CEPD-SEPD

Dictamen conjunto 4/2022

sobre la propuesta de Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores

Adoptado el 28 de julio de 2022

ÍNDICE

Resumen

El 11 de mayo de 2022, la Comisión Europea publicó la propuesta de Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores.

La propuesta impondría a los prestadores de servicios de alojamiento de datos, servicios de comunicaciones interpersonales y otros servicios obligaciones relacionadas con la detección, la denuncia, la eliminación y el bloqueo de material conocido y nuevo de abuso sexual de menores en línea y del embaucamiento de menores. La propuesta también contempla la creación de una nueva agencia descentralizada de la UE (el «Centro de la UE») y una red de autoridades nacionales de coordinación en materia de abusos sexuales de menores para facilitar la ejecución del Reglamento propuesto. Como se indica en la exposición de motivos de la propuesta, las medidas recogidas en esta afectarían al ejercicio de los derechos fundamentales de los usuarios de los servicios en cuestión.

El abuso sexual de menores es un delito especialmente grave y abyecto, y con la adopción de medidas efectivas para combatirlo se persigue un objetivo de interés general reconocido por la Unión y se busca proteger los derechos y las libertades de las víctimas. Al mismo tiempo, el CEPD y el SEPD recuerdan que cualquier limitación de derechos fundamentales, como las que se prevén en la propuesta, debe cumplir los requisitos establecidos en el artículo 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea.

El CEPD y el SEPD recalcan que la propuesta suscita serias dudas con respecto a la proporcionalidad de la injerencia y las limitaciones previstas a la protección de los derechos fundamentales a la vida privada y la protección de los datos personales. En ese sentido, el CEPD y el SEPD señalan que las garantías procesales nunca pueden reemplazar por completo a las garantías sustantivas. Un sistema complejo de progresividad que vaya de la evaluación de riesgos y las medidas de mitigación hasta las órdenes de detección no puede sustituir la claridad necesaria de las obligaciones sustantivas.

El CEPD y el SEPD consideran que la propuesta es poco clara respecto a los elementos clave, como ocurre con el concepto de «riesgo significativo». Además, las entidades encargadas de aplicar dichas garantías, desde los operadores privados hasta las autoridades administrativas o judiciales, gozan de un margen de apreciación muy amplio, lo que genera inseguridad jurídica respecto a cómo conciliar los derechos en juego en cada caso particular. El CEPD y el SEPD insisten en que, cuando autorice injerencias importantes con derechos fundamentales, el legislador debe aportar claridad jurídica sobre los momentos y las circunstancias particulares en que están permitidas tales injerencias. Si bien admiten que la legislación no puede ser demasiado prescriptiva y debe permitir cierta flexibilidad en su aplicación práctica, el CEPD y el SEPD consideran que la propuesta deja demasiado margen para posibles abusos debido a la inexistencia de unas normas sustantivas claras.

En cuanto a la necesidad y la proporcionalidad de las medidas de detección previstas, al CEPD y el SEPD les preocupan particularmente las medidas previstas para detectar material de abuso sexual de menores desconocido y el embaucamiento de menores con fines sexuales (práctica también conocida como «captación de menores») en los servicios de comunicación interpersonal. Debido a su carácter intrusivo, su naturaleza probabilística y las tasas de error asociadas a dichas tecnologías, el CEPD y el SEPD consideran que la injerencia que generan estas medidas sobrepasa lo que es necesario y proporcionado. Es más, las medidas que permiten a las autoridades públicas acceder de forma generalizada al contenido de una comunicación para detectar embaucamiento de menores tienen más probabilidades de afectar a la esencia

de los derechos garantizados en los artículos 7 y 8 de la Carta. Por lo tanto, se deberían suprimir de la propuesta las disposiciones relevantes referentes a la captación de menores. Además, la propuesta no excluye de su ámbito de aplicación el escaneado de comunicaciones de audio. El CEPD y el SEPD creen que el escaneado de comunicaciones de audio es especialmente intrusivo, por lo que debe permanecer al margen de las obligaciones de detección establecidas en el Reglamento propuesto en lo que respecta tanto a los mensajes de voz como a las comunicaciones en directo.

El CEPD y el SEPD expresan igualmente sus dudas con respecto a la eficiencia de las medidas de bloqueo, y consideran que sería desproporcionado exigir a los prestadores de servicios de internet que descifren las comunicaciones en línea para bloquear las relacionadas con material de abuso sexual de menores.

Asimismo, el CEPD y el SEPD señalan que las tecnologías de cifrado contribuyen de una manera fundamental al respeto de la vida privada y la confidencialidad de las comunicaciones, a la libertad de expresión, a la innovación y al crecimiento de la economía digital, que se fundamenta en el elevado nivel de seguridad y confianza que proporcionan dichas tecnologías. El considerando 26 de la propuesta advierte de que tanto la elección de tecnologías de detección como las medidas técnicas destinadas a proteger la confidencialidad de las comunicaciones, tales como el cifrado, deben cumplir los requisitos del Reglamento propuesto, es decir, deben permitir la detección. Esto refuerza la noción de que un prestador no puede oponerse a la ejecución de una orden de detección aduciendo su imposibilidad técnica que se desprende del artículo 8, apartado 3, y el artículo 10, apartado 2, de la propuesta. El CEPD y el SEPD consideran que debería haber un mayor equilibrio entre la necesidad social de contar con canales de comunicación seguros y privados y de luchar contra su uso indebido. Conviene indicar claramente en la propuesta que ninguna de sus disposiciones debe interpretarse en el sentido de que prohíbe o debilita el cifrado.

Aunque el CEPD y el SEPD aplauden que en la propuesta se estipule que no afecta a las facultades y competencias de las autoridades de protección de datos en virtud del RGPD, aun así, consideran que debe regularse mejor la relación entre las funciones de las autoridades de coordinación y las de las autoridades de protección de datos. En este sentido, el CEPD y el SEPD agradecen la función que la propuesta asigna al CEPD al exigir su implicación en la aplicación práctica de la propuesta, y en particular la necesidad de que el CEPD emita un dictamen sobre las tecnologías que el Centro de la UE pondrá a disposición para ejecutar las órdenes de detección. No obstante, se debe aclarar cuál será la finalidad del dictamen en el proceso y cómo actuará el Centro de la UE tras recibir un dictamen del CEPD.

