UNIÓN EUROPEA

EL PARLAMENTO EUROPEO **EL CONSEJO**

Bruselas, 14 de julio de 2021
(OR. en)

2020/0259 (COD)
LEX 2115

PE-CONS 38/1/21
REV 1

TELECOM 213
COMPET 370
MI 361
DATAPROTECT 131
CONSOM 122
JAI 561
DIGIT 62
FREMP 138
CYBER 150
CODEC 722

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO POR EL QUE SE ESTABLECE UNA EXCEPCIÓN TEMPORAL A DETERMINADAS DISPOSICIONES DE LA DIRECTIVA 2002/58/CE EN LO QUE RESPECTA AL USO DE TECNOLOGÍAS POR PROVEEDORES DE SERVICIOS DE COMUNICACIONES INTERPERSONALES INDEPENDIENTES DE LA NUMERACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES Y DE OTRO TIPO CON FINES DE LUCHA CONTRA LOS ABUSOS SEXUALES DE MENORES EN LÍNEA

REGLAMENTO (UE) 2021/…
DEL PARLAMENTO EUROPEO Y DEL CONSEJO

de 14 de julio de 2021

por el que se establece una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE en lo que respecta al uso de tecnologías por proveedores de servicios de comunicaciones interpersonales independientes de la numeración para el tratamiento de datos personales y de otro tipo con fines de lucha contra los abusos sexuales de menores en línea

(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 su artículo 16, apartado 2, en relación con su artículo 114, apartado 1,

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],

De conformidad con el procedimiento legislativo ordinario[2],

---

1 DO C 10 de 11.1.2021, p. 63.

2 Posición del Parlamento Europeo de 6 de julio de 2021 (pendiente de publicación en el Diario Oficial) y Decisión del Consejo de 12 de julio de 2021.

Considerando lo siguiente:

(1) La Directiva 2002/58/CE del Parlamento Europeo y del Consejo[1] establece normas que garantizan el derecho a la intimidad y la confidencialidad en lo que respecta al tratamiento de datos personales en los intercambios de datos en el sector de las comunicaciones electrónicas. Dicha Directiva desarrolla y completa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo[2].

[1] 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).

[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, p. 1).

(2) La Directiva 2002/58/CE se aplica al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas puestos a disposición del público. Hasta el 21 de diciembre de 2020 era aplicable la definición de «servicio de comunicaciones electrónicas» establecida en el artículo 2, letra c), de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo[1]. En esa fecha, la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo[2] derogó la Directiva 2002/21/CE. La definición de «servicios de comunicaciones electrónicas» del artículo 2, punto 4, de la Directiva (UE) 2018/1972 incluye los servicios de comunicaciones interpersonales independientes de la numeración, tal como se definen en el artículo 2, punto 7, de dicha Directiva. Los servicios de comunicaciones interpersonales independientes de la numeración, que incluyen, por ejemplo, los servicios de voz por protocolo de Internet, la mensajería y los servicios de correo electrónico basados en la web, se incluyeron, por lo tanto, en el ámbito de aplicación de la Directiva 2002/58/CE el 21 de diciembre de 2020.

(3) De conformidad con el artículo 6, apartado 1, del Tratado de la Unión Europea, la Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, «Carta»). El artículo 7 de la Carta protege el derecho fundamental de toda persona al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones, derecho que incluye la confidencialidad de las comunicaciones. El artículo 8 de la Carta consagra el derecho a la protección de los datos de carácter personal.

---

1 Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco) (DO L 108 de 24.4.2002, p. 33).

2 Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (DO L 321 de 17.12.2018, p. 36).

(4) El artículo 3, apartado 1, de la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989 y el artículo 24, apartado 2, de la Carta establecen que, en todos los actos relativos a los niños llevados a cabo por autoridades públicas o instituciones privadas, el interés superior del niño constituirá una consideración primordial. El artículo 3, apartado 2, de la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989 y el artículo 24, apartado 1, de la Carta contemplan, además, el derecho de los niños a tales protección y cuidados necesarios para su bienestar.

(5) La protección de los menores, tanto fuera de línea como en línea, es una de las prioridades de la Unión. El abuso sexual y la explotación sexual de los menores constituyen graves violaciones de los derechos humanos y fundamentales, en particular de los derechos de los menores a ser protegidos contra cualquier forma de violencia, abuso y abandono, maltrato o explotación, incluido el abuso sexual, tal como establecen la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989 y la Carta. La digitalización ha traído consigo muchas ventajas para la sociedad y la economía, pero también ha traído consigo desafíos, como el aumento del abuso sexual de menores en línea. El 24 de julio de 2020, la Comisión adoptó una Comunicación titulada «Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores» (en lo sucesivo, «Estrategia»). La Estrategia tiene por objeto ofrecer una respuesta eficaz, a escala de la Unión, al delito de abuso sexual de menores.

(6) En consonancia con la Directiva 2011/93/UE del Parlamento Europeo y del Consejo[1], el presente Reglamento no regula las políticas de los Estados miembros con respecto a los actos sexuales consentidos en los que puedan participar menores y que pueden considerarse como el descubrimiento normal de la sexualidad en el proceso de desarrollo personal, habida cuenta de las diferentes tradiciones culturales y jurídicas y de las nuevas formas de entablar y mantener relaciones de los menores y adolescentes, incluso mediante tecnologías de la información y de las comunicaciones.

