores de

[4] 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, pp. 1-88).

servicios de comunicaciones electrónicas solo debe autorizarse de conformidad con el presente Reglamento.

(6) Aunque los principios y las principales disposiciones de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo[5] sigan siendo por lo general válidos, dicha Directiva no se ha adaptado del todo al ritmo de la evolución de la tecnología y del mercado, debido a lo cual se ha deparado una protección incoherente e insuficientemente eficaz de la privacidad y la confidencialidad en relación con las comunicaciones electrónicas. Entre esas novedades figura la entrada en el mercado de servicios de comunicaciones electrónicas que, desde la perspectiva del consumidor, pueden sustituir a los servicios tradicionales, pero no tienen que cumplir el mismo conjuntos de normas. Otra novedad la constituyen las nuevas técnicas, no reguladas por la Directiva 2002/58/CE, que permiten rastrear los comportamientos en línea de los usuarios finales. Por lo tanto, procede derogar la Directiva 2002/58/CE y sustituirla por el presente Reglamento.

(7) Dentro de los límites del presente Reglamento, conviene autorizar a los Estados miembros a mantener o introducir disposiciones nacionales que precisen o aclaren la aplicación de las normas del presente Reglamento con el fin de garantizar la aplicación e interpretación efectivas de dichas normas. Por consiguiente, el margen de apreciación de que disponen los Estados miembros en este sentido debe mantener un equilibrio entre la protección de la vida privada y de los datos de carácter personal y la libre circulación de los datos de las comunicaciones electrónicas.

(8) El presente Reglamento debe aplicarse a los proveedores de servicios de comunicaciones electrónicas, a los proveedores de guías accesibles al público y a los proveedores de programas informáticos que permiten acceder a servicios de comunicaciones electrónicas, incluyendo la recuperación y presentación de información de Internet. El presente Reglamento debe aplicarse también a las personas físicas y jurídicas que utilizan los servicios de comunicaciones electrónicas para el envío de comunicaciones comerciales de mercadotecnia directa o recopilan información relativa a los usuarios finales o que está almacenada en sus equipos terminales.

(9) El presente Reglamento debe aplicarse a los datos de comunicaciones electrónicas tratados en relación con la prestación y el uso de servicios de comunicaciones electrónicas en la Unión, independientemente de que el tratamiento se efectúe en la Unión o no. Por otra parte, con el fin de no privar a los usuarios finales de la Unión de una protección efectiva, el presente Reglamento debe aplicarse también a los datos de comunicaciones electrónicas tratados en relación con la prestación de servicios de comunicaciones electrónicas desde fuera de la Unión a usuarios finales de la Unión.

(10) Los equipos radioeléctricos y los soportes lógicos correspondientes que se introduzcan en el mercado interior de la Unión deben ajustarse a lo dispuesto en la Directiva

[5] 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, p. 37).

2014/53/UE del Parlamento Europeo y del Consejo[6]. El presente Reglamento no debe afectar a la aplicabilidad de ninguno de los requisitos de la Directiva 2014/53/UE ni a los poderes de la Comisión para adoptar con arreglo a dicha Directiva actos delegados en los que se exija que determinadas categorías o clases de equipos radioeléctricos incorporen salvaguardias para garantizar la protección de los datos personales y la privacidad de los usuarios finales.

(11) Los servicios utilizados para fines de comunicación y los medios técnicos para su prestación han evolucionado considerablemente. Los usuarios finales sustituyen cada vez más los servicios tradicionales de telefonía vocal, mensajes de texto (SMS) y correo electrónico por servicios en línea de función equivalente, como voz sobre IP, servicios de mensajería y servicios de correo electrónico basados en la web. Con el fin de garantizar una protección efectiva y equivalente de los usuarios finales cuando estos utilizan servicios de función equivalente, el presente Reglamento emplea la definición de servicios de comunicaciones electrónicas establecida en la [Directiva del Parlamento Europeo y del Consejo por la que se establece el Código Europeo de las Comunicaciones Electrónicas[7]]. Dicha definición engloba no solo los servicios de acceso a Internet y los servicios que consisten total o parcialmente en la transmisión de señales, sino también los servicios de comunicaciones interpersonales, que pueden estar basados en números o no como, por ejemplo, los servicios de voz sobre IP, los servicios de mensajería y los servicios de correo electrónico basados en la web. La protección de la confidencialidad de las comunicaciones es también fundamental en lo que se refiere a los servicios de comunicaciones interpersonales complementarios de otros servicios; este tipo de servicios también posee una funcionalidad de comunicación, por lo que ha de quedar regulado por el presente Reglamento.

(12) Los dispositivos y máquinas conectados se comunican cada vez más entre sí mediante redes de comunicaciones electrónicas (internet de las cosas). La transmisión de comunicaciones de máquina a máquina comporta el transporte de señales a través de una red y, por ende, constituye generalmente un servicio de comunicaciones electrónicas. Con el fin de garantizar la plena protección de los derechos a la privacidad y la confidencialidad de las comunicaciones y promover una internet de las cosas fiable y segura en el mercado único digital, es necesario aclarar que el presente Reglamento ha de aplicarse a la transmisión de comunicaciones de máquina a máquina. Por lo tanto, el principio de confidencialidad establecido en el presente Reglamento también ha de aplicarse a la transmisión de comunicaciones de máquina a máquina. También se podrían adoptar salvaguardias específicas en la normativa sectorial, como por ejemplo la Directiva 2014/53/UE.

(13) El desarrollo de tecnologías inalámbricas rápidas y eficientes ha favorecido un mayor acceso público a Internet a través de redes inalámbricas en espacios públicos y semiprivados tales como los puntos de acceso situados en diferentes lugares de una ciudad, grandes almacenes, centros comerciales u hospitales. En la medida en que esas redes de comunicaciones están a disposición de un grupo indefinido de usuarios

---

6 Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE (DO L 153 de 22.5.2014, p. 62).

7 Propuesta de la Comisión relativa a una Directiva del Parlamento Europeo y del Consejo por la que se establece el Código Europeo de las Comunicaciones Electrónicas (refundición) [COM/2016/0590 final — 2016/0288 (COD)].

finales, es preciso proteger la confidencialidad de las comunicaciones transmitidas a través de ellas. Que los servicios de comunicaciones electrónicas inalámbricas puedan ser complementarios de otros servicios no ha de suponer un obstáculo para garantizar la protección de la confidencialidad de los datos de comunicaciones y la aplicación del presente Reglamento. Por consiguiente, el presente Reglamento debe aplicarse a los datos de comunicaciones electrónicas que utilicen servicios de comunicaciones electrónicas y redes públicas de comunicaciones. Por el contrario, el presente Reglamento no ha de aplicarse a los grupos cerrados de usuarios finales, tales como las redes corporativas, cuyo acceso esté reservado a los miembros de la empresa.

(14) Los datos de comunicaciones electrónicas deben definirse de manera lo suficientemente amplia y tecnológicamente neutra como para incluir cualquier información relativa al contenido transmitido o intercambiado (contenido de las comunicaciones electrónicas) y la información relativa al usuario final de servicios de comunicaciones electrónicas que se haya tratado con el fin de transmitir, distribuir o permitir el intercambio de contenido de comunicaciones electrónicas; incluidos los datos para rastrear e identificar el origen y el destino de una comunicación, la localización geográfica y la fecha, hora, duración y tipo de comunicación. Con independencia de que esas señales y los datos correspondientes se transmitan por cable, ondas hertzianas, medios ópticos o electromagnéticos, en particular las redes por satélite, las redes de cable, las redes terrestres fijas (de conmutación de circuitos y de paquetes, incluida Internet) y móviles, y sistemas de tendido eléctrico, los datos relativos a estas señales deben considerarse metadatos de comunicaciones electrónicas y estar por tanto sujetos a las disposiciones del presente Reglamento. 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.