Por último, el CEPD y el SEPD señalan que la propuesta contempla una estrecha cooperación entre el Centro de la UE y Europol, que deberán facilitarse mutuamente «el acceso más completo posible a los sistemas de información pertinentes». Si bien el CEPD y el SEPD apoyan en principio la cooperación entre ambos organismos, puesto que el Centro de la UE no es un cuerpo de seguridad, el CEPD y el SEPD formulan varias recomendaciones para mejorar las disposiciones pertinentes, lo que incluye especificar que la transmisión de datos personales entre el Centro de la UE y Europol únicamente tendrá lugar tras valorar las características de cada caso, en respuesta a una solicitud debidamente evaluada y por medio de una herramienta de intercambio de comunicaciones segura, como la red SIENA.

El Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos

Visto el artículo 42, apartado 2 del Reglamento (UE) 2018/1725, 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 estos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE («RPDUE»)[1],

Visto el Acuerdo sobre el Espacio Económico Europeo y, en particular, su anexo XI y su Protocolo 37, modificados por la Decisión del Comité Mixto del EEE n.º 154/2018, de 6 de julio de 2018[2],

Vista la solicitud de la Comisión Europea de un dictamen conjunto del Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos, de 12 de mayo de 2022, sobre la propuesta de Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores[3],

HAN ADOPTADO EL SIGUIENTE DICTAMEN CONJUNTO

1. ANTECEDENTES

1. El 11 de mayo de 2022, la Comisión Europea (la «Comisión») publicó una propuesta de Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores (en lo sucesivo, la «propuesta» o el «Reglamento propuesto»)[4].

2. La propuesta se publicó tras la adopción del Reglamento (UE) 2021/1232 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 (en lo sucesivo, el «Reglamento provisional»)[5]. El Reglamento provisional no exige que los prestadores de servicios relevantes tomen medidas para detectar materiales de abuso sexual de menores desconocidos (como imágenes o vídeos, por ejemplo) o embaucamiento de menores (práctica también conocida como «captación de menores») en sus

[1] DO L 295, de 21.11.2018, p. 39.
[2] Las referencias a los «Estados miembros» realizadas en el presente documento deben entenderse como referencias a los «Estados miembros del EEE».
[3] Propuesta de Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores, COM(2022) 209 final.
[4] Ibíd.
[5] Reglamento (UE) 2021/1232 del Parlamento Europeo y el 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 [DO (2021) L 274/41].

servicios, pero permite que lo hagan de manera voluntaria, de acuerdo con las condiciones establecidas en dicho Reglamento[6].

3. La propuesta se sustenta sobre dos pilares principales. En primer lugar, impone a los prestadores de servicios de alojamiento de datos, servicios de comunicaciones interpersonales y otros servicios obligaciones relacionadas con la detección, la denuncia, el bloqueo y la eliminación de material conocido y nuevo de abuso sexual de menores en línea y el embaucamiento de menores. En segundo lugar, la propuesta contempla la creación de una nueva agencia descentralizada de la UE (el «Centro de la UE sobre Abuso Sexual de Menores» o el «Centro de la UE») y una red de autoridades nacionales de coordinación en materia de abusos sexuales de menores para facilitar la ejecución del Reglamento propuesto[7].

4. Como se indica en la exposición de motivos de la propuesta, las medidas recogidas en esta afectarían al ejercicio de los derechos fundamentales de los usuarios de los servicios en cuestión. Entre tales derechos se encuentran, en particular, los derechos fundamentales al respeto de la vida privada (incluida la confidencialidad de las comunicaciones, en el marco del derecho más amplio al respeto de la vida privada y familiar), la protección de los datos personales y la libertad de expresión y de información[8].

5. Asimismo, las medidas propuestas buscan fundamentarse en la legislación existente en la UE en materia de protección de datos y privacidad y, en cierta medida, complementarla. En este sentido, en la exposición de motivos se señala que:

> «La propuesta se basa en el Reglamento General de Protección de Datos (RGPD). En la práctica, los prestadores suelen aducir diversos motivos para el tratamiento previstos en el RGPD para llevar a cabo el tratamiento de datos personales inherente a la detección y denuncia voluntarias de abusos sexuales de menores en línea. La propuesta establece un sistema de órdenes de detección específicas y precisa las condiciones para la detección, proporcionando una mayor seguridad jurídica a estas actividades. Por lo que se refiere a las actividades de detección obligatorias que implican el tratamiento de datos personales, la propuesta, en particular las órdenes de detección dictadas sobre esta base, establece el motivo para el tratamiento a que se refiere el artículo 6, apartado 1, letra c), del RGPD, que prevé el tratamiento de datos personales necesario para el cumplimiento de una obligación legal en virtud del Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento.
>
> La propuesta abarca, entre otros, a los prestadores que ofrecen servicios de comunicaciones electrónicas interpersonales y, por tanto, están sujetos a las disposiciones nacionales de aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas y su propuesta de revisión, actualmente en fase de negociación. Las medidas establecidas en la propuesta restringen en algunos aspectos el alcance de los derechos y las obligaciones en virtud de las disposiciones pertinentes de dicha Directiva, a saber, en relación con las actividades

[6] Véase también SEPD, *Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online* [«Dictamen 7/2020 sobre la propuesta relativa a la aplicación de excepciones temporales a la Directiva 2002/58/CE para combatir el abuso sexual de menores en línea», documento no disponible en español], 10 de noviembre de 2020.
[7] COM(2022) 209 final, p. 19.
[8] COM(2022) 209 final, pp. 13 y 14.

estrictamente necesarias para ejecutar las órdenes de detección. En este sentido, la propuesta implica la aplicación, por analogía, del artículo 15, apartado 1, de dicha Directiva»[9].

6. Dada la gravedad de las injerencias en derechos fundamentales previstas, la propuesta reviste especial importancia para la protección de los derechos y las libertades de los ciudadanos en lo que respecta al tratamiento de sus datos personales. Por este motivo, el 12 de mayo de 2022 la Comisión decidió consultar al Comité Europeo de Protección de Datos (CEPD) y al Supervisor Europeo de Protección de Datos (SEPD), de conformidad con el artículo 42, apartado 2, del RPDUE.

2. ALCANCE DEL DICTAMEN

7. El presente Dictamen conjunto recoge las opiniones comunes del CEPD y el SEPD sobre la propuesta. Se limita a los aspectos de la propuesta referentes a la protección de la privacidad y los datos personales. En particular, el Dictamen conjunto señala aquellos ámbitos en los que la propuesta no garantiza una protección suficiente de los derechos fundamentales a la vida privada y la protección de datos, o que deben armonizarse mejor con el marco jurídico de la UE relativo a la protección de la privacidad y los datos personales.