[1] Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión Marco 2004/68/JAI del Consejo (DO L 335 de 17.12.2011, p. 1).

(7) Algunos proveedores de determinados servicios de comunicaciones interpersonales independientes de la numeración (en lo sucesivo, «proveedores»), como el correo web y los servicios de mensajería, ya utilizan de forma voluntaria tecnologías específicas con el fin de detectar el abuso sexual de menores en línea cometido en sus servicios y denunciarlo a las autoridades policiales y a las organizaciones que actúan en interés público contra los abusos sexuales de menores, escaneando el contenido, incluidas imágenes y texto, o los datos de tráfico de las comunicaciones, mediante el uso, en algunos casos, de datos históricos. La tecnología utilizada para dichas actividades podría consistir en tecnología de funciones de resumen («hashing») para imágenes y vídeos, y en clasificadores e inteligencia artificial para el análisis de textos o datos de tráfico. Cuando se usa una tecnología de funciones de resumen, el material de abuso sexual de menores en línea se detecta cuando se obtiene una respuesta positiva, es decir, una coincidencia que resulta de comparar una imagen o un vídeo y una firma digital única y no reconvertible («hash») de una base de datos gestionada por una organización que actúa en interés público contra los abusos sexuales de menores y que contiene material verificado de abuso sexual de menores en línea. Dichos proveedores se remiten a líneas directas nacionales que permiten denunciar la existencia de material de abuso sexual de menores en línea y a organizaciones, establecidas ambas tanto dentro de la Unión como en terceros países, cuyo objetivo es identificar a los menores y reducir la explotación sexual y el abuso sexual de menores y prevenir la victimización de menores. Estas organizaciones podrían no estar comprendidas en el ámbito de aplicación del Reglamento (UE) 2016/679. En conjunto, este tipo de actividades voluntarias tienen un gran valor, al permitir la identificación y el rescate de las víctimas, cuyos derechos fundamentales a la dignidad humana y a la integridad física y mental han sido gravemente vulnerados. Asimismo tales actividades voluntarias tienen su importancia para reducir la difusión de material relacionado con el abuso sexual de menores, y contribuir a la identificación e investigación de los delincuentes y a la prevención, detección, investigación y enjuiciamiento de los delitos de abuso sexual de menores.

(8) A pesar de que su objetivo sea legítimo, las actividades voluntarias de los proveedores para detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos representan una injerencia en los derechos fundamentales al respeto de la vida privada y familiar y a la protección de los datos personales de todos los usuarios de servicios de comunicaciones interpersonales independientes de la numeración (en lo sucesivo, «usuarios»). Ninguna limitación del ejercicio del derecho fundamental al respeto a la vida privada y familiar, incluida la confidencialidad de las comunicaciones, puede encontrar justificación en el mero hecho de que los proveedores empleasen determinadas tecnologías en un momento en el que los servicios de comunicaciones interpersonales independientes de la numeración no estaban comprendidos en la definición de «servicios de comunicaciones electrónicas». Dichas limitaciones son posibles únicamente en determinadas circunstancias. En virtud del artículo 52, apartado 1, de la Carta, dichas limitaciones deben estar establecidas por la ley y respetar el contenido esencial de los derechos a la protección de la vida privada y familiar y a la protección de los datos personales y, dentro del respeto del principio de proporcionalidad, ser necesarias y responder efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás. Cuando tales limitaciones impliquen con carácter permanente el seguimiento y análisis general e indiscriminado del contenido de las comunicaciones de todos los usuarios, constituyen una injerencia en el derecho a la confidencialidad de las comunicaciones.

(9) Hasta el 20 de diciembre de 2020, el tratamiento de datos personales por parte de los proveedores mediante medidas voluntarias destinadas a detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y a retirar el material de abuso sexual de menores en línea de sus servicios se regía únicamente por el Reglamento (UE) 2016/679. La Directiva (UE) 2018/1972, cuyo plazo de transposición expiró el 20 de diciembre de 2020, incluyó a los proveedores en el ámbito de aplicación de la Directiva 2002/58/CE. Con el fin de seguir utilizando dichas medidas voluntarias después del 20 de diciembre de 2020, los proveedores deben cumplir los requisitos establecidos en el presente Reglamento. El Reglamento (UE) 2016/679 seguirá aplicándose al tratamiento de datos personales efectuado mediante tales medidas voluntarias.

(10) La Directiva 2002/58/CE no contiene ninguna disposición específica relativa al tratamiento de datos personales por los proveedores en relación con la prestación de servicios de comunicación electrónica con el fin de detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y de retirar el material de abuso sexual de menores en línea de sus servicios. No obstante, de conformidad con el artículo 15, apartado 1, de dicha Directiva, los Estados miembros pueden adoptar medidas legislativas para restringir el alcance de los derechos y obligaciones establecidos, entre otros, en los artículos 5 y 6 de dicha Directiva, que se refieren a la confidencialidad de las comunicaciones y los datos de tráfico, con fines de prevención, detección, investigación y enjuiciamiento de delitos relacionados con el abuso sexual de menores. A falta de tales medidas legislativas nacionales, y a la espera de la adopción de un marco jurídico a más largo plazo para luchar contra el abuso sexual de menores a escala de la Unión, los proveedores ya no pueden acogerse al artículo 6 del Reglamento (UE) 2016/679 para seguir empleando medidas voluntarias para detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y retirar el material de abuso sexual de menores en línea de sus servicios después del 21 de diciembre de 2020. El presente Reglamento no proporciona una base jurídica para el tratamiento de datos personales por parte de los proveedores con el único fin de detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y de retirar de sus servicios el material de abuso sexual de menores en línea, pero establece una excepción a determinadas disposiciones de la Directiva 2002/58/CE. El presente Reglamento establece nuevas salvaguardias que deben ser respetadas por los proveedores si desean acogerse a él.