(15) Los datos de comunicaciones electrónicas han de considerarse confidenciales, lo cual significa que debe prohibirse toda interferencia en su transmisión, bien directamente por intervención humana, bien a través de un tratamiento automatizado por máquinas, sin el consentimiento de todas las partes que intervienen en la comunicación. 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. Puede producirse interceptación de datos de comunicaciones electrónicas, por ejemplo, cuando una persona distinta de las partes que intervienen en la comunicación escucha llamadas, lee, escanea o almacena el contenido de las comunicaciones electrónicas o los metadatos correspondientes para fines distintos del intercambio de comunicaciones. También puede producirse interceptación cuando terceras partes hacen un seguimiento de los sitios visitados, el calendario de las visitas, la interacción con otras personas, etc., sin el consentimiento del usuario final afectado. A medida que la tecnología avanza, aumentan también los medios técnicos para la interceptación. Dichos medios pueden abarcar desde la instalación de equipos que recopilan datos de los equipos terminales de las zonas seleccionadas, como los denominados receptores de IMSI (identidad internacional de abonado móvil), hasta algunos programas y técnicas que, por ejemplo, efectúan un seguimiento subrepticio de los hábitos de navegación para crear perfiles de usuarios finales. Otros ejemplos de interceptación pueden ser la captura de datos de la carga útil o de datos de contenido de redes y encaminadores inalámbricos sin cifrar, entre ellos los hábitos de navegación, sin el consentimiento de los usuarios finales.

(16) La prohibición de almacenar comunicaciones no tiene por objeto impedir el almacenamiento automático, intermedio y transitorio de la información en la medida en que se lleve a cabo con el único propósito de efectuar la transmisión en la red de comunicaciones electrónicas. Tampoco se debería prohibir el tratamiento de datos de comunicaciones electrónicas para garantizar la seguridad y continuidad de los servicios de comunicaciones electrónicas, incluyendo la verificación de amenazas para la seguridad tales como la presencia de programas maliciosos o el tratamiento de metadatos para cubrir requisitos necesarios de calidad del servicio tales como la latencia, la fluctuación de fase, etc.

(17) El tratamiento de los datos de comunicaciones electrónicas puede ser útil para las empresas, los consumidores y la sociedad en su conjunto. En relación con la Directiva 2002/58/CE, el presente Reglamento ofrece a los proveedores de servicios de comunicaciones electrónicas mayores posibilidades para tratar los metadatos de dichas comunicaciones, siempre que hayan obtenido el consentimiento de los usuarios finales. No obstante, los usuarios finales conceden gran importancia a la confidencialidad de sus comunicaciones, incluidas sus actividades en línea, y al control de la utilización de los datos de comunicaciones electrónicas para fines distintos de la transmisión de la comunicación. Por tanto, el presente Reglamento debe exigir a los proveedores de servicios de comunicaciones electrónicas que obtengan el consentimiento de los usuarios finales para tratar metadatos de comunicaciones electrónicas, entre ellos datos de localización del dispositivo generados a efectos de concesión y mantenimiento del acceso y la conexión al servicio. Los datos de localización que se generen en un contexto distinto al de la prestación de servicios de comunicaciones electrónicas no han de considerarse metadatos. Entre los ejemplos de usos comerciales de metadatos de comunicaciones electrónicas por parte de los proveedores de servicios de comunicaciones electrónicas puede incluirse la realización de mapas térmicos, que consisten en la representación gráfica de datos con colores para indicar la presencia de personas. Para mostrar los movimientos del tráfico en ciertas direcciones durante un determinado período de tiempo, es necesario un identificador que conecte las posiciones de las personas en determinados intervalos de tiempo. Ese identificador faltaría si tuvieran que utilizarse datos anónimos y el movimiento no se podría mostrar. Este uso de metadatos de comunicaciones electrónicas podría, por ejemplo, ayudar a las autoridades públicas y los operadores de transporte público a determinar en qué lugar pueden crear nuevas infraestructuras en función del uso de las estructuras existentes y de la presión ejercida sobre ellas. Cuando un tipo de tratamiento de metadatos de comunicaciones electrónicas, en particular mediante la utilización de las nuevas tecnologías, y teniendo en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, puede entrañar un riesgo elevado para los derechos y libertades de las personas físicas, antes del tratamiento se ha de efectuar una evaluación de impacto relativa a la protección de datos y, en su caso, consultar a la autoridad de control, de conformidad con los artículos 35 y 36 del Reglamento (UE) 2016/679.

(18) Los usuarios finales pueden consentir en que se traten sus metadatos para recibir servicios específicos tales como servicios de protección contra actividades fraudulentas (mediante el análisis de los datos de uso, la ubicación y la cuenta del cliente en tiempo real). En la economía digital, los servicios se prestan con frecuencia a cambio de una contraprestación distinta del dinero, por ejemplo exponiendo a los usuarios finales a anuncios publicitarios. A los efectos del presente Reglamento, el consentimiento del usuario final, independientemente de si es una persona física o

jurídica, debe tener el mismo significado y estar sujeto a las mismas condiciones que el consentimiento del interesado a tenor del Reglamento (UE) 2016/679. Los servicios de acceso a la Internet de banda ancha básica y de comunicaciones de voz han de considerarse servicios esenciales para que los particulares puedan comunicarse y participar en las ventajas de la economía digital. El consentimiento para el tratamiento de datos derivados del uso de Internet o de comunicaciones de voz no será válido si el interesado no goza de verdadera libertad de elección o no puede denegar o retirar su consentimiento sin verse perjudicado.

(19) El contenido de las comunicaciones electrónicas es una parte esencial del derecho fundamental al respeto de la vida privada y familiar, el domicilio y las comunicaciones, protegido por el artículo 7 de la Carta. Cualquier interferencia en el contenido de las comunicaciones electrónicas debe autorizarse únicamente en condiciones claramente definidas, para fines específicos y con garantías adecuadas contra el uso abusivo. El presente Reglamento prevé la posibilidad de que los proveedores de servicios de comunicaciones electrónicas traten datos de comunicaciones electrónicas en tránsito, con el consentimiento informado de todos los usuarios finales interesados. Por ejemplo, los proveedores pueden ofrecer servicios que comporten el examen de correos electrónicos para suprimir determinados materiales predefinidos. Habida cuenta del carácter delicado del contenido de las comunicaciones, el presente Reglamento establece la presunción de que el tratamiento de tales datos de contenido supondrá un elevado riesgo para los derechos y libertades de las personas físicas. En el tratamiento de este tipo de datos, el proveedor del servicio de comunicaciones electrónicas debe consultar siempre a la autoridad de control antes del tratamiento. Esta consulta debe ser conforme al artículo 36, apartados 2 y 3, del Reglamento (UE) 2016/679. La presunción no se aplica al tratamiento de datos de contenido para prestar un servicio solicitado por el usuario final si este ha dado el consentimiento oportuno y el tratamiento se efectúa con la finalidad y la duración estrictamente necesarias y proporcionadas a tal servicio. Cuando el contenido de las comunicaciones electrónicas haya sido enviado por el usuario final y recibido por el usuario o los usuarios finales a los que se destina, puede ser registrado o almacenado por el usuario final, los usuarios finales o por un tercero encargado por ellos de registrar o almacenar tales datos. Todo tratamiento de tales datos debe cumplir lo dispuesto en el Reglamento (UE) 2016/679.

(20) Los equipos terminales de los usuarios finales de redes de comunicaciones electrónicas y toda la información relativa a la utilización de dichos equipos, en particular la almacenada o emitida por ellos, solicitada o tratada para permitir que puedan conectarse a otro dispositivo o equipo de red, forman parte de la esfera privada de los usuarios finales, que debe ser protegida en virtud de la Carta de los Derechos Fundamentales de la Unión Europea y el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Dado que dichos equipos contienen o tratan información que puede desvelar pormenores de una persona en los ámbitos afectivo, político o social, incluyendo el contenido de las comunicaciones, las imágenes, la localización de personas a través del acceso a las capacidades de GPS del dispositivo, las listas de contactos y otros datos ya almacenados en el dispositivo, la información relativa a esos equipos requiere una mayor protección de la privacidad. Por otra parte, los denominados «programas espía», las balizas web, los identificadores ocultos, las *cookies* de rastreo y otros dispositivos similares de seguimiento no deseados pueden introducirse en el equipo terminal del usuario final sin su conocimiento para acceder a los datos, archivar información oculta o rastrear

actividades. También es posible recopilar a distancia información relacionada con el dispositivo del usuario final a efectos de identificación y seguimiento utilizando técnicas tales como la «huella digital de dispositivo», con frecuencia sin el conocimiento del usuario final, lo cual puede suponer una grave intromisión en la vida privada de esos usuarios finales. Las técnicas que, de manera subrepticia, hacen un seguimiento de las acciones de los usuarios finales, por ejemplo rastreando sus actividades en línea o la localización de sus equipos terminales, o alteran el funcionamiento de los equipos terminales de los usuarios finales suponen una grave amenaza para la privacidad de estos. Por consiguiente, las interferencias de ese tipo en el equipo terminal del usuario final solo han de permitirse con el consentimiento del usuario final y para fines específicos y transparentes.