8. Como se explica en más detalle en el presente Dictamen conjunto, la propuesta suscita serias dudas respecto a la necesidad y la proporcionalidad de las injerencias y las limitaciones previstas a la protección de los derechos fundamentales a la vida privada y la protección de los datos personales. No obstante, el objetivo del presente Dictamen conjunto no es proporcionar una lista exhaustiva de todos los aspectos de la protección de la privacidad y los datos personales que resultan problemáticos en la propuesta ni formular sugerencias específicas para mejorar su redacción, sino aportar observaciones de alto nivel sobre los principales problemas que el CEPD y el SEPD han observado en la propuesta. Aun así, el CEPD y el SEPD quedan a disposición de los colegisladores para formular más observaciones y recomendaciones durante el proceso legislativo de la propuesta.

3. OBSERVACIONES GENERALES SOBRE LOS DERECHOS A LA CONFIDENCIALIDAD DE LAS COMUNICACIONES Y A LA PROTECCIÓN DE LOS DATOS PERSONALES

9. La confidencialidad de las comunicaciones es un elemento esencial del derecho fundamental al respeto de la vida privada y familiar, consagrado en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, la «Carta»)[10]. Asimismo, el artículo 8 de la Carta reconoce el derecho fundamental a la protección de los datos personales. Los derechos a la confidencialidad de las comunicaciones y al respeto a la vida privada y familiar quedan igualmente

[9] COM(2022) 209 final, p. 5.
[10] Véase, por ejemplo, *Declaración del CEPD relativa a la revisión del Reglamento sobre la privacidad y las comunicaciones electrónicas y su repercusión en la protección de las personas en lo que respecta a la privacidad y la confidencialidad de sus comunicaciones*, 25 de mayo de 2018.

garantizados en el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH) y forman parte de las tradiciones constitucionales que comparten los Estados miembros[11].

10. El CEPD y el SEPD recuerdan que los derechos consagrados en los artículos 7 y 8 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse según su función en la sociedad[12]. El abuso sexual de menores es un delito especialmente grave y abyecto, y con la adopción de medidas efectivas para combatirlo se persigue un objetivo de interés general reconocido por la Unión y se busca proteger los derechos y las libertades de las víctimas. En lo que respecta a la adopción de medidas efectivas para combatir los delitos cometidos contra menores y otras personas vulnerables, el Tribunal de Justicia de la Unión Europea (TJUE) ha señalado que del artículo 7 de la Carta pueden desprenderse obligaciones positivas que exijan a las autoridades públicas adoptar medidas jurídicas para proteger la vida privada y familiar, los hogares y las comunicaciones. Tales obligaciones pueden desprenderse igualmente de los artículos 3 y 4 de la Carta, que se refieren a la protección de la integridad física y mental de las personas y a la prohibición de la tortura y de las penas o los tratos inhumanos o degradantes[13].

11. Al mismo tiempo, cualquier limitación de los derechos garantizados en la Carta, como las que se prevén en la propuesta[14], deben cumplir los requisitos establecidos en el artículo 52, apartado 1, de la Carta. Toda medida que interfiera con el derecho a la confidencialidad de las comunicaciones y el derecho a la vida privada y familiar debe respetar ante todo la esencia de tales derechos[15]. La esencia de un derecho se ve afectada si el derecho queda vacío de su contenido básico y la persona no puede ejercerlo[16]. La injerencia no puede ser, en relación con el objetivo que se persiga, tan desproporcionada e intolerable que menoscabe la esencia misma del derecho garantizado[17]. Esto significa que incluso un derecho fundamental que no sea absoluto, como el derecho a la confidencialidad de las comunicaciones y el derecho a la protección de los datos personales, presentan ciertos componentes básicos que no pueden limitarse.

12. El TJUE ha efectuado en múltiples ocasiones la prueba de la «esencia de un derecho» en el ámbito de la privacidad de las comunicaciones electrónicas. En Tele2 Sverige y Watson, el Tribunal dictaminó que la normativa que no autorice la conservación del contenido de las comunicaciones no puede vulnerar

---

[11] Prácticamente todas las constituciones europeas contemplan el derecho a la protección de la confidencialidad de las comunicaciones. Véase, por ejemplo, el artículo 15 de la Constitución de la República Italiana, el artículo 10 de la Ley Fundamental de la República Federal de Alemania, el artículo 22 de la Constitución belga y el artículo 13 de la Constitución del Reino de los Países Bajos.

[12] Véase, entre otros, la sentencia del TJUE, asunto C-311/18, Facebook Ireland y Schrems, apartado 172 y la jurisprudencia que en él se cita. Véase asimismo el considerando 4 del RGPD.

[13] TJUE, asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, apartados 126 a 128. Véase también SEPD, *Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online* [«Dictamen 7/2020 sobre la propuesta relativa a la aplicación de excepciones temporales a la Directiva 2002/58/CE para combatir el abuso sexual de menores en línea», documento no disponible en español], 10 de noviembre de 2020, apartado 12.

[14] Véase COM(2022) 209 final, pp. 13 a 15.

[15] Artículo 52, apartado 1, de la Carta.

[16] Véase SEPD, *Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales*, 19 de diciembre de 2019, p. 7. Disponible en: https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

[17] TJUE, asunto C-393/19, OM, apartado 53.

el contenido esencial de los derechos a la vida privada y a la protección de los datos personales[18]. En Schrems, el Tribunal determinó que se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta[19]. En Digital Rights Ireland, Seitlinger y otros, el Tribunal concluyó que, aunque la conservación de datos que la Directiva 2006/24 impone constituye una injerencia especialmente grave en el derecho a la privacidad y los demás derechos consagrados en el artículo 7 de la Carta, no puede vulnerar el contenido esencial de dichos derechos porque la Directiva no permite conocer el contenido de las comunicaciones electrónicas como tal[20]. De esta jurisprudencia se puede inferir que las medidas que permiten a las autoridades públicas acceder de forma generalizada al contenido de una comunicación tienen más probabilidades de afectar al contenido esencial de los derechos garantizados en los artículos 7 y 8 de la Carta. Estas consideraciones son igualmente relevantes en relación con las medidas para la detección de material de abuso sexual de menores desconocido y embaucamiento de menores, como las que recoge la propuesta.

13. Asimismo, el TJUE ha determinado que las medidas para la seguridad de los datos son primordiales para garantizar que no se vulnere el contenido esencial del derecho fundamental a la protección de datos de carácter personal reconocido en el artículo 8 de la Carta[21]. En la era digital, las soluciones técnicas para asegurar y proteger la confidencialidad de las comunicaciones digitales, en particular las medidas de cifrado, son importantes para garantizar el disfrute de todos los derechos fundamentales[22]. Hay que tener debidamente en cuenta esto cuando se evalúen las medidas para la detección obligatoria de material de abuso sexual de menores desconocido y embaucamiento de menores, en particular si pueden debilitar o deteriorar el cifrado[23].