(11) El tratamiento de datos a efectos del presente Reglamento podría implicar el tratamiento de categorías especiales de datos personales establecidos en el Reglamento (UE) 2016/679. El tratamiento de imágenes y vídeos mediante medios técnicos específicos que permiten la identificación o autenticación unívocas de una persona física se considera tratamiento de categorías especiales de datos personales.

(12) El presente Reglamento establece una excepción temporal al artículo 5, apartado 1, y al artículo 6, apartado 1, de la Directiva 2002/58/CE, que protegen la confidencialidad de las comunicaciones y los datos de tráfico. La utilización voluntaria por parte de los proveedores de tecnologías para el tratamiento de datos personales y de otro tipo en la medida necesaria para detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y para retirar material de abuso sexual de menores en línea de sus servicios está comprendida en el ámbito de aplicación de la excepción establecida por el presente Reglamento, siempre que tal utilización cumpla las condiciones establecidas en el presente Reglamento y, por tanto, esté sujeta a las salvaguardias y condiciones establecidas en el Reglamento (UE) 2016/679.

(13) La Directiva 2002/58/CE se adoptó sobre la base del artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE). Además, no todos los Estados miembros han adoptado medidas legislativas de conformidad con la Directiva 2002/58/CE para restringir el alcance de los derechos y obligaciones relacionados con la confidencialidad de las comunicaciones y los datos de tráfico como se dispone en dicha Directiva, y la adopción de tales medidas entraña un riesgo significativo de fragmentación que puede afectar negativamente al mercado interior. Por ello, el presente Reglamento debe basarse en el artículo 114 TFUE.

(14) Dado que los datos relativos a comunicaciones electrónicas que impliquen a personas físicas se consideran generalmente datos personales, el presente Reglamento también debe basarse en el artículo 16 del TFUE, que proporciona una base jurídica específica para la adopción de normas sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, así como 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 esos datos.

(15) El Reglamento (UE) 2016/679 se aplica al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas por los proveedores con el único fin de detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y de retirar el material de abuso sexual de menores en línea de sus servicios en la medida en que dicho tratamiento esté comprendido en el ámbito de aplicación de la excepción establecida en el presente Reglamento.

(16) Los tipos de tecnologías utilizadas a efectos del presente Reglamento deben ser los menos intrusivos para la intimidad a la vista del estado de la técnica en el sector. Dichas tecnologías no deben emplearse para filtrar y escanear sistemáticamente el texto de las comunicaciones, salvo con el fin de detectar pautas que apunten a posibles razones concretas para sospechar de abuso sexual de menores en línea, y no deben poder deducir la sustancia del contenido de las comunicaciones. En el caso de la tecnología utilizada para identificar el embaucamiento de menores, tales razones concretas de sospecha deben basarse en factores de riesgo identificados objetivamente, como la diferencia de edad y la probable participación de un menor en la comunicación escaneada.

(17) Deben establecerse procedimientos y mecanismos de recurso adecuados para garantizar que los particulares puedan presentar reclamaciones ante los proveedores. Dichos procedimientos y mecanismos son especialmente pertinentes cuando se hayan retirado contenidos que no constituyan abusos sexuales de menores en línea, o cuando se hayan denunciado tales contenidos a las autoridades policiales o a una organización que actúe en interés público contra los abusos sexuales de menores.

(18) Con el fin de garantizar en la medida de lo posible la exactitud y fiabilidad, la tecnología utilizada a efectos del presente Reglamento, a la vista del estado de la técnica en el sector, debe limitar al máximo el número y las tasas de errores (falsos positivos) y debe, en caso necesario, corregir sin demora los errores que, no obstante, podrían producirse.

(19) Los datos de contenido y los datos de tráfico tratados y los datos personales generados en la realización de las actividades cubiertas por el presente Reglamento, y el período durante el cual se almacenan los datos en caso de detectarse un presunto abuso sexual de menores en línea, deben seguir limitados a lo estrictamente necesario para realizar dichas actividades. Los datos deben suprimirse inmediatamente y de manera permanente cuando ya no sean estrictamente necesarios para alguno de los fines enunciados en el presente Reglamento, también en el caso de que no se detecte ningún presunto abuso sexual de menores en línea, y, en cualquier caso, a más tardar doce meses a partir de la fecha de detección del presunto abuso sexual de menores en línea. Esto debe entenderse sin perjuicio de la posibilidad de almacenar los datos de contenido y datos de tráfico pertinentes de conformidad con la Directiva 2002/58/CE. El presente Reglamento no afecta a la aplicación de las obligaciones legales de conservación de datos impuestas por el Derecho de la Unión o de los Estados miembros impuestas a los proveedores.