(21) Las excepciones a la obligación de obtener consentimiento para hacer uso de las capacidades de tratamiento y almacenamiento de equipos terminales o acceder a la información almacenada en ellos deberían limitarse a situaciones que no entrañen intromisión alguna, o una intromisión muy limitada, en la vida privada. Por ejemplo, no ha de solicitarse consentimiento para autorizar el acceso o almacenamiento técnico que sean estrictamente necesarios y proporcionados al fin legítimo de permitir el uso de un servicio específico expresamente solicitado por el usuario final. Ello puede incluir el almacenamiento de *cookies* mientras dure una sesión única determinada en un sitio web, a fin de conservar las entradas del usuario final cuando este rellena formularios en línea de varias páginas. Las *cookies* pueden ser también un instrumento legítimo y útil, por ejemplo a la hora de medir el tráfico en un sitio web. No debe considerase acceso a un dispositivo o utilización de sus capacidades de tratamiento la comprobación de la configuración por parte de un proveedor de la sociedad de la información para prestar el servicio de acuerdo con los parámetros del usuario final ni el mero registro por el proveedor del hecho de que el dispositivo del usuario final no puede recibir el contenido que ha solicitado.

(22) Los métodos empleados para suministrar información y obtener el consentimiento del usuario final deben ser lo más sencillos posible. Habida cuenta de la utilización generalizada de *cookies* de rastreo y otras técnicas de seguimiento, a los usuarios finales se les pide cada vez más que den su consentimiento para almacenar dichas *cookies* en sus equipos terminales. Como consecuencia de ello, los usuarios finales se ven agobiados por las solicitudes de consentimiento. Este problema se puede resolver con el uso de medios técnicos para dar el consentimiento, por ejemplo a través de parámetros trasparentes y sencillos. El presente Reglamento debe prever, pues, la posibilidad de manifestar el consentimiento mediante el uso de los ajustes adecuados del navegador o de otra aplicación. Las opciones que elijan los usuarios finales al establecer la configuración general de privacidad de un navegador u otra aplicación deben ser vinculantes y oponibles frente a terceros. Los navegadores web son un tipo de aplicación informática que permite recuperar y presentar la información de Internet. Otros tipos de aplicaciones, como las que permiten llamar, enviar mensajes o facilitar orientación vial, poseen también las mismas capacidades. Los navegadores intervienen en gran parte de lo que ocurre entre el usuario final y el sitio web. Desde este punto de vista, ocupan una posición privilegiada para desempeñar un papel activo con el fin de ayudar a los usuarios finales a controlar el flujo de información que reciben y emiten los equipos terminales. Más concretamente, los navegadores pueden servir para montar la guardia, ayudando a los usuarios finales a impedir el acceso a la información de su equipo terminal (por ejemplo, un teléfono inteligente, una tableta o un ordenador) o el almacenamiento de la misma.

(23) Los principios de protección de datos desde el diseño y por defecto quedaron codificados en el artículo 25 del Reglamento (UE) 2016/679. En la actualidad, la mayoría de los navegadores están configurados por defecto para «aceptar todas las *cookies*». Por consiguiente, conviene que los proveedores de programas informáticos que permiten la recuperación y presentación de información de Internet estén obligados a configurar los programas de modo que ofrezcan la posibilidad de impedir a terceros almacenar información en el equipo terminal; esta opción suele presentarse con la frase «rechazar *cookies* de terceros». Los usuarios finales han de disponer de una serie de opciones de configuración que les permitan elegir entre distintos niveles de privacidad, desde el nivel más elevado (por ejemplo, «no aceptar nunca *cookies*») hasta el nivel más bajo (por ejemplo, «aceptar *cookies* siempre»), pasando por el nivel intermedio (por ejemplo, «rechazar *cookies* de terceros» o «solo aceptar *cookies* de origen»). Estos ajustes de privacidad han de presentarse de forma bien visible e inteligible.

(24) Para obtener el consentimiento de los usuarios finales, tal como se define en el Reglamento (UE) 2016/679 —por ejemplo, para el almacenamiento de *cookies* de rastreo de terceros—, los navegadores deben, en particular, solicitar al usuario final del equipo terminal un acto afirmativo claro que manifieste su voluntad libre, específica, informada e inequívoca de aceptar el almacenamiento de esas *cookies* en el equipo y el acceso a las mismas. Dicho acto puede considerarse afirmativo, por ejemplo, si se solicita a los usuarios finales que seleccionen la opción «aceptar *cookies* de terceros» para confirmar su acuerdo y se les ofrece la información necesaria para poder elegir. A tal fin, es preciso exigir a los proveedores de programas informáticos que facilitan el acceso a Internet que, en el momento de la instalación, informen a los usuarios finales de la posibilidad de elegir la configuración de privacidad entre las diversas opciones y les pidan que escojan una opción. La información proporcionada no ha de disuadir a los usuarios finales de seleccionar una configuración de mayor privacidad y debe incluir la información pertinente sobre los riesgos que puede entrañar autorizar el almacenamiento de *cookies* de terceros en el ordenador, incluyendo la conservación a largo plazo de registros de los historiales de navegación y el uso de los mismos para enviar publicidad personalizada. Conviene que los navegadores propongan a los usuarios finales métodos sencillos para modificar la configuración de privacidad en cualquier momento durante la utilización y les permitan excluir o aceptar determinados sitios web o especificar en qué sitios web aceptan siempre o no aceptan nunca *cookies* (de terceros).

(25) El acceso a las redes de comunicaciones electrónicas requiere la emisión periódica de determinados paquetes de datos a fin de descubrir o mantener una conexión con la red u otros dispositivos en la red. Además, a los dispositivos se les debe asignar una dirección única para que sean identificables en dicha red. De igual modo, las normas de telefonía inalámbrica y móvil comportan la emisión de señales activas que contienen identificadores únicos tales como una dirección MAC, la IMEI (identidad internacional de estación móvil), el IMSI, etc. Una sola estación base inalámbrica (es decir, un transmisor y receptor), como por ejemplo un punto de acceso inalámbrico, posee un alcance específico dentro del que puede obtenerse esa información. Han surgido proveedores de servicios que ofrecen servicios de seguimiento basados en el análisis de información asociada a los equipos con diversas funcionalidades, entre ellas hacer un recuento de personas, proporcionar datos sobre el número de personas de una cola de espera, determinar el número de personas en una zona concreta, etc. Esta información puede utilizarse para fines más intrusivos, como enviar mensajes

comerciales a los usuarios finales, por ejemplo cuando entran en una tienda, con ofertas personalizadas. Algunas de estas funcionalidades no entrañan riesgos graves para la privacidad, pero otras sí como, por ejemplo, las relacionadas con el seguimiento de las personas a lo largo del tiempo, incluidas las visitas repetidas a determinados sitios. Los proveedores que adoptan estas prácticas deben colocar en el límite de la zona de cobertura advertencias claras que informen a los usuarios finales, antes de entrar en la zona delimitada, de que esa tecnología está en funcionamiento dentro de un determinado perímetro, de la finalidad del seguimiento, de la persona responsable y de las medidas que puede tomar el usuario final del equipo terminal para reducir al mínimo o detener la recogida de datos. Debe facilitarse información adicional en los casos en que se recopilan datos personales con arreglo a lo dispuesto en el artículo 13 del Reglamento (UE) 2016/679.

(26) Cuando el tratamiento de datos de comunicaciones electrónicas por parte de los proveedores de servicios de comunicaciones electrónicas entre en su ámbito de aplicación, el presente Reglamento debe prever la posibilidad de que, en determinadas condiciones, la Unión o los Estados miembros limiten por ley determinadas obligaciones y derechos, siempre que tal limitación constituya una medida necesaria y proporcionada en una sociedad democrática para proteger determinados intereses públicos como la seguridad nacional, la defensa, la seguridad pública y la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección y prevención frente a las amenazas para la seguridad pública 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, o una función de control, de inspección o reglamentaria relacionada con el ejercicio del poder público en aras de tales intereses. Por consiguiente, el presente Reglamento no debe afectar a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando ello sea necesario y proporcionado para proteger los intereses públicos mencionados anteriormente, de conformidad con la Carta de los Derechos Fundamentales de la Unión Europea y el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, tal como han sido interpretados por el Tribunal de Justicia de la Unión Europea y el Tribunal Europeo de Derechos Humanos. Los proveedores de servicios de comunicaciones electrónicas deben prever procedimientos apropiados para facilitar las exigencias legítimas de las autoridades competentes, en su caso teniendo también en cuenta la función del representante nombrado con arreglo al artículo 3, apartado 3.