14. El artículo 52, apartado 1, de la Carta también estipula que cualquier limitación del ejercicio de un derecho fundamental reconocido en ella deberá ser establecida por ley. Dentro del respeto del principio de proporcionalidad, solo se podrán introducir limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás[24]. Para cumplir el requisito de proporcionalidad, una normativa debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger de manera eficaz esos datos contra los riesgos de abuso[25]. Dicha normativa debe indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario[26]. Tal y como aclara el

[18] TJUE, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige y Watson, apartado 101.
[19] TJUE, asunto C-362/14, Schrems, apartado 94.
[20] TJUE, asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland, Seitlinger y otros, apartado 39.
[21] Ibíd., apartado 40.
[22] Véase Consejo de Derechos Humanos, Resolución 47/16 sobre la promoción, protección y disfrute de los derechos humanos en Internet, documento de las Naciones Unidas A/HRC/RES/47/16, 26 de julio de 2021.
[23] Véase también el considerando 25 del Reglamento provisional.
[24] Véase *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit* [«Herramientas para determinar la necesidad de medidas que limiten el derecho fundamental a la protección de los datos personales», documento no disponible en español], 11 de abril de 2017. Disponible en: https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.
[25] TJUE, asuntos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, apartado 132.
[26] Ibíd.

TJUE, la necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automatizado y cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles[27].

15. La propuesta limitaría el ejercicio de los derechos y las obligaciones previstos en el artículo 5, apartados 1 y 3, y el artículo 6, apartado 1, de la Directiva 2002/58/CE (la «Directiva sobre la privacidad y las comunicaciones electrónicas»)[28], en la medida en que sea necesario para la ejecución de las órdenes de detección emitidas de acuerdo con el capítulo I, sección 2, de la propuesta. El CEPD y el SEPD consideran que, por lo tanto, es necesario evaluar la propuesta teniendo en cuenta no solo la Carta y el RGPD, sino también los artículos 5 y 6 y el artículo 15, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

[27] Ibíd.

[28] 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), en su versión modificada por la Directiva 2006/24/CE y la Directiva 2009/136/CE.

4. OBSERVACIONES ESPECÍFICAS

4.1 Relación con la legislación existente

4.1.1 Relación con el RGPD y la Directiva sobre la privacidad y las comunicaciones electrónicas

16. La propuesta indica que debe entenderse sin perjuicio de las normas que emanan de otros actos de la Unión, en particular el RGPD[29] y la Directiva sobre la privacidad y las comunicaciones electrónicas. A diferencia del Reglamento provisional, la propuesta no establece explícitamente una excepción temporal al ejercicio de los derechos y obligaciones contemplados en el artículo 5, apartados 1 y 3, y el artículo 6, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas, sino una limitación de dicho ejercicio. Del mismo modo, cabe señalar que el Reglamento provisional únicamente establece una excepción a lo dispuesto en el artículo 5, apartado 1, y el artículo 6, apartado 1, y no al artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

17. La propuesta menciona asimismo que el artículo 15, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas permite a los Estados miembros adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6 de dicha Directiva cuando tal limitación constituya una medida necesaria, proporcionada y apropiada en una sociedad democrática, entre otras cosas, para la prevención, investigación, detección y persecución de delitos. Según la propuesta, el artículo 15, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas se aplica por analogía en aquellos supuestos en que la propuesta limita el ejercicio de los derechos y las obligaciones previstos en el artículo 5, apartados 1 y 3, y en el artículo 6, apartado 1, de dicha Directiva.

18. El CEPD y el SEPD recuerdan que el TJUE ha dejado claro que el artículo 15, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas debe interpretarse en sentido estricto, lo que significa que la excepción al principio de la confidencialidad de las comunicaciones autorizada por el artículo 15, apartado 1, debe seguir siendo una excepción y no debe convertirse en la regla[30]. Como se expone más adelante en el presente Dictamen conjunto, el CEPD y el SEPD consideran que la propuesta no satisface los requisitos de (estricta) necesidad, eficacia y proporcionalidad. Asimismo, el CEPD y el SEPD concluyen que la propuesta implica que la injerencia en la confidencialidad de las comunicaciones podría convertirse *de facto* en la regla, en lugar de seguir siendo la excepción.

4.1.2 Relación con el Reglamento (UE) 2021/1232 e impacto en la detección voluntaria de abuso sexual de menores en línea

19. De conformidad con el artículo 88 de la propuesta, esta derogaría el Reglamento provisional, que establece una excepción temporal a determinadas disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas para permitir el uso voluntario de tecnologías por prestadores de servicios de comunicaciones interpersonales independientes de la numeración para la detección de

[29] 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) (Texto pertinente a efectos del EEE) (DO L 119 de 4.5.2016, pp. 1 a 88).
[30] Sentencia de 21 de diciembre de 2016, asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB y Watson, apartado 89.

material de abuso sexual de menores desconocido y el embaucamiento de menores. Por consiguiente, a partir de la fecha de aplicación del Reglamento propuesto, no existiría excepción alguna a la Directiva sobre la privacidad y las comunicaciones electrónicas que permitiera la detección voluntaria de abusos sexuales de menores en línea por parte de dichos prestadores.

20. Puesto que las obligaciones de detección introducidas por la propuesta únicamente se aplicarían a los destinatarios de órdenes de detección, convendría aclarar en el texto del Reglamento propuesto que el uso voluntario de tecnologías para la detección de material de abuso sexual de menores desconocido y el embaucamiento de menores continúa estando autorizado en la medida en que lo permitan la Directiva sobre la privacidad y las comunicaciones electrónicas y el RGPD. Esto implicaría, por ejemplo, que los prestadores de servicios de comunicaciones interpersonales independientes de la numeración no podrían usar dichas tecnologías de forma voluntaria, a menos que dicho uso esté autorizado en virtud de las leyes nacionales que transpongan la Directiva sobre la privacidad y las comunicaciones electrónicas, de conformidad con el artículo 15, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas y con la Carta.

21. En términos más generales, convendría aclarar en el Reglamento propuesto la situación de la detección voluntaria de abusos sexuales de menores en línea tras su entrada en vigor, así como la transición del régimen de detección voluntaria previsto en el Reglamento provisional a las obligaciones de detección establecidas en el Reglamento propuesto. Por ejemplo, el CEPD y el SEPD recomiendan aclarar que el Reglamento propuesto no constituiría un fundamento jurídico para el tratamiento de datos personales con el único objetivo de detectar abusos sexuales de menores en línea de forma voluntaria.