(20) El presente Reglamento no impide a los proveedores que hayan denunciado abusos sexuales de menores en línea a las autoridades policiales solicitar un acuse de recibo de la denuncia a dichas autoridades.

(21) A fin de garantizar la transparencia y la rendición de cuentas con respecto a las actividades realizadas en virtud de la excepción prevista en el presente Reglamento, los proveedores deben, a más tardar el … [seis meses después de la fecha de entrada en vigor del presente Reglamento] y, posteriormente, a más tardar, el 31 de enero de cada año, publicar y presentar informes a la autoridad de control competente designada con arreglo al Reglamento (UE) 2016/679 (en lo sucesivo, «autoridad de control») y a la Comisión sobre el tratamiento comprendido en el ámbito de aplicación del presente Reglamento, incluidos el tipo y el volumen de datos tratados, los motivos específicos invocados para el tratamiento de datos personales de conformidad con el Reglamento (UE) 2016/679, los motivos invocados para las transferencias de datos personales fuera de la Unión de conformidad con el capítulo V del Reglamento (UE) 2016/679, en su caso, el número de casos detectados de abusos sexuales de menores en línea, diferenciando entre material de abuso sexual de menores en línea y embaucamiento de menores, el número de casos en los que un usuario haya presentado una reclamación ante el mecanismo de recurso interno o interpuesto una acción judicial y el resultado de dichas reclamaciones y causas judiciales, el número y las tasas de errores (falsos positivos) de las diferentes tecnologías utilizadas, las medidas aplicadas para limitar la tasa de error y la tasa de error alcanzada, la política de conservación de los datos y las salvaguardias de protección de datos aplicadas conforme al Reglamento (UE) 2016/679, y el nombre de las organizaciones que actúan en interés público contra los abusos sexuales de menores con las que se hayan compartido datos en virtud del presente Reglamento.

(22) A fin de apoyar en su labor a las autoridades de control, la Comisión debe solicitar al Comité Europeo de Protección de Datos que emita directrices sobre el cumplimiento del Reglamento (UE) 2016/679 en lo que respecta al tratamiento comprendido en el ámbito de aplicación de la excepción establecida en el presente Reglamento. Cuando las autoridades de control evalúen si una tecnología consolidada o nueva que se vaya a utilizar corresponde al estado de la técnica en el sector, es la menos intrusiva para la intimidad y opera sobre una base jurídica adecuada con arreglo al Reglamento (UE) 2016/679, dichas directrices deben, en particular, ayudar a las autoridades de control a prestar asesoramiento en el marco del procedimiento de consulta previa establecido en el Reglamento (UE) 2016/679.

(23) El presente Reglamento restringe el derecho a la protección de la confidencialidad de las comunicaciones y establece una excepción a la decisión adoptada en el marco de la Directiva (UE) 2018/1972 de someter los servicios de comunicaciones interpersonales independientes de la numeración a las mismas normas que se aplican a todos los demás servicios de comunicaciones electrónicas en lo que respecta a la privacidad, con el único fin de detectar abusos sexuales de menores en línea cometidos en dichos servicios y denunciarlos a las autoridades policiales o a organizaciones que actúen en interés público contra los abusos sexuales de menores y de retirar el material de abuso sexual de menores en línea de dichos servicios. Por consiguiente, el período de aplicación del presente Reglamento debe limitarse a tres años a partir de su fecha de aplicación, de modo que se deje el tiempo necesario para adoptar un nuevo marco jurídico a largo plazo. En caso de que el marco jurídico a largo plazo se adopte y entre en vigor antes de esa fecha, dicho marco jurídico a largo plazo debe derogar el presente Reglamento.

(24) Por lo que se refiere a todas las demás actividades comprendidas en el ámbito de aplicación de la Directiva 2002/58/CE, los proveedores deben estar sujetos a las obligaciones específicas establecidas en dicha Directiva, y, por tanto, a los poderes de control e investigación de las autoridades competentes designadas en virtud de esa Directiva.

(25) El cifrado de extremo a extremo es un instrumento importante para garantizar la seguridad y la confidencialidad de las comunicaciones de los usuarios, incluidas las de los menores. Todo debilitamiento del cifrado puede ser aprovechado por terceros malintencionados. Por tanto, ninguna disposición del presente Reglamento debe interpretarse en el sentido de que prohíbe o debilita el cifrado de extremo a extremo.

(26) El derecho al respeto de la vida privada y familiar, incluida la confidencialidad de las comunicaciones, es un derecho fundamental garantizado por el artículo 7 de la Carta. Por tanto, también es una condición necesaria para que haya comunicaciones seguras entre las víctimas de abusos sexuales de menores y un adulto de confianza o las organizaciones que se dedican a la lucha contra los abusos sexuales de menores, y comunicaciones entre las víctimas y sus abogados.

(27) El presente Reglamento debe entenderse sin perjuicio de las normas sobre secreto profesional de Derecho nacional, por ejemplo, las normas sobre la protección de las comunicaciones profesionales, entre médicos y sus pacientes, entre periodistas y sus fuentes, o entre abogados y sus clientes, en particular porque la confidencialidad de las comunicaciones entre abogados y sus clientes es fundamental para garantizar el ejercicio efectivo de los derechos de la defensa, que son parte esencial del derecho a un juicio justo. El presente Reglamento, debe entenderse también sin perjuicio de las normas nacionales sobre registros de autoridades públicas u organizaciones que ofrecen asesoramiento a personas en dificultades.