(27) Por lo que respecta a la identificación de la línea llamante, es necesario proteger el derecho del interlocutor que efectúa la llamada a reservarse la identificación de la línea desde la que realiza dicha llamada y el derecho del interlocutor llamado a rechazar llamadas procedentes de líneas no identificadas. Determinados usuarios finales, en particular las líneas de ayuda y otras organizaciones similares, tienen interés en garantizar el anonimato de sus interlocutores. Por lo que respecta a la identificación de la línea conectada, es necesario proteger el derecho y el interés legítimo del interlocutor llamado a reservarse la presentación de la identificación de la línea a la que está conectado realmente el interlocutor llamante.

(28) Está justificado anular la eliminación de la presentación de la identificación de la línea llamante en casos particulares. El derecho a la privacidad de los usuarios finales por lo que se refiere a la identificación de la línea llamante debe restringirse en los casos en

que ello sea necesario para rastrear llamadas molestas, y en lo tocante a los datos de identificación y localización de dicha línea, cuando ello sea preciso para que servicios de socorro como eCall cumplan su cometido con la máxima eficacia posible.

(29) Existen medios técnicos para que los proveedores de servicios de comunicaciones electrónicas limiten la recepción de llamadas no deseadas por los usuarios finales de distintas maneras, entre ellas el bloqueo de las llamadas silenciosas y otras llamadas fraudulentas y molestas. Los proveedores de servicios de comunicaciones interpersonales basados en números y disponibles al público han de emplear esos medios técnicos para proteger de forma gratuita a los usuarios finales de las llamadas molestas. Los proveedores deben velar por que los usuarios finales conozcan la existencia de tales funcionalidades, por ejemplo presentándolas en su página web.

(30) Las guías de usuarios finales de los servicios de comunicaciones electrónicas accesibles al público son objeto de amplia distribución. Se consideran guías accesibles al público cualesquiera guías o servicios que contienen información sobre los usuarios finales, como los números de teléfono (incluidos los teléfonos móviles) y los datos de contacto de correo electrónico, y se incluyen los servicios de información. El derecho a la privacidad y a la protección de los datos personales de una persona física requiere que se solicite el consentimiento de los usuarios finales que sean personas físicas antes de introducir sus datos personales en una guía. El interés legítimo de las personas jurídicas exige que los usuarios finales que sean entidades jurídicas tengan derecho a oponerse a la introducción de datos que les conciernan en una guía.

(31) Si los usuarios finales que sean personas físicas dan su consentimiento para que se incluyan sus datos en una guía, les ha de ser posible determinar sobre la base del consentimiento las categorías de datos personales que deben figurar en la guía (por ejemplo, nombre y apellidos, dirección de correo electrónico, dirección postal, nombre de usuario o número de teléfono). Además, los proveedores de guías accesibles al público deben informar a los usuarios finales de la finalidad de la guía y de sus funciones de búsqueda antes de incluirlos en ella. Los usuarios finales han de poder determinar mediante consentimiento las categorías de datos personales que pueden servir de base para buscar sus datos de contacto. Las categorías de los datos personales que figuren en la guía y las categorías de datos personales a partir de las que pueden buscarse los datos de contacto del usuario final no deben ser necesariamente las mismas.

(32) En el presente Reglamento se entiende por «mercadotecnia directa» cualquier forma de publicidad mediante la cual una persona física o jurídica envía comunicaciones comerciales directas a uno o varios usuarios finales identificados o identificables empleando servicios de comunicaciones electrónicas. Además de la oferta de productos y servicios con fines comerciales, esta actividad ha de incluir también los mensajes enviados por los partidos políticos que se ponen en contacto con las personas físicas a través de servicios de comunicaciones electrónicas con fines de propaganda política. También ha de abarcar los mensajes enviados por otras organizaciones sin ánimo de lucro para apoyar los objetivos de la organización.

(33) Deben ofrecerse garantías para proteger a los usuarios finales de las comunicaciones no solicitadas que se les envían con fines de mercadotecnia directa y constituyen una intromisión en su vida privada. El grado de intromisión en la vida privada y molestia se considera relativamente similar, independientemente de la amplia gama de

tecnologías y canales utilizados para efectuar esas comunicaciones electrónicas, bien mediante sistemas automatizados de llamada y comunicación, bien mediante aplicaciones de mensajería instantánea, correo electrónico, SMS, MMS, *Bluetooth*, etc. Está justificado por tanto exigir que se obtenga el consentimiento del usuario final antes de enviarle comunicaciones electrónicas comerciales con fines de mercadotecnia directa a fin de proteger eficazmente a las personas de la intromisión en su vida privada, así como de garantizar los intereses legítimos de las personas jurídicas. La seguridad jurídica y la pertinencia futura de las normas de protección frente a las comunicaciones electrónicas no solicitadas justifican la necesidad de establecer un conjunto único de normas que no varíen en función de la tecnología utilizada para transmitir esas comunicaciones no solicitadas, garantizando al mismo tiempo un nivel de protección equivalente a todos los ciudadanos de la Unión. Con todo, es razonable autorizar el uso de los datos de contacto de correo electrónico en el contexto de una relación preexistente con el cliente para ofrecerle productos o servicios similares. Esta posibilidad solo debería aplicarse a la misma empresa que haya obtenido los datos de contacto electrónicos de conformidad con el Reglamento (UE) 2016/679.

(34) Los usuarios finales que hayan consentido en recibir comunicaciones no solicitadas con fines de mercadotecnia directa han de poder retirar fácilmente su consentimiento en cualquier momento. Para facilitar la aplicación efectiva de las normas de la Unión en materia de mensajes de mercadotecnia directa no solicitados, es preciso prohibir 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 directa. Las comunicaciones comerciales no solicitadas deben ser por tanto claramente identificables como tales e indicar la identidad de la persona física o jurídica que transmite o en cuyo nombre se transmite la comunicación, y proporcionar la información necesaria para que los destinatarios puedan ejercer su derecho a oponerse a recibir nuevos mensajes comerciales escritos u orales.

(35) A fin de facilitar la retirada del consentimiento, las personas físicas o jurídicas que realizan comunicaciones de mercadotecnia directa por correo electrónico deben presentar un enlace o una dirección de correo electrónico válida que puedan utilizar fácilmente los usuarios finales para retirar su consentimiento. Las personas físicas o jurídicas que realizan comunicaciones de mercadotecnia directa a través de llamadas de voz a voz o llamadas mediante sistemas automatizados de llamada y comunicación deben mostrar la identificación de la línea de contacto de la empresa o presentar un código específico que indique que se trata de una llamada comercial.

(36) Las llamadas de voz a voz con fines de mercadotecnia directa que no entrañan la utilización de sistemas automatizados de llamada y comunicación resultan más onerosas para quienes las hacen y no imponen cargas financieras a los usuarios finales. Por consiguiente, conviene que los Estados miembros puedan establecer o mantener sistemas nacionales que únicamente autoricen las llamadas de este tipo a los usuarios finales que no se hayan opuesto a ellas.

(37) Es oportuno que los proveedores de servicios que ofrecen servicios de comunicaciones electrónicas informen a los usuarios finales de las medidas que pueden adoptar para proteger la seguridad de sus comunicaciones, por ejemplo utilizando determinados tipos de programas o técnicas de cifrado. La exigencia de informar a los usuarios finales de riesgos de seguridad particulares no exime al proveedor del servicio de la obligación de tomar a sus expensas medidas inmediatas y adecuadas para hacer frente

a cualesquiera riesgos nuevos e imprevistos de seguridad y restablecer el nivel normal de seguridad del servicio. La información sobre riesgos de seguridad ha de proporcionarse al abonado final de forma gratuita. La seguridad ha de evaluarse a luz de lo dispuesto en el artículo 32 del Reglamento (UE) 2016/679.

(38) Para garantizar la plena coherencia con el Reglamento (UE) 2016/679, la aplicación de las disposiciones del presente Reglamento y el control de su cumplimiento deben confiarse a las mismas autoridades encargadas de velar por el cumplimiento de las disposiciones del Reglamento (UE) 2016/679. El presente Reglamento se basa en el mecanismo de coherencia del Reglamento (UE) 2016/679. Los Estados miembros deben tener la posibilidad de contar con más de una autoridad de control a fin de reflejar su estructura constitucional, organizativa y administrativa. Las autoridades de control también han de encargarse de supervisar la aplicación del presente Reglamento por lo que se refiere a los datos de comunicaciones electrónicas en relación con las personas jurídicas. Estas tareas adicionales no deben comprometer la capacidad de la autoridad de control de desempeñar sus tareas en materia de protección de los datos personales en el marco del Reglamento (UE) 2016/679 y del presente Reglamento. 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 presente Reglamento.