4.2 Fundamento jurídico en virtud del RGPD

22. La propuesta tiene por objeto establecer un fundamento jurídico, en el sentido del RGPD, para el tratamiento de datos personales con el fin de detectar material de abuso sexual de menores desconocido y el embaucamiento de menores. En consecuencia, en la exposición de motivos se indica lo siguiente: «Por lo que se refiere a las actividades de detección obligatorias que implican el tratamiento de datos personales, la propuesta, en particular las órdenes de detección dictadas sobre esta base, establece el motivo para el tratamiento a que se refiere el artículo 6, apartado 1, letra c), del RGPD, que prevé el tratamiento de datos personales necesario para el cumplimiento de una obligación legal en virtud del Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento»[31].

23. El CEPD y el SEPD aplauden la decisión de la Comisión de acabar con la inseguridad jurídica con respecto al fundamento jurídico del tratamiento de datos personales que ha suscitado el Reglamento provisional. El CEPD y el SEPD coinciden también con la conclusión de la Comisión de que las consecuencias de la implantación de medidas de detección tienen un alcance demasiado amplio y son demasiado graves como para dejar la decisión de implementarlas o no en manos de los prestadores de servicios[32]. Al mismo tiempo, el CEPD y el SEPD señalan que cualquier fundamento jurídico que obligue a los prestadores de servicios a interferir con los derechos fundamentales a la protección de datos y la vida privada solo será válido en la medida en que respete los requisitos estipulados en el artículo 52, apartado 1, de la Carta, tal y como se analiza en las siguientes secciones.

[31] Ibíd., p. 5.
[32] COM(2022) 209 final, p. 16.

4.3 Obligaciones de evaluación y mitigación de riesgos

24. En virtud del capítulo II, sección 1, de la propuesta, los prestadores de servicios de alojamiento de datos y los prestadores de servicios de comunicaciones interpersonales deben determinar, analizar y evaluar, para cada uno de los servicios que ofrezcan, el riesgo de uso del servicio con fines de abuso sexual de menores en línea, y tratar de minimizar el riesgo que detecten aplicando «medidas razonables de reducción del riesgo, adaptadas al riesgo determinado».

25. El CEPD y el SEPD señalan que, cuando lleve a cabo una evaluación del riesgo, el prestador debe tener en cuenta en particular los elementos enumerados en el artículo 3, apartado 2, letras a) a e), de la propuesta, entre los que se incluyen las prohibiciones y restricciones establecidas en las condiciones del prestador de servicios; la forma en que los usuarios utilizan el servicio y la repercusión de dicho uso en el riesgo; la forma en que el prestador ha diseñado y explota el servicio, incluidos el modelo de negocio, la gobernanza y los sistemas y procesos pertinentes, y su repercusión en el riesgo. En cuanto al riesgo de embaucamiento de menores, los elementos propuestos que deben tenerse en cuenta son: la medida en que el servicio sea utilizado o exista la probabilidad de que sea utilizado por menores; los diferentes grupos de edad de los usuarios menores y el riesgo de embaucamiento en relación con esos grupos de edad, y la disponibilidad de funcionalidades que permitan que los usuarios busquen a otros usuarios, establezcan contacto directo con otros usuarios, en particular a través de comunicaciones privadas, o compartan imágenes o vídeos con otros usuarios.

26. Aunque el CEPD y el SEPD reconocen que estos criterios parecen relevantes, les preocupa que dejan un margen bastante amplio de interpretación y apreciación. Varios de estos criterios se describen con términos extremadamente genéricos (p. ej.: «la forma en que los usuarios utilizan el servicio y la repercusión de dicho uso en el riesgo») o se refieren a funcionalidades básicas comunes a muchos servicios en línea (p. ej., «que permitan que los usuarios compartan imágenes o vídeos con otros usuarios»). En consecuencia, los criterios parecen proclives a una valoración subjetiva, en vez de objetiva.

27. El CEPD y el SEPD opinan que ocurre lo mismo con las medidas de reducción del riesgo que deben adoptarse de conformidad con el artículo 4 de la propuesta. Medidas como la adaptación, a través de medidas técnicas, operativas y de dotación de personal adecuadas, de los sistemas de moderación de contenidos o de recomendación del prestador parecen relevantes para reducir el riesgo identificado. No obstante, si se adoptan en el marco de un proceso complejo de evaluación de riesgos y se combinan con el uso de términos abstractos y vagos para describir el nivel aceptable de riesgo (p. ej., «de manera apreciable»), estos criterios no cumplen los requisitos de seguridad jurídica y previsibilidad necesarios para justificar la injerencia en la confidencialidad de las comunicaciones entre particulares, lo que constituye una injerencia clara en los derechos fundamentales a la vida privada y a la libertad de expresión.

28. Aunque los prestadores no están autorizados a interferir en la confidencialidad de las comunicaciones como parte de sus estrategias de evaluación y reducción de riesgos antes de recibir una orden de detección, existe un vínculo directo entre las obligaciones de evaluación y reducción de riesgos y las consiguientes obligaciones de detección. El artículo 7, apartado 4, de la propuesta supedita la emisión de una orden de detección a la existencia de pruebas de un riesgo significativo de que el servicio en cuestión se esté utilizando para fines de abuso sexual de menores en línea. Antes de que se dicte una orden de detección, se debe seguir un proceso complejo en el que intervengan los prestadores, la autoridad de coordinación y la autoridad judicial u otra autoridad administrativa independiente encargada de su emisión. En primer lugar, los prestadores deben evaluar el riesgo de que sus servicios se utilicen con fines de abuso sexual de menores en línea (artículo 3 de la propuesta) y valorar posibles

medidas de reducción del riesgo (artículo 4 de la propuesta) para mitigarlo. A continuación, deberán comunicar los resultados de este ejercicio a la autoridad de coordinación competente (artículo 5 de la propuesta). Si la evaluación de riesgos demuestra que sigue existiendo un riesgo importante a pesar de los esfuerzos realizados para reducirlo, la autoridad de coordinación escuchará al prestador acerca de un proyecto de solicitud para la emisión de una orden de detección y le dará la posibilidad de hacer observaciones. En el caso de que se detecte embaucamiento de menores, el prestador está además obligado a presentar un plan de ejecución que incluya un dictamen de la autoridad de protección de datos competente. Si la autoridad de coordinación sigue adelante con el caso, se solicita una orden de detección que un órgano jurisdiccional u otra autoridad administrativa independiente finalmente emite. Por lo tanto, la evaluación de riesgos inicial y las medidas que se elijan para reducir el riesgo encontrado son una base determinante para que la autoridad de coordinación y la autoridad judicial o administrativa competente valoren si es necesaria una orden de detección.