(28) Los proveedores deben comunicar a la Comisión los nombres de las organizaciones que actúan en interés público contra los abusos sexuales de menores a las que denuncian posibles abusos sexuales de menores en línea en virtud del presente Reglamento. Si bien es responsabilidad exclusiva de los proveedores que actúan como responsables del tratamiento evaluar con qué tercero pueden compartir datos personales con arreglo al Reglamento (UE) 2016/679, la Comisión debe garantizar la transparencia respecto de la transferencia de posibles casos de abusos sexuales de menores en línea publicando en su sitio web una lista de las organizaciones que actúan en interés público contra los abusos sexuales de menores que se le hayan comunicado. Dicha lista pública debe ser de fácil acceso. También debe ser posible para los proveedores utilizar dicha lista a fin de conocer las organizaciones pertinentes en la lucha mundial contra los abusos sexuales de menores en línea. Dicha lista debe entenderse sin perjuicio de las obligaciones de los proveedores que actúen como responsables del tratamiento en virtud del Reglamento (UE) 2016/679, en particular en lo que se refiere a su obligación de respetar el capítulo V de dicho Reglamento en las transferencias de datos personales fuera de la Unión y a su obligación de cumplir todas las obligaciones previstas en el capítulo IV de dicho Reglamento.

(29) Las estadísticas que han de ser presentadas por los Estados miembros con arreglo al presente Reglamento son indicadores importantes para evaluar la política en este ámbito, incluidas las medidas legislativas. Además, es importante tener presente el impacto de la victimización secundaria inherente al intercambio de imágenes y vídeos de víctimas de abusos sexuales de menores, que podrían haber estado circulando desde hace años, impacto que no se refleja plenamente en dichas estadísticas.

(30) En consonancia con las obligaciones establecidas en el Reglamento (UE) 2016/679, en particular con la obligación de que los Estados miembros velen por que las autoridades de control dispongan de los recursos humanos, técnicos y financieros necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, los Estados miembros deben velar por que las autoridades de control dispongan de los recursos suficientes para el cumplimiento efectivo de las funciones y el ejercicio de los poderes que prevé el presente Reglamento.

(31) Cuando un proveedor haya realizado una evaluación de impacto relativa a la protección de datos y haya consultado a las autoridades de control en relación con una tecnología de conformidad con el Reglamento (UE) 2016/679 antes de la entrada en vigor del presente Reglamento, dicho proveedor no debe estar obligado, en virtud del presente Reglamento, a efectuar una nueva evaluación de impacto relativa a la protección de datos o una nueva consulta, siempre que las autoridades de control hayan indicado que el tratamiento de datos por dicha tecnología no entrañaría un riesgo elevado para los derechos y libertades de las personas físicas o que el responsable del tratamiento haya adoptado medidas para mitigar dicho riesgo.

(32) Los usuarios deben tener derecho a la tutela judicial efectiva cuando sus derechos hayan sido vulnerados como consecuencia del tratamiento de datos personales o de otro tipo con fines de detección de abusos sexuales de menores en línea en servicios de comunicaciones interpersonales independientes de la numeración y de su denuncia y de retirada de material de abuso sexual de menores en línea de dichos servicios, como en los casos en que el contenido o la identidad de los usuarios hayan sido comunicados a una organización que actúe en interés público contra los abusos sexuales de menores o a las autoridades policiales, o en que se hayan retirado contenidos o bloqueado la cuenta de un usuario o suspendido un servicio que se le ofrecía.

(33) De acuerdo con la Directiva 2002/58/CE y con el principio de minimización de datos, el tratamiento de datos personales y de otro tipo debe limitarse a datos de contenido y datos de tráfico conexos, en la medida que sea estrictamente necesaria para alcanzar el objetivo del presente Reglamento.

(34) La excepción establecida en el presente Reglamento debe extenderse a las categorías de datos a que se refieren los artículos 5, apartado 1, y 6, apartado 1, de la Directiva 2002/58/CE, que son aplicables al tratamiento de datos personales y no personales tratados en el contexto de la prestación de un servicio de comunicaciones interpersonales independiente de la numeración.

(35) El objetivo del presente Reglamento es establecer una excepción temporal a determinadas disposiciones de la Directiva 2002/58/CE sin crear fragmentación en el mercado interior. Además, es improbable que los Estados miembros puedan adoptar medidas legislativas nacionales a tiempo. Dado que el objetivo del presente Reglamento no puede ser alcanzado de manera suficiente por los Estados miembros, sino que 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 TUE. De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo. El presente Reglamento introduce una excepción temporal y estrictamente limitada a la aplicabilidad de los artículos 5, apartado 1, y 6, apartado 1, de la Directiva 2002/58/CE, con una serie de salvaguardias que garantizan que dicha excepción no va más allá de lo necesario para alcanzar el objetivo fijado.

(36) El Supervisor Europeo de Protección de Datos, al que se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) n.º 2018/1725 del Parlamento Europeo y del Consejo[1], emitió su dictamen el 10 de noviembre de 2020.