(39) Cada autoridad de control debe ser competente en el territorio de su propio Estado miembro para ejercer las competencias y desempeñar las tareas que se establecen en el presente Reglamento. A fin de garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben ejercer las mismas tareas y competencias efectivas en cada Estado miembro, sin perjuicio de las atribuciones del ministerio fiscal con arreglo a la legislación del Estado miembro, para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales. Se exhorta a los Estados miembros y a sus autoridades de control a tomar en consideración las necesidades específicas de las microempresas y las pequeñas y medianas empresas a la hora de aplicar el presente Reglamento.

(40) Al objeto de reforzar la aplicación de las normas del presente Reglamento, cada autoridad de control debe estar facultada para imponer sanciones, entre ellas multas administrativas, por cualquier infracción del presente Reglamento, además de otras medidas apropiadas de conformidad con el presente Reglamento o en lugar de ellas. El presente Reglamento debe indicar las infracciones y el límite máximo y criterios para fijar las correspondientes multas administrativas, que la autoridad de control competente debe determinar en cada caso concreto teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o atenuar las consecuencias de la infracción. A los efectos de la imposición de una multa con arreglo al presente Reglamento, una empresa debe entenderse como una empresa con arreglo a los artículos 101 y 102 del Tratado.

(41) A fin de cumplir los objetivos del presente Reglamento, a saber, proteger los derechos y las libertades fundamentales de las personas físicas, y en particular su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos personales en la Unión, debe delegarse en la Comisión el poder de adoptar actos de

conformidad con el artículo 290 del Tratado para completar el presente Reglamento. En particular, conviene adoptar actos delegados en relación con la información que se ha de presentar, en particular mediante iconos normalizados que ofrezcan un panorama general visible e inteligible de la recogida de la información emitida por los equipos terminales, su finalidad, las personas responsables y cualquier medida que el usuario final del equipo terminal puede adoptar para reducir al mínimo dicha recogida. También son necesarios actos delegados para determinar un código que identifique las llamadas de mercadotecnia directa, entre ellas las efectuadas mediante sistemas automatizados de llamada y comunicación. Reviste especial importancia que la Comisión realice las consultas apropiadas y que estas se lleven a cabo de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación, de 13 de abril de 2016[8]. En particular, a fin de garantizar una participación equitativa en la preparación de los actos delegados, el Parlamento Europeo y el Consejo deben recibir toda la documentación al mismo tiempo que los expertos de los Estados miembros, y sus expertos han de tener acceso sistemáticamente a las reuniones de los grupos de expertos de la Comisión que se ocupen de la preparación de actos delegados. Además, a fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011.

(42) Dado que el objetivo del presente Reglamento, a saber, garantizar un nivel equivalente de protección de las personas físicas y jurídicas y la libre circulación de datos de comunicaciones electrónicas en la Unión, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones o los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(43) Procede derogar la Directiva 2002/58/CE.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

[8] Acuerdo interinstitucional entre el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea sobre la mejora de la legislación, de 13 de abril de 2016 (DO L 123 de 12.5.2016, pp. 1-14).

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1
Objeto

1. El presente Reglamento establece normas relativas a la protección de los derechos y las libertades fundamentales de las personas físicas y jurídicas en el ámbito de la prestación y utilización de servicios de comunicaciones electrónicas y, en particular, los derechos al respeto de la vida privada y las comunicaciones y la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

2. El presente Reglamento garantiza la libre circulación de datos de comunicaciones electrónicas y servicios de comunicaciones electrónicas en la Unión, que no será posible restringir ni prohibir por motivos relacionados con el respeto de la vida privada y las comunicaciones de las personas físicas y jurídicas y la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

3. Las disposiciones del presente Reglamento precisan y complementan las del Reglamento (UE) 2016/679 estableciendo normas específicas a los efectos mencionados en los apartados 1 y 2.

Artículo 2
Ámbito de aplicación material

1. El presente Reglamento será aplicable al tratamiento de datos de comunicaciones electrónicas llevado a cabo en relación con la prestación y utilización de servicios de comunicaciones electrónicas, así como a la información relacionada con los equipos terminales de los usuarios finales.

2. El presente Reglamento no será aplicable:

a) a las actividades excluidas del ámbito del Derecho de la Unión;

b) a las actividades de los Estados miembros comprendidas en el ámbito de aplicación del título V, capítulo 2, del Tratado de la Unión Europea;

c) a los servicios de comunicaciones electrónicas no accesibles al público;

d) a las actividades llevadas a cabo por las autoridades competentes a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección y prevención frente a amenazas para la seguridad pública.

3. El tratamiento de datos de comunicaciones electrónicas por parte de las instituciones, órganos y organismos de la Unión se regirá por el Reglamento (UE) 00/0000 [nuevo Reglamento que sustituye al Reglamento (CE) n.º 45/2001]

4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE[9], y en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios establecidas en los artículos 15 a 12 de dicha Directiva.

5. El presente Reglamento no afectará a la aplicación de las disposiciones de la Directiva 2014/53/UE.

Artículo 3
Ámbito de aplicación territorial y representante

1. El presente Reglamento será aplicable:

a) a la prestación de servicios de comunicaciones electrónicas a los usuarios finales en la Unión, independientemente de si el usuario final tiene que pagar por ellos;

b) a la utilización de dichos servicios;

c) a la protección de la información relativa a los equipos terminales de los usuarios finales situados en la Unión.

2. 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.

3. El representante estará establecido en uno de los Estados miembros en que estén situados los usuarios finales de esos servicios de comunicaciones electrónicas.

4. El representante estará facultado para responder a preguntas y facilitar información que complemente o supla la del proveedor al que representa, en particular a las autoridades de control y los usuarios finales, sobre todos los asuntos relativos al tratamiento de datos de comunicaciones electrónicas a fin de garantizar el cumplimiento del presente Reglamento.

5. La designación de un representante con arreglo a lo dispuesto en el apartado 2 se entenderá sin perjuicio de las acciones legales que puedan emprenderse contra una persona física o jurídica que trate datos de comunicaciones electrónicas en relación con la prestación de servicios de comunicaciones electrónicas desde fuera de la Unión a usuarios finales de la Unión.

[9] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, pp. 1-16).

Artículo 4
Definiciones

1. A los efectos del presente Reglamento, serán aplicables las siguientes definiciones:

a) las definiciones recogidas en el Reglamento (UE) 2016/679;

b) las definiciones de «red de comunicaciones electrónicas», «servicio de comunicaciones electrónicas», «servicio de comunicaciones interpersonales», «servicio de comunicaciones interpersonales basado en números», «servicio de comunicaciones interpersonales independiente de los números», «usuario final» y «llamada» que figuran en el artículo 2, puntos 1, 4, 5, 6, 7, 14 y 21, de la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas];

c) la definición de «equipo terminal» que figura en el artículo 1, punto 1, de la Directiva 2008/63/CE de la Comisión[10].

2. A los efectos del apartado 1, letra b), la definición de «servicio de comunicaciones interpersonales» englobará los servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio.