29. El CEPD y el SEPD toman nota de los complejos pasos que han de seguirse para la emisión de una orden de detección, tales como la evaluación inicial de riesgos por el prestador y la propuesta por su parte de medidas de reducción de riesgos, seguida de su interacción con la autoridad de coordinación competente. El CEPD y el SEPD consideran que hay muchas posibilidades de que el prestador influya en el resultado del proceso. En este sentido, el CEPD y el SEPD señalan que el considerando 17 de la propuesta estipula que los prestadores deben poder indicar, como parte de la notificación de riesgos, «su voluntad y preparación» para que, en última instancia, se dicte una orden de detección. Por consiguiente, no se puede asumir que todos los prestadores tratarán de evitar la emisión de una orden de detección para preservar la confidencialidad de las comunicaciones de sus usuarios aplicando las medidas de reducción de los riesgos más efectivas y menos intrusivas, especialmente cuando dichas medidas de reducción interfieran con la libertad de empresa del prestador consagrada en el artículo 16 de la Carta.

30. El CEPD y el SEPD desean insistir en que las garantías procesales nunca pueden reemplazar por completo a las garantías sustantivas. Por lo tanto, el complejo proceso conducente a la posible emisión de una orden de detección que se ha descrito antes debería ir acompañado de unas obligaciones sustantivas claras. El CEPD y el SEPD consideran que la propuesta es poco clara en varios elementos clave (p. ej., los conceptos de «riesgo significativo» o «de manera apreciable»), lo cual no puede remediarse con la presencia de varios niveles de garantías procesales. Esto es aún más relevante en vista de que las entidades encargadas de aplicar dichas garantías (p. ej., los prestadores, las autoridades judiciales, etc.) disfrutan de un amplio margen de apreciación respecto a cómo conciliar los derechos en liza en cada caso particular. Habida cuenta de las enormes injerencias en derechos fundamentales que se derivarían de la adopción de la propuesta, el legislador debería asegurarse de que esta arroje una mayor claridad respecto a los momentos y circunstancias particulares en que están permitidas tales injerencias. Si bien admiten que las medidas legislativas no pueden ser demasiado prescriptivas y deben permitir cierta flexibilidad en su aplicación práctica, el CEPD y el SEPD consideran que la redacción actual de la propuesta deja demasiado margen para posibles abusos debido a la inexistencia de unas normas sustantivas claras.

31. Puesto que podría tener un impacto significativo para una gran cantidad de interesados (potencialmente, todos los usuarios de servicios de comunicaciones interpersonales), el CEPD y el SEPD hacen hincapié en la necesidad de que la legislación aporte un alto nivel de seguridad jurídica, claridad y previsibilidad, a fin de garantizar que las medidas propuestas sean realmente efectivas para alcanzar el objetivo que persiguen y, al mismo tiempo, sean lo menos perjudiciales posible para los derechos fundamentales en juego.

4.4 Condiciones para la emisión de órdenes de detección

32. El artículo 7 de la propuesta estipula que la autoridad de coordinación del país de establecimiento estará facultada para solicitar a la autoridad judicial competente, o a otra autoridad administrativa independiente de ese Estado miembro, que emita una orden de detección por la que se exija a un prestador de servicios de alojamiento de datos o a un prestador de servicios de comunicaciones interpersonales que adopte las medidas especificadas en el artículo 10 para detectar los abusos sexuales de menores en línea en un servicio específico.

33. El CEPD y el SEPD tienen debidamente en cuenta las siguientes condiciones que deben darse antes de la emisión de una orden de detección:

    a. existen pruebas de un riesgo significativo de que el servicio se esté utilizando para fines de abuso sexual de menores en línea, en el sentido del artículo 7, apartados 5, 6 y 7, según proceda;

    b. los motivos para emitir la orden de detección compensan las consecuencias negativas en los derechos e intereses legítimos de todas las partes afectadas, teniendo en cuenta, en particular, la necesidad de garantizar un equilibrio justo entre los derechos fundamentales de dichas partes.

34. El significado de «riesgo significativo» se especifica en el artículo 7, apartado 5 y siguientes, dependiendo del tipo de orden de detección de que se trate. En el caso de las órdenes de detección relativas a la difusión de material de abuso sexual de menores conocido, se asumirá que existe un riesgo significativo cuando se cumplan las siguientes condiciones:

    a. es probable que el servicio se utilice de manera apreciable para la difusión de material conocido de abuso sexual de menores, a pesar de las medidas de reducción del riesgo que el prestador haya adoptado o vaya a adoptar;

    b. hay pruebas de que el servicio, o un servicio comparable si el servicio aún no se ha ofrecido en la Unión en la fecha de la solicitud de emisión de la orden de detección, se ha utilizado en los últimos doce meses y en una medida apreciable para la difusión de material conocido de abuso sexual de menores.

35. Para que se dicte una orden de detección de material desconocido de abuso sexual de menores, debe existir la posibilidad y pruebas objetivas de que el servicio se usa para difundir material nuevo de abuso sexual de menores, se debe haber emitido una orden de detección relativa a la difusión de material conocido de abuso sexual de menores, y el prestador debe haber presentado un número significativo de denuncias relativas a material de abuso sexual de menores (artículo 7, apartado 6, de la propuesta). En cuanto a las órdenes de detección relativas al embaucamiento de menores, se considerará que existe un riesgo significativo cuando el prestador cumpla los requisitos para ser considerado prestador de servicios de comunicaciones interpersonales, sea probable que el servicio se utilice de manera apreciable para el embaucamiento de menores, y haya pruebas de que el servicio se ha utilizado en los últimos doce meses y en una medida apreciable para el embaucamiento de menores (artículo 7, apartado 7, de la propuesta).

36. El CEPD y el SEPD observan que, incluso con las especificaciones del artículo 7, apartados 5 a 7, de la propuesta, las condiciones para la emisión de una orden de detección contienen una gran cantidad de términos jurídicos vagos como «medida apreciable» o «número significativo», y son en parte repetitivas, ya que la existencia de pruebas de anteriores abusos normalmente llevará a determinar la probabilidad de futuros abusos.

37. La propuesta prevé un sistema con el que, cuando se decida si una orden de detección es necesaria, habrá que vaticinar si un servicio se usará en el futuro con el fin de cometer abusos sexuales de menores en línea. Por lo tanto, resulta comprensible que las condiciones establecidas en el artículo 7 tengan carácter pronóstico. No obstante, el uso en la propuesta de conceptos vagos dificulta que los prestadores, así como la autoridad judicial competente u otra autoridad administrativa independiente debidamente facultada, apliquen los requisitos jurídicos introducidos por la propuesta de manera predecible y no arbitraria. Al CEPD y el SEPD les preocupa que estos conceptos amplios y vagos den lugar a inseguridad jurídica y a unas divergencias considerables en la ejecución concreta de la propuesta en la Unión, pues dependerá de cómo interpreten las autoridades judiciales u otras autoridades administrativas independientes de los Estados miembros conceptos como «probabilidad» y «en una medida apreciable». Un resultado así no sería aceptable, dado que las disposiciones relativas a las órdenes de detección para prestadores de servicios de comunicaciones interpersonales constituirán «limitaciones» al principio de confidencialidad de las comunicaciones establecido en el artículo 5 de la Directiva sobre la privacidad y las comunicaciones electrónicas y, por lo tanto, es sumamente importante que sean claras y previsibles, a fin de garantizar que estas limitaciones se apliquen de manera uniforme en toda la Unión.