HAN ADOPTADO EL PRESENTE REGLAMENTO:

[1] Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

Artículo 1

Objeto y ámbito de aplicación

1. El presente Reglamento introduce normas temporales y estrictamente limitadas que establecen una excepción a determinadas obligaciones impuestas por la Directiva 2002/58/CE, con el único objetivo de permitir a determinados proveedores de servicios de comunicaciones interpersonales independientes de la numeración (en lo sucesivo, «proveedores») usar, sin perjuicio de lo dispuesto en el Reglamento (UE) 2016/679, tecnologías específicas para el tratamiento de datos personales y de otro tipo en la medida estrictamente necesaria para detectar abusos sexuales de menores en línea cometidos en sus servicios y denunciarlos y para retirar el material de abuso sexual de menores en línea de sus servicios.

2. El presente Reglamento no se aplicará al escaneado de comunicaciones de audio.

Artículo 2

Definiciones

A efectos del presente Reglamento, se entenderá por:

1) «servicio de comunicaciones interpersonales independiente de la numeración»: un servicio de comunicaciones interpersonales independiente de la numeración tal como se define en el artículo 2, punto 7, de la Directiva (UE) 2018/1972;

2) «material de abuso sexual de menores en línea»:

a) pornografía infantil tal como se define en el artículo 2, letra c), de la Directiva 2011/93/UE;

b) espectáculo pornográfico tal como se define en el artículo 2, letra e), de la Directiva 2011/93/UE;

3) «embaucamiento de menores»: cualquier conducta intencionada constitutiva de infracción penal conforme al artículo 6 de la Directiva 2011/93/UE;

4) «abuso sexual de menores en línea»: material de abuso sexual de menores en línea» y embaucamiento de menores.

Artículo 3

Alcance de la excepción

1. El artículo 5, apartado 1, y el artículo 6, apartado 1, de la Directiva 2002/58/CE no se aplicarán a la confidencialidad de las comunicaciones que impliquen el tratamiento de datos personales y de otro tipo por parte de los proveedores en relación con la prestación de servicios de comunicaciones interpersonales independientes de la numeración, siempre que:

   a) el tratamiento sea:

      i) estrictamente necesario para el uso de tecnologías específicas con el único fin de detectar y retirar el material de abuso sexual de menores en línea y denunciarlo a las autoridades policiales y a las organizaciones que actúen en interés público contra los abusos sexuales de menores, y de detectar el embaucamiento de menores y denunciarlo a las autoridades policiales y a las organizaciones que actúen en interés público contra los abusos sexuales de menores,

      ii) proporcionado y se limite a tecnologías utilizadas por los proveedores para los fines establecidos en el inciso i),

      iii) limitado a los datos de contenido y de datos de tráfico conexos que sean estrictamente necesarios para los fines establecidos en el inciso i),

      iv) limitado a lo estrictamente necesario para los fines establecidos en el inciso i);

b) las tecnologías utilizadas para los fines establecidos en la letra a), inciso i),del presente apartado correspondan al estado de la técnica en el sector y sean las menos intrusivas para la intimidad, teniendo en cuenta también el principio de protección de datos desde el diseño y por defecto, tal como se establece en el artículo 25 del Reglamento (UE) 2016/679 y, en la medida en que se utilicen para escanear el texto de comunicaciones, que no sean capaces de deducir la sustancia del contenido de las comunicaciones, sino que sean únicamente capaces de detectar patrones que apunten a posibles abusos sexuales de menores en línea;

c) en relación con cualquier tecnología específica utilizada para los fines establecidos en la letra a), inciso i), del presente apartado, se hayan llevado a cabo previamente una evaluación de impacto relativa a la protección de datos a que se refiere el artículo 35 del Reglamento (UE) 2016/679 y un procedimiento de consulta previa a que se refiere el artículo 36 de dicho Reglamento;

d) con respecto a tecnologías nuevas, es decir, tecnologías utilizadas para detectar material de abuso sexual de menores en línea que no hayan sido utilizadas por ningún proveedor para servicios prestados a los usuarios de servicios de comunicaciones interpersonales independientes de la numeración (en lo sucesivo, «usuarios») en la Unión antes de … [fecha de entrada en vigor del presente Reglamento], y con respecto a tecnologías utilizadas para detectar el posible embaucamiento de menores, el proveedor informe a la autoridad competente sobre las medidas adoptadas para demostrar la conformidad con el asesoramiento por escrito emitido de conformidad con el artículo 36, apartado 2, del Reglamento (UE) 2016/679 por la autoridad de control competente designada a efectos del capítulo VI, sección 1, de dicho Reglamento (en lo sucesivo, «autoridad de control») durante el procedimiento de consulta previa;

e) las tecnologías utilizadas sean lo suficientemente fiables en cuanto que limiten en la mayor medida posible la tasa de errores en la detección de contenidos que representan abusos sexuales de menores en línea y, cuando se produzcan tales errores ocasionales, permitan rectificar sus consecuencias sin demora;

f) las tecnologías utilizadas para detectar patrones del posible embaucamiento de menores se limiten al uso de indicadores fundamentales pertinentes y factores de riesgo identificados objetivamente, como la diferencia de edad y la probable participación de un menor en la comunicación escaneada, sin perjuicio del derecho a una revisión humana;

g) los proveedores:

i) hayan establecido procedimientos internos para prevenir el abuso, el acceso no autorizado y las transferencias no autorizadas de datos personales y de otro tipo,

ii) garanticen la supervisión y, en caso necesario, la intervención humanas en relación con el tratamiento de datos personales y de otro tipo mediante la utilización de tecnologías a las que se aplica el presente Reglamento,

iii) se aseguren de que el material que no se haya considerado anteriormente material de abuso sexual de menores en línea no se remita sin confirmación humana previa a las autoridades policiales o a las organizaciones que actúan en interés público contra los abusos sexuales de menores,

iv) hayan establecido procedimientos y mecanismos de recurso adecuados para garantizar que los usuarios les puedan presentar reclamaciones en un plazo razonable con el fin de hacer oír su opinión,

v) informen a los usuarios de manera clara, destacada y comprensible de que han invocado, de conformidad con el presente Reglamento, la excepción legal a los artículos 5, apartado 1, y 6, apartado 1, de la Directiva 2002/58/CE en relación con la confidencialidad de las comunicaciones de los usuarios, únicamente para los fines establecidos en la letra a), inciso i), del presente apartado, la lógica subyacente a las medidas que hayan tomado en virtud de la excepción y el impacto en la confidencialidad de las comunicaciones de los usuarios, incluida la posibilidad de que los datos personales se compartan con las autoridades policiales y las organizaciones que actúen en interés público contra los abusos sexuales de menores,

vi) informen a los usuarios de los siguientes extremos, en caso de retirada de sus contenidos o bloqueo de su cuenta o suspensión del servicio que se les ofrecía:

1) las vías para recurrir ante ellos,

2) la posibilidad de presentar una reclamación ante una autoridad de control, y

3) el derecho a un recurso judicial,

vii) a más tardar el … [seis meses después de la fecha de entrada en vigor del presente Reglamento] y, posteriormente, a más tardar, el 31 de enero de cada año, publiquen y presenten un informe a la autoridad de control competente y a la Comisión sobre el tratamiento de datos personales en virtud del presente Reglamento, incluyendo sobre:

1) el tipo y el volumen de datos tratados,

2) el motivo específico invocado para el tratamiento de conformidad con el Reglamento (UE) 2016/679,

3) el motivo invocado para las transferencias de datos personales fuera de la Unión de conformidad con el capítulo V del Reglamento (UE) 2016/679, en su caso,

4) el número de casos detectados de abusos sexuales de menores en línea, diferenciando entre material de abuso sexual de menores en línea y embaucamiento de menores,

5) el número de casos en los que un usuario ha presentado una reclamación ante el mecanismo de recurso interno o ante una autoridad judicial y el resultado de dichas reclamaciones,

6) el número y las tasas de errores (falsos positivos) de las diferentes tecnologías utilizadas,

7) las medidas aplicadas para limitar la tasa de error y la tasa de error alcanzada,

8) la política de conservación de los datos y las salvaguardias de protección de datos aplicadas conforme al Reglamento (UE) 2016/679,

9) el nombre de las organizaciones que actúan en interés público contra los abusos sexuales de menores con las que se hayan compartido datos en virtud del presente Reglamento;

h) cuando se haya detectado un presunto abuso sexual de menores en línea, los datos de contenido y los datos de tráfico conexos tratados a los efectos de la letra a), inciso i), así como los datos personales generados mediante dicho tratamiento se almacenen de manera segura y únicamente con los fines siguientes:

i) denunciar sin demora el presunto abuso sexual de menores en línea a las autoridades policiales y judiciales competentes o a organizaciones que actúen en interés público contra los abusos sexuales de menores,

ii) bloquear la cuenta del usuario de que se trata, o de suspender o poner fin a la prestación del servicio a dicho usuario,

iii) crear una firma digital única y no reconvertible («hash») de datos identificados de forma fiable como material de abuso sexual de menores en línea,

iv) permitir al usuario de que se trate recurrir ante el proveedor o interponer recursos administrativos o judiciales en asuntos relacionados con el presunto abuso sexual de menores en línea, o

v) responder a las solicitudes emitidas por las autoridades policiales y judiciales competentes de conformidad con el Derecho aplicable para proporcionarles los datos necesarios para la prevención, detección, investigación o enjuiciamiento de infracciones penales establecidas en la Directiva 2011/93/UE;

i) los datos no se almacenen más tiempo del estrictamente necesario para el fin pertinente establecido en la letra h) y, en cualquier caso, no más de doce meses a partir de la fecha en que se detectó el presunto abuso sexual de menores en línea;

j) se denuncie sin demora todo caso de sospecha fundada y verificada de abuso sexual de menores en línea a las autoridades policiales nacionales competentes o a organizaciones que actúen en interés público contra los abusos sexuales de menores.

2. La condición establecida en el apartado 1, letra c), no se aplicará hasta el … [ocho meses después de la fecha de entrada en vigor del presente Reglamento] a los proveedores:

a) que utilizaban una tecnología específica antes del … [fecha de entrada en vigor del presente Reglamento] para los fines establecidos en el apartado 1, letra a), inciso i), sin haber completado previamente un procedimiento de consulta con respecto a dicha tecnología;

b) que inicien un procedimiento de consulta antes del … [un mes después de la fecha de entrada en vigor del presente Reglamento]; y

c) que cooperen debidamente con la autoridad de control competente en relación con el procedimiento de consulta a que se refiere la letra b).