3. Además, a los efectos del presente Reglamento se entenderá por:

a) «datos de comunicaciones electrónicas»: el contenido de las comunicaciones electrónicas y los metadatos de las comunicaciones electrónicas;

b) «contenido de comunicaciones electrónicas»: el contenido intercambiado por medio de servicios de comunicaciones electrónicas, como texto, voz, vídeos, imágenes y sonidos;

c) «metadatos de comunicaciones electrónicas»: datos tratados en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas; se incluyen los datos utilizados para rastrear e identificar el origen y el destino de una comunicación, los datos sobre la ubicación del dispositivo generados en el contexto de la prestación de servicios de comunicaciones electrónicas, así como la fecha, la hora, la duración y el tipo de comunicación;

d) «guía accesible al público»: una guía de usuarios finales de servicios de comunicaciones electrónicas en formato impreso o electrónico que se publica o se pone a disposición del público o de una parte del público, entre otros medios a través de un servicio de información;

e) «correo electrónico»: todo mensaje electrónico que contenga información como texto, voz, vídeos, sonidos o imágenes enviado a través de una red de comunicaciones electrónicas y que pueda almacenarse en la red, en instalaciones informáticas asociadas, o en el equipo terminal del destinatario;

[10] Directiva 2008/63/CE de la Comisión, de 20 de junio de 2008, relativa a la competencia en los mercados de equipos terminales de telecomunicaciones (DO L 162 de 21.6.2008, pp. 20-26).

f) «comunicaciones de mercadotecnia directa»: toda forma de publicidad oral o escrita enviada a uno o varios usuarios finales identificados o identificables de servicios de comunicaciones electrónicas, incluyendo la utilización de sistemas automatizados de llamada y comunicación con interacción humana o sin ella, correo electrónico, SMS, etc.;

g) «llamadas de voz a voz con fines de mercadotecnia directa»: llamadas en vivo que no comportan la utilización de sistemas automatizados de llamada y comunicación;

h) «sistemas automatizados de llamada y comunicación»: sistemas que pueden iniciar automáticamente llamadas a uno o más destinatarios de acuerdo con las instrucciones establecidas y transmitir sonidos no emitidos en directo, incluidas las llamadas efectuadas mediante sistemas automatizados de llamada y comunicación que conectan a la persona llamada a otra persona.

CAPÍTULO II
PROTECCIÓN DE LAS COMUNICACIONES ELECTRÓNICAS DE LAS PERSONAS FÍSICAS Y JURÍDICAS Y DE LA INFORMACIÓN ALMACENADA EN SUS EQUIPOS TERMINALES

Artículo 5
Confidencialidad de los datos de comunicaciones electrónicas

Los datos de comunicaciones electrónicas serán confidenciales. Salvo cuando lo autorice el presente Reglamento, estará prohibida cualquier interferencia con datos de comunicaciones electrónicas como, por ejemplo, la escucha, el pinchado, el almacenamiento, el seguimiento, el análisis u otros tipos de interceptación, vigilancia o tratamiento de datos de comunicaciones electrónicas, por parte de personas distintas de los usuarios finales.

Artículo 6
Tratamiento autorizado de datos de comunicaciones electrónicas

1. Los proveedores de redes y servicios de comunicaciones electrónicas podrán tratar datos de comunicaciones electrónicas:

a) cuando sea necesario para transmitir la comunicación, y ello durante el período necesario para ese fin, o

b) cuando sea necesario para mantener o restablecer la seguridad de las redes y servicios de comunicaciones electrónicas, o detectar fallos o errores técnicos en la transmisión de las comunicaciones electrónicas, y ello durante el período necesario para ese fin.

2. Los proveedores de servicios de comunicaciones electrónicas podrán tratar metadatos de comunicaciones electrónicas:

c) cuando sea necesario para cumplir las obligaciones en materia de calidad del servicio con arreglo a la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas] o al Reglamento (UE) 2015/2120[11] durante el período necesario para ese fin, o

d) cuando sea necesario para proceder a la facturación, calcular las tarifas de interconexión, detectar o impedir la utilización abusiva o fraudulenta de los servicios de comunicaciones electrónica o abonarse a ellos, o

e) cuando el usuario final haya dado su consentimiento para el tratamiento de sus metadatos de comunicaciones para uno o más fines concretos, entre ellos la prestación de servicios específicos a ese usuario final, siempre que el fin o los fines de que se trate no puedan alcanzarse mediante el tratamiento de información anonimizada.

3. Los proveedores de servicios de comunicaciones electrónicas únicamente podrán tratar contenido de comunicaciones electrónicas:

a) con el fin exclusivo de prestar un servicio específico a un usuario final, siempre que el usuario final o los usuarios finales interesados hayan dado su consentimiento para el tratamiento del contenido de sus comunicaciones electrónicas y la prestación de dicho servicio no pueda llevarse a cabo sin el tratamiento de ese contenido, o

b) cuando todos los usuarios finales interesados hayan dado su consentimiento para el tratamiento del contenido de sus comunicaciones electrónicas con uno o más fines específicos que no puedan alcanzarse mediante el tratamiento de información anonimizada, y el proveedor haya consultado a la autoridad de control. El artículo 36, puntos 2 y 3, del Reglamento (UE) 2016/679 será aplicable a la consulta de la autoridad de control.

Artículo 7
Almacenamiento y supresión de datos de comunicaciones electrónicas

1. Sin perjuicio de lo dispuesto en el artículo 6, apartado 1, letra b), y en el artículo 6, apartado 3, letras a) y b), el proveedor del servicio de comunicaciones electrónicas suprimirá el contenido de las comunicaciones electrónicas o anonimizará esos datos una vez los hayan recibido el destinatario o destinatarios previstos. Tales datos podrán ser registrados o almacenados por los usuarios finales o por un tercero encargado por ellos de registrar, almacenar o tratar de cualquier otra forma los datos, de conformidad con el Reglamento (UE) 2016/679.

2. Sin perjuicio de lo dispuesto en el artículo 6, apartado 1, letra b), y en el artículo 6, apartado 2, letras a) y b), el proveedor del servicio de comunicaciones electrónicas suprimirá los metadatos de comunicaciones electrónicas o los anonimizará cuando ya no sean necesarios para transmitir una comunicación.

[11] Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, por el que se establecen medidas en relación con el acceso a una internet abierta y se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (UE) n.º 531/2012 relativo a la itinerancia en las redes públicas de comunicaciones móviles en la Unión (DO L 310 de 26.11.2015, pp. 1-18).

3. Cuando el tratamiento de metadatos de comunicaciones electrónicas se lleve a cabo a efectos de facturación de conformidad con el artículo 6, apartado 2, letra b), los metadatos correspondientes podrán conservarse hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse su pago con arreglo a la legislación nacional.

Artículo 8
Protección de la información almacenada en los equipos terminales de los usuarios finales y relativa a dichos equipos

1. El uso de las capacidades de tratamiento y almacenamiento de los equipos terminales y la recopilación de información del equipo terminal de los usuarios finales, incluida la relativa a su soporte físico y lógico, excepto por parte del usuario final, estarán prohibidos, salvo por los motivos siguientes:

a) cuando sean necesarios con el fin exclusivo de efectuar la transmisión de una comunicación electrónica a través de una red de comunicaciones electrónicas, o

b) cuando el usuario final haya dado su consentimiento, o

c) cuando sean necesarios para la prestación de un servicio de la sociedad de la información solicitado por el usuario final, o

d) cuando sean necesarios para medir la audiencia en la web, siempre que esa medición corra a cargo del proveedor del servicio de la sociedad de la información solicitado por el usuario final.

2. Estará prohibido recopilar la información emitida por un equipo terminal para poder conectarse a otro dispositivo o a un equipo de red, excepto en los siguientes casos:

a) cuando se lleve a cabo con el fin exclusivo de establecer una conexión y solamente durante el tiempo necesario para ello, o

b) cuando se muestre una advertencia clara y destacada que informe, como mínimo, de las modalidades de recopilación, su finalidad, las personas responsables de ella y la información restante requerida de conformidad con el artículo 13 del Reglamento (UE) 2016/679 en caso de que se recojan datos personales, así como de cualquier medida que pueda adoptar el usuario final del equipo terminal para interrumpir o reducir al mínimo la recopilación.

La recopilación de esta información quedará supeditada a la aplicación de medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado en relación con los riesgos, según lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

3. La información que debe facilitarse con arreglo al apartado 2, letra b), podrá proporcionarse en combinación con el uso de iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto.

4. Se otorgan a la Comisión poderes para adoptar actos delegados de conformidad con el artículo 27 en los que se determine la información que se ha de presentar mediante iconos normalizados y los procedimientos para suministrar dichos iconos.

Artículo 9
Consentimiento

1. Serán aplicables la definición y las condiciones relativas al consentimiento previstas en el artículo 4, punto 11, y en el artículo 7 del Reglamento (UE) 2016/679.

2. Sin perjuicio de lo dispuesto en el apartado 1, cuando sea técnicamente posible y factible, a los efectos del artículo 8, apartado 1, letra b), el consentimiento podrá expresarse mediante la configuración técnica adecuada de una aplicación informática que permita acceder a Internet.

3. Los usuarios finales que hayan dado su consentimiento para el tratamiento de datos de comunicaciones electrónicas con arreglo al artículo 6, apartado 2, letra c), y al artículo 6, apartado 3, letras a) y b), dispondrán de la posibilidad de retirar su consentimiento en cualquier momento, según lo dispuesto en el artículo 7, apartado 3, del Reglamento (UE) 2016/679, y se les recordará esta posibilidad a intervalos regulares de seis meses mientras continúe el tratamiento.