4.5 Análisis de la necesidad y proporcionalidad de las medidas previstas [33]

38. Como se ha indicado anteriormente, se pueden dictar tres tipos de órdenes de detección: órdenes de detección relativas a la difusión de material de abuso sexual de menores conocido (artículo 7, apartado 5, de la propuesta), órdenes de detección relativas a la difusión de nuevo material de abuso sexual de menores (artículo 7, apartado 6, de la propuesta) y órdenes de detección relativas al embaucamiento de menores (artículo 7, apartado 7, de la propuesta). Por lo general, cada orden de detección requerirá una tecnología distinta para su ejecución práctica. En consecuencia, son intrusivas a distintos niveles y, por tanto, afectan de manera diferente a los derechos a la vida privada y a la protección de los datos personales.

39. Las tecnologías usadas para detectar material de abuso sexual de menores conocido suelen ser tecnologías de correspondencia, en el sentido de que se apoyan en una base de datos existente de material de abuso sexual de menores conocido con la que pueden cotejar imágenes, incluidas capturas de vídeos. Para poder realizar el cotejo, las imágenes que el prestador trata y las que figuran en la base de datos deben haberse digitalizado, lo que por lo general se hace convirtiéndolas en valores resumen. Esta clase de tecnología de resumen tiene una tasa estimada de falsos positivos de no más de 1 en 50 000 millones o, lo que es lo mismo, del 0,000000002 %. [34]

40. Para detectar material nuevo de abuso sexual de menores, se suele usar otro tipo de tecnología, como los clasificadores y la inteligencia artificial (IA)[35]. Sin embargo, por lo general sus tasas de error son

---

[33] Véase también *The EDPS quick guide to necessity and proportionality* [«Guía rápida del SEPD para determinar la necesidad y la proporcionalidad», documento no disponible en español], que se puede consultar en: https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

[34] Véase Comisión Europea, documento de trabajo de los servicios de la Comisión, *Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse* [«Evaluación de impacto que acompaña a la propuesta de Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores», documento no disponible en español], SWD(2022) 209 final (en lo sucesivo, la «evaluación de impacto» o «el documento SWD(2022) 209 final»), p. 281, nota al pie 511.

[35] Evaluación de impacto, p. 281.

significativamente mayores. Por ejemplo, la evaluación de impacto indica que hay tecnologías para la detección de material nuevo de abuso sexual de menores con una tasa de precisión del 99,9 % (es decir, tienen una tasa de falsos positivos del 0,1 %), pero con dicha tasa de precisión solo son capaces de identificar el 80 % de todos los materiales de abuso sexual de menores en el conjunto de datos correspondiente[36].

41. Por otro lado, la evaluación de impacto explica que la detección de embaucamiento de menores en comunicaciones por escrito se suele basar en la detección de patrones. La evaluación de impacto señala que algunas de las tecnologías existentes para detectar embaucamiento de menores tienen una «tasa de precisión» del 88 %[37]. Según la Comisión, esto significa que «de las 100 conversaciones señaladas como posible embaucamiento ilícito de menores, 12 pueden excluirse tras su revisión [según la propuesta, por el Centro de la UE] y no se denunciarán a las fuerzas y cuerpos de seguridad»[38]. No obstante, aunque la propuesta se aplicaría también a las comunicaciones de audio —no así el Reglamento provisional—, la evaluación de impacto no profundiza en las soluciones tecnológicas que podrían usarse para detectar embaucamiento de menores en ese contexto.

4.5.1 Eficacia de la detección

42. La necesidad implica que se requiere una evaluación basada en hechos sobre la eficacia de las medidas previstas para alcanzar el objetivo perseguido y sobre si resulta menos intrusiva en comparación con otras opciones para lograr el mismo objetivo[39]. Otro factor que debe tenerse en cuenta en la evaluación de la proporcionalidad de una medida propuesta es la eficacia de las medidas existentes por encima de la propuesta[40]. Si ya existen medidas para un propósito similar o idéntico, su eficacia debe evaluarse como parte de la evaluación de la proporcionalidad. Sin esa evaluación de la eficacia de las medidas existentes que persiguen un objetivo similar o el mismo, no se puede considerar que se haya realizado debidamente la evaluación de la proporcionalidad de una nueva medida.

43. La detección de material de abuso sexual de menores o captación de menores por parte de los prestadores de servicios de alojamiento de datos y los prestadores de servicios de comunicaciones interpersonales puede contribuir al objetivo general de prevenir y combatir el abuso sexual de menores y la difusión en línea de material de abuso sexual de menores. Al mismo tiempo, la necesidad de evaluar la eficacia de las medidas previstas en la propuesta desencadena tres preguntas esenciales:

- ¿Es posible eludir con facilidad las medidas orientadas a detectar abuso sexual de menores en línea?

[36] Ibíd., p. 282.
[37] Ibíd., p. 283.
[38] Propuesta, COM(2022) 209 final, p. 16, nota al pie 32.
[39] Véanse SEPD, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit* [«Herramientas para determinar la necesidad de medidas que limiten el derecho fundamental a la protección de los datos personales», documento no disponible en español], 11 de abril de 2017, p. 5; y SEPD, *Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales*, 19 de diciembre de 2019, p. 9.
[40] SEPD, *Directrices del SEPD para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales*, 19 de diciembre de 2019, p. 10.

- ¿Qué repercusiones tendrán las actividades de detección en la actuación de las autoridades policiales?[41]
- ¿Cómo reduciría la propuesta la inseguridad jurídica?

44. No corresponde al CEPD y el SEPD responder a estas preguntas de manera pormenorizada. No obstante, señalan que ni la evaluación de impacto ni la propuesta abordan estas cuestiones por completo.

45. En cuanto a la posibilidad de eludir la detección de material de abuso sexual de menores, cabe señalar que al parecer en la actualidad no existe una solución tecnológica para detectar los materiales de abuso sexual de menores que se comparten de forma cifrada. Por lo tanto, es posible eludir cualquier actividad de detección, incluidos los escaneos desde el cliente destinados a esquivar el cifrado de extremo a extremo del prestador [42], mediante el cifrado del contenido con una aplicación independiente antes de enviarlo o subirlo. Por consiguiente, es posible que las medidas de detección previstas en la propuesta tengan un impacto en la difusión por internet de material de abuso sexual de menores menor del que cabría esperar.