3. La condición establecida en el apartado 1, letra d), no se aplicará hasta el … [ocho meses después de la fecha de entrada en vigor del presente Reglamento] a los proveedores que:

a) utilizaban una tecnología contemplada en el apartado 1, letra d), antes del … [fecha de entrada en vigor del presente Reglamento] sin haber completado previamente un procedimiento de consulta con respecto a dicha tecnología;

b) inicien un procedimiento a que se refiere el apartado 1, letra d), antes del … [un mes después de la fecha de entrada en vigor del presente Reglamento]; y

c) cooperen debidamente con la autoridad de control competente en relación con el procedimiento previsto en el apartado 1, letra d).

Artículo 4

Directrices del Comité Europeo de Protección de Datos

A más tardar el … [un mes después de la fecha de entrada en vigor del presente Reglamento], y con arreglo al artículo 70 del Reglamento (UE) 2016/679, la Comisión solicitará al Comité Europeo de Protección de Datos que emita directrices con el fin de ayudar a las autoridades de control a determinar si el tratamiento comprendido en el ámbito de aplicación del presente Reglamento en lo que respecta tanto a las tecnologías existentes como a las futuras, utilizado para los fines establecidos en el artículo 3, apartado 1, letra a), inciso i), del presente Reglamento, cumple lo dispuesto en el Reglamento (UE) 2016/679.

Artículo 5

Tutela judicial efectiva

De conformidad con el artículo 79 del Reglamento (UE) 2016/679 y el artículo 15, apartado 2, de la Directiva 2002/58/CE, los usuarios tendrán derecho a la tutela judicial efectiva cuando consideren que sus derechos han sido vulnerados como consecuencia del tratamiento de datos personales y de otro tipo para los fines establecidos en el artículo 3, apartado 1, letra a), inciso i), del presente Reglamento.

Artículo 6

Autoridades de control

Las autoridades de control designadas de conformidad con el capítulo VI, sección 1, del Reglamento (UE) 2016/679 controlarán el tratamiento comprendido en el ámbito de aplicación del presente Reglamento con arreglo a las competencias y poderes que le atribuye dicho capítulo.

Artículo 7

Lista pública de organizaciones que actúan en interés público contra los abusos sexuales de menores

1. A más tardar el … [un mes después de la fecha de entrada en vigor del presente Reglamento], los proveedores comunicarán a la Comisión una lista con los nombres de las organizaciones que actúan en interés público contra los abusos sexuales de menores a las que los proveedores denuncian abusos sexuales de menores en línea con arreglo al presente Reglamento. Los proveedores comunicarán periódicamente a la Comisión toda modificación de dicha lista.

2. A más tardar el … [dos meses después de la fecha de entrada en vigor del presente Reglamento], la Comisión publicará una lista con los nombres de las organizaciones que actúan en interés público contra los abusos sexuales de menores que se le haya comunicado con arreglo al apartado 1. La Comisión mantendrá dicha lista actualizada.

Artículo 8

Estadísticas

1. A más tardar el … [doce meses después de la fecha de entrada en vigor del presente Reglamento], y anualmente a partir de entonces, los Estados miembros publicarán y enviarán a la Comisión informes con datos estadísticos sobre los elementos siguientes:

   a) el número total de denuncias de abusos sexuales de menores en línea detectados que hayan presentado los proveedores y las organizaciones que actúan en interés público contra los abusos sexuales de menores ante las autoridades policiales nacionales competentes, diferenciando, cuando se disponga de tal información, entre el número absoluto de casos y los casos denunciados varias veces, y también según el tipo de proveedor en cuyo servicio se detectó el abuso sexual de menores en línea;

   b) el número de menores identificados mediante acciones con arreglo al artículo 3 del presente Reglamento, desglosado por género;

   c) el número de infractores condenados.

2. La Comisión agregará las estadísticas contempladas a que se refiere el apartado 1 del presente artículo y las tomará en cuenta al elaborar el informe de aplicación contemplado en el artículo 9.

Artículo 9

Informe de aplicación

1. Sobre la base de los informes presentados con arreglo al artículo 3, apartado 1, letra g), inciso vii) y de las estadísticas facilitadas con arreglo al artículo 8, la Comisión elaborará, a más tardar el … [dos años después de la fecha de entrada en vigor del presente Reglamento], un informe sobre la aplicación del presente Reglamento y lo presentará al Parlamento Europeo y al Consejo.

2. En el informe de aplicación, la Comisión tomará en consideración, en particular:

   a) las condiciones para el tratamiento de datos personales y de otro tipo establecidas en el artículo 3, apartado 1, letra a), inciso ii) y letras b), c) y d);

   b) la proporcionalidad de la excepción prevista en el presente Reglamento, incluida la evaluación de las estadísticas presentadas por los Estados miembros con arreglo al artículo 8;

   c) los avances tecnológicos relativos a las actividades contempladas en el presente Reglamento, y la medida en que estos avances mejoran la precisión y reducen el número y las tasas de errores (falsos positivos).

Artículo 10

Entrada en vigor y aplicación

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

Será aplicable hasta el … [tres años después de la fecha de entrada en vigor del presente Reglamento].

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*