Artículo 10
Información y opciones de configuración de privacidad que han de proporcionarse

1. Los programas informáticos comercializados que permiten comunicaciones electrónicas, incluyendo la recuperación y presentación de información de Internet, ofrecerán la posibilidad de impedir a terceros almacenar información sobre el equipo terminal de un usuario final o el tratamiento de información ya almacenada en ese equipo.

2. Al iniciarse la instalación, los programas deberán informar a los usuarios finales acerca de las opciones de configuración de confidencialidad y, para que pueda proseguir la instalación, solicitar el consentimiento del usuario final respecto de una configuración determinada.

3. En el caso de los programas que ya se hayan instalado el 25 de mayo de 2018, los requisitos establecidos en los apartados 1 y 2 deberán cumplirse en el momento de la primera actualización de los programas, pero no más tarde del 25 de agosto de 2018.

Artículo 11
Limitaciones

1. El Derecho de la Unión o de un Estado miembro podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y los derechos previstos en los artículos 5 a 8, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria, adecuada y proporcionada en una sociedad democrática para salvaguardar uno o varios de los intereses públicos generales contemplados en el artículo 23, apartado 1, letras a) a e), del Reglamento

(UE) 2016/679 o una función de control, inspección o reglamentación vinculada al ejercicio de la autoridad pública en aras de tales intereses.

2. Los proveedores de servicios de comunicaciones electrónicas establecerán procedimientos internos para responder a las solicitudes de acceso a los datos de las comunicaciones electrónicas de los usuarios finales sobre la base de una medida legislativa adoptada de conformidad con el apartado 1. Previa solicitud, facilitarán a las autoridades de control competentes información sobre esos procedimientos, el número de solicitudes recibidas, la motivación jurídica aducida y la respuesta ofrecida.

CAPÍTULO III
DERECHOS DE LAS PERSONAS FÍSICAS Y JURÍDICAS EN RELACIÓN CON EL CONTROL DE LAS COMUNICACIONES ELECTRÓNICAS

Artículo 12
Presentación y restricción de la identificación de la línea llamante y la línea conectada

1. Cuando la presentación de la identificación de la línea llamante y la línea conectada se ofrezca de conformidad con el artículo [107] de la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas], los proveedores de servicios de comunicaciones interpersonales basados en números y disponibles al público deberán ofrecer lo siguiente:

a) al usuario final llamante, la posibilidad de impedir la presentación de la identificación de la línea llamante por llamada, por conexión o de forma permanente;

b) al usuario final llamado, la posibilidad de impedir la presentación de la identificación de la línea llamante de las llamadas entrantes;

c) al usuario final llamado, la posibilidad de rechazar las llamadas entrantes cuando el usuario final llamante haya impedido la presentación de la identificación de la línea llamante;

d) al usuario final llamado, la posibilidad de impedir la presentación de la identificación de la línea conectada al usuario final llamante.

2. Las posibilidades contempladas en el apartado 1, letras a), b), c) y d), se ofrecerán los usuarios finales por medios sencillos y de forma gratuita.

3. El apartado 1, letra a), será también aplicable a las llamadas efectuadas desde la Unión a terceros países. El apartado 1, letras b), c) y d), será también aplicable a las llamadas entrantes procedentes de terceros países.

4. Cuando se ofrezca la posibilidad de presentar la identificación de la línea llamante o la línea conectada, los proveedores de servicios de comunicaciones interpersonales basados en números y disponibles al público facilitarán información al público acerca de las opciones establecidas en el apartado 1, letras a), b), c) y d).

Artículo 13
Excepciones respecto de la presentación y restricción de la identificación de la línea llamante y la línea conectada

1. Independientemente de que el usuario final llamante haya impedido la presentación de la identificación de la línea llamante, cuando se efectúe una llamada a los servicios de emergencia, los proveedores de servicios de comunicaciones interpersonales basados en números y disponibles al público no tendrán en cuenta la supresión de la presentación de la identificación de la línea llamante y el rechazo o la ausencia de consentimiento del usuario final en relación con el tratamiento de metadatos, de manera selectiva por línea con respecto a las organizaciones que se ocupan de comunicaciones de emergencia, incluidos los puntos de respuesta de seguridad pública, para responder a esa comunicación.

2. Los Estados miembros establecerán disposiciones más específicas en lo que se refiere al establecimiento de procedimientos y a las circunstancias en que los proveedores de servicios de comunicaciones interpersonales basados en números y disponibles al público podrán pasar por alto la supresión de la presentación de la identificación de la línea llamante por un período de tiempo limitado cuando los usuarios finales soliciten la identificación de llamadas malintencionadas o molestas.

Artículo 14
Bloqueo de llamadas entrantes

Los proveedores de servicios de comunicaciones interpersonales basados en números y disponibles al público aplicarán las medidas más avanzadas para limitar la recepción de llamadas no deseadas por los usuarios finales y ofrecerán también al usuario final llamado las siguientes posibilidades de forma gratuita:

a) bloquear las llamadas entrantes de determinados números o de fuentes anónimas;

b) detener las llamadas desviadas automáticamente por un tercero al equipo terminal del usuario final.

Artículo 15
Guías accesibles al público

1. Los proveedores de guías accesibles al público deberán obtener el consentimiento de los usuarios finales que sean personas físicas para incluir sus datos personales en la guía y, consiguientemente, deberán obtener el consentimiento de esos usuarios finales para incluir datos por categorías de datos personales en la medida en que tales datos sean pertinentes para la finalidad de la guía, según lo determinado por el proveedor de la misma. Los proveedores deberán facilitar a los usuarios finales que sean personas físicas los medios para comprobar, corregir o suprimir esos datos.

2. Los proveedores de guías accesibles al público deberán informar a los usuarios finales que sean personas físicas y cuyos datos personales figuren en la guía de las funciones de búsqueda de que esta dispone y obtener el consentimiento de los usuarios finales antes de habilitar esas funciones de búsqueda en relación con sus propios datos.

3. Los proveedores de guías accesibles al público ofrecerán a los usuarios finales que sean personas jurídicas la posibilidad de oponerse a la introducción de sus datos en la guía. Los proveedores deberán facilitar a los usuarios finales que sean personas jurídicas los medios para comprobar, corregir o suprimir esos datos.

4. Se ofrecerá gratuitamente a los usuarios finales la posibilidad de no figurar en una guía accesible al público, así como de comprobar, corregir o suprimir los datos que les conciernan.

Artículo 16
Comunicaciones no solicitadas

1. Las personas físicas o jurídicas podrán utilizar servicios de comunicaciones electrónicas para el envío de comunicaciones de mercadotecnia directa a los usuarios finales que sean personas físicas y hayan dado su consentimiento.

2. Cuando una persona física o jurídica obtenga los datos de contacto electrónicos de su cliente en el contexto de la venta de un producto o servicio, de conformidad con el Reglamento (UE) 2016/679, dicha persona física o jurídica únicamente podrá utilizar esos datos de contacto para la comercialización directa de sus propios productos o servicios similares cuando ofrezca de manera clara y precisa a los clientes la oportunidad de oponerse de manera sencilla y gratuita a esa utilización. El derecho de oposición se concederá en el momento de la recopilación y cada vez que se envíe un mensaje.

3. Sin perjuicio de lo dispuesto en los apartados 1 y 2, las personas físicas o jurídicas que utilicen servicios de comunicaciones electrónicas para efectuar llamadas de mercadotecnia directa deberán:

a) presentar la identificación de una línea en la que se les pueda contactar, o

b) presentar un código o prefijo específico que permita identificar que se trata de una llamada de mercadotecnia.

4. No obstante lo dispuesto en el apartado 1, los Estados miembros podrán establecer en su legislación que la realización de llamadas de voz a voz con fines de mercadotecnia directa a usuarios finales que sean personas físicas solo quede autorizada con respecto a los usuarios finales que sean personas físicas y no hayan expresado su oposición a recibir tales comunicaciones.

5. Los Estados miembros velarán por que, en el marco del Derecho de la Unión y la legislación nacional aplicable, el interés legítimo de los usuarios finales que sean personas jurídicas esté suficientemente protegido en lo que se refiere a las comunicaciones no solicitadas enviadas por los medios contemplados en el apartado 1.

6. Toda persona física o jurídica que utilice servicios de comunicaciones electrónicas para transmitir comunicaciones de mercadotecnia directa deberá informar a los usuarios finales del carácter comercial de la comunicación y de la identidad de la persona física o jurídica en nombre de la cual se transmite la comunicación, y proporcionará la información necesaria a los destinatarios para que estos puedan

ejercer fácilmente su derecho a retirar su consentimiento para no recibir nuevas comunicaciones de mercadotecnia.

7. Se otorgarán poderes a la Comisión para adoptar medidas de ejecución de conformidad con el artículo 26, apartado 2, por las que se especifique el código o prefijo que ha de utilizarse para identificar las llamadas de mercadotecnia, con arreglo al apartado 3, letra b).

Artículo 17
Información sobre los riesgos de seguridad detectados

En caso de que exista un riesgo concreto que pueda comprometer la seguridad de las redes y los servicios de comunicaciones electrónicas, el proveedor del servicio de comunicaciones electrónicas de que se trate informará a los usuarios finales de dicho riesgo y, cuando este quede fuera del ámbito de las medidas que debe adoptar el proveedor de servicios, informará a los usuarios finales de las posibles soluciones, con una indicación de los posibles costes.

CAPÍTULO IV
AUTORIDADES DE CONTROL INDEPENDIENTES Y EJECUCIÓN

Artículo 18
Autoridades de control independientes

1. La autoridad o las autoridades de control independientes encargadas de supervisar la aplicación del Reglamento (UE) 2016/679 también serán responsables de supervisar la aplicación del presente Reglamento. Serán de aplicación, *mutatis mutandis*, los capítulos VI y VII del Reglamento (CE) 2016/679. Las funciones y competencias de las autoridades de control se ejercerán con respecto a los usuarios finales.

2. La autoridad o las autoridades de control a que se refiere el apartado 1 cooperarán, cuando proceda, con las autoridades nacionales de reglamentación establecidas con arreglo a la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas].

Artículo 19
Comité Europeo de Protección de Datos

El Comité Europeo de Protección de Datos, creado en virtud del artículo 68 del Reglamento (UE) 2016/679, dispondrá de competencias para garantizar la aplicación coherente del presente Reglamento. A tal efecto, el Comité Europeo de Protección de Datos ejercerá las funciones previstas en el artículo 70 del Reglamento (UE) 2016/679. El Comité también desempeñará las siguientes funciones:

a) asesorar a la Comisión sobre cualquier propuesta de modificación del presente Reglamento;

b) examinar, por iniciativa propia, a instancias de uno de sus miembros o a petición de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, y elaborar directrices, recomendaciones y mejores prácticas a fin de fomentar la aplicación coherente del presente Reglamento.

Artículo 20
Mecanismos de cooperación y coherencia

Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII del Reglamento (UE) 2016/679 en relación con los asuntos regulados por el presente Reglamento.

CAPÍTULO V
RECURSOS, RESPONSABILIDAD Y SANCIONES

Artículo 21
Vías de recurso

1. Sin perjuicio de cualquier otra vía de recurso administrativa o judicial, todos los usuarios finales de servicios de comunicaciones electrónicas dispondrán de las mismas vías de recurso previstas en los artículos 77, 78 y 79 del Reglamento (UE) 2016/679.

2. Cualquier persona física o jurídica distinta de los usuarios finales que se vea perjudicada por infracciones de las disposiciones del presente Reglamento y tenga un interés legítimo en que cesen o se prohíban las presuntas infracciones, incluidos los proveedores de servicios de comunicaciones electrónicas que protejan sus intereses comerciales legítimos, tendrá derecho a ejercitar una acción judicial con respecto a tales infracciones.

Artículo 22
Derecho a indemnización y responsabilidad

Todos los usuarios finales de servicios de comunicaciones electrónicas que hayan sufrido perjuicios materiales o morales como consecuencia de una infracción del presente Reglamento tendrán derecho a recibir una indemnización del infractor por los perjuicios sufridos, a menos que el infractor demuestre que no es en modo alguno responsable del hecho que haya dado lugar al perjuicio de conformidad con el artículo 82 del Reglamento (UE) 2016/679.

Artículo 23
Condiciones generales para la imposición de multas administrativas

1. A los efectos del presente artículo, se aplicará el capítulo VII del Reglamento (UE) 2016/679 a las infracciones del presente Reglamento.

2. Las infracciones de las disposiciones del presente Reglamento que se enumeran a continuación se sancionarán, de conformidad con el apartado 1, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocios anual total a escala mundial del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) obligaciones de una persona jurídica o física que efectúe el tratamiento de datos de comunicaciones electrónicas de conformidad con el artículo 8;

b) obligaciones del proveedor de programas informáticos que permitan las comunicaciones electrónicas de conformidad con el artículo 10;

c) obligaciones de los proveedores de guías accesibles al público de conformidad con el artículo 15;

d) obligaciones de una persona jurídica o física que utilice servicios de comunicaciones electrónicas de conformidad con el artículo 16.

3. Las infracciones del principio de confidencialidad de las comunicaciones, del tratamiento autorizado de datos de comunicaciones electrónicas y de los plazos de supresión previstos en los artículos 5, 6 y 7 se sancionarán, de conformidad con el apartado 1 del presente artículo, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocios anual total a escala mundial del ejercicio financiero anterior, optándose por la de mayor cuantía.

4. Los Estados miembros establecerán normas sobre las sanciones aplicables a las infracciones de lo dispuesto en los artículos 12, 13, 14 y 17.

5. El incumplimiento de una orden de una autoridad de control a que se refiere el artículo 18 se sancionará con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocios anual total a escala mundial del ejercicio financiero anterior, optándose por la de mayor cuantía.

6. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 18, cada Estado miembro podrá establecer normas que determinen si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en ese Estado miembro.

7. El ejercicio por una autoridad de control de los poderes que le otorga el presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

8. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate

notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el [xxx] y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 24
Sanciones

1. Los Estados miembros establecerán normas sobre las demás sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 23, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1, a más tardar 18 meses después de la fecha especificada en el artículo 29, apartado 2, y, sin demora, cualquier modificación posterior de las mismas.

CAPÍTULO VI
ACTOS DELEGADOS Y ACTOS DE EJECUCIÓN

Artículo 25
Ejercicio de la delegación

1. Se otorgan a la Comisión los poderes para adoptar actos delegados en las condiciones establecidas en el presente artículo.

2. Los poderes para adoptar los actos delegados a que se refiere el artículo 8, apartado 4, se otorgarán a la Comisión por un período de tiempo indefinido a partir de [la fecha de entrada en vigor del presente Reglamento].

3. La delegación de poderes mencionada en el artículo 8, apartado 4, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La Decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La Decisión surtirá efecto al día siguiente de su publicación en el *Diario Oficial de la Unión Europea* o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Antes de la adopción de un acto delegado, la Comisión consultará a los expertos designados por cada Estado miembro de conformidad con los principios establecidos en el Acuerdo interinstitucional sobre la mejora de la legislación, de 13 de abril de 2016.

5. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

6. Los actos delegados adoptados en virtud del artículo 8, apartado 4, entrarán en vigor únicamente si, en un plazo de dos meses desde su notificación al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o

si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. El plazo se prorrogará dos meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 26
Comité

1. La Comisión estará asistida por el Comité de Comunicaciones creado en virtud del artículo 110 de la [Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas]. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011[12].

2. En los casos en que se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.

CAPÍTULO VII
DISPOSICIONES FINALES

Artículo 27
Derogación

1. Queda derogada la Directiva 2002/58/CE con efecto a partir del 25 de mayo de 2018.

2. Las referencias a la Directiva derogada se entenderán hechas al presente Reglamento.

Artículo 28
Cláusula de seguimiento y evaluación

A más tardar el 1 de enero de 2018, la Comisión elaborará un programa detallado para el seguimiento de la eficacia del presente Reglamento.

A más tardar tres años después de la fecha de aplicación del presente Reglamento y posteriormente cada tres años, la Comisión llevará a cabo una revisión del presente Reglamento y presentará un informe con sus principales conclusiones al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo. La evaluación inspirará, en su caso, una propuesta de modificación o de derogación del presente Reglamento a la luz de la evolución jurídica, técnica o económica.

[12] Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, pp. 13-18).

Artículo 29
Entrada en vigor y aplicación

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

2. Será aplicable a partir del 25 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el

Por el Parlamento Europeo	*Por el Consejo*
El Presidente	*El Presidente*