46. Por otra parte, la Comisión espera que el número de denuncias de abuso sexual de menores presentadas a las autoridades policiales aumente cuando se adopten las obligaciones de detección que introduce la propuesta[43]. Sin embargo, ni la propuesta ni la evaluación de impacto explican cómo resolverá esto las deficiencias de la situación actual. Habida cuenta de los escasos recursos de las autoridades policiales, parece necesario dilucidar si el aumento del número de denuncias repercutiría de manera significativa en las actividades policiales contra el abuso sexual de menores. Sea como fuere, el CEPD y el SEPD desean hacer hincapié en que dichas denuncias se deben evaluar con prontitud para garantizar que se tome lo antes posible una decisión con respecto a la relevancia delictiva del material denunciado y para limitar lo máximo lo posible la retención de datos irrelevantes.

4.5.2 No es la medida menos invasiva

47. Suponiendo que se pudieran conseguir los efectos positivos de la detección de material de abuso sexual de menores y embaucamiento de menores contemplados por la Comisión, la detección debe ser la medida menos invasiva en comparación con otras medidas igual de efectivas. El artículo 4 de la propuesta establece que, como primer paso, los prestadores deben plantearse adoptar medidas para reducir el riesgo de que su servicio se utilice con el fin de cometer abuso sexual de menores en línea por debajo del umbral que justifica la emisión de una orden de detección. Si existen medidas que podrían reducir sustancialmente la cantidad de comunicaciones con fines de captación de menores o de material de abuso sexual de menores que se intercambian en el servicio en cuestión, estas medidas normalmente serían menos invasivas que una orden de detección[44]. Por lo tanto, si el prestador correspondiente no adoptase dichas medidas de forma voluntaria, la autoridad administrativa independiente o la autoridad judicial competente debería poder dotar de carácter obligatorio y ejecutivo a la implementación de medidas de reducción, en lugar de dictar una orden de detección. El

[41] Según la evaluación de impacto, anexo II, p. 132, el 85,71 % de los miembros de las autoridades policiales que respondieron la encuesta manifestaron su preocupación por el aumento de la cantidad de material de abuso sexual de menores en la última década y por la falta de recursos (humanos y técnicos, entre otros).
[42] Véase más información en el apartado 4.10.
[43] Véase, entre otros, evaluación de impacto, anexo 3, SWD(2022) 209 final, p. 176.
[44] Por ejemplo, se podrían valorar medidas como bloquear desde el cliente la transmisión de material de abuso sexual de menores impidiendo la subida y el envío de contenido, ya que en determinados contextos podrían ayudar a evitar la circulación de material de abuso sexual de menores conocido.

CEPD y el SEPD consideran que el hecho de que el artículo 5, apartado 4, de la propuesta permita a la autoridad de coordinación «exigir» al prestador que introduzca, revise, interrumpa o amplíe las medidas de reducción del riesgo no es suficiente, ya que dicha exigencia no podría hacerse valer de manera independiente y su incumplimiento únicamente «se sancionaría» con la emisión de una orden de detección.

48. En consecuencia, el CEPD y el SEPD consideran que la autoridad de coordinación o la autoridad administrativa independiente o la autoridad judicial competente deberían estar explícitamente facultadas para imponer medidas de reducción del riesgo menos intrusivas antes de dictar una orden de detección o como alternativa a su emisión.

4.5.3 Proporcionalidad en el sentido estricto de la palabra

49. Para que una medida respete el principio de proporcionalidad consagrado en el artículo 52, apartado 1, de la Carta, los beneficios que genere deben ser mayores que los perjuicios que ocasione en relación con el ejercicio de derechos fundamentales. Por tanto, el principio de proporcionalidad «limita a las autoridades en el ejercicio de sus facultades al exigir que se encuentre un equilibrio entre los medios usados y el objetivo que se desea lograr (o el resultado que se alcanza)»[45].

50. Para poder evaluar el impacto de una medida en los derechos fundamentales a la vida privada y a la protección de los datos personales, es especialmente importante identificar con precisión: [46]

- el **alcance de la medida**, incluido el número de personas afectadas y si plantea «intrusiones colaterales», es decir, injerencias en la intimidad de personas distintas de los sujetos de la medida;
- la **magnitud de la medida**, lo que incluye la cantidad de información recogida, durante cuánto tiempo, si la medida examinada requiere la recogida y el tratamiento de categorías especiales de datos;
- el **nivel de intrusión**, tomando en cuenta: la naturaleza de la actividad sometida a la medida (si afecta a actividades cubiertas por el deber de confidencialidad o no, la relación abogado-cliente; actividad médica); el contexto; si equivale a la elaboración de perfiles de las personas afectadas o no; si el tratamiento implica el uso de un sistema de toma de decisiones (parcial o totalmente) automatizado con un «margen de error»;
- si afecta a **personas vulnerables** o no;

[45] Véanse asunto C-343/09, Afton Chemical, apartado 45; asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke y Hartmut Eifert, apartado 74; asuntos C-581/10 y C-629/10, Nelson y otros, apartado 71; asunto C-283/11, Sky Österreich, apartado 50; y asunto C-101/12, Schaible, apartado 29. Véase asimismo SEPD, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit* [«Herramientas para determinar la necesidad de medidas que limiten el derecho fundamental a la protección de los datos personales», documento no disponible en español], 11 de abril de 2017.

[46] SEPD, *Directrices para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales*, 19 de diciembre de 2019, p. 23.

- si también afecta a **otros derechos fundamentales** (por ejemplo, el derecho a la libertad de expresión, como en los asuntos Digital Rights Ireland y Seitlinger y otros y Tele2 Sverige y Watson)[47].

51. En este contexto, también es importante señalar que el impacto puede ser menor en lo que respecta a la persona en cuestión y, sin embargo, significativo o muy significativo en lo que respecta a la sociedad en su conjunto[48].

52. En los tres tipos de órdenes de detección (detección de material de abuso sexual de menores conocido y nuevo, y de embaucamiento de menores), las tecnologías actualmente disponibles se basan en el tratamiento automatizado de datos de contenido de todos los usuarios afectados. Por lo general, las tecnologías utilizadas para analizar el contenido son complejas y suelen implicar el uso de IA. En consecuencia, es posible que el usuario del servicio no entienda totalmente el comportamiento de esta tecnología. Además, se sabe que las tecnologías actualmente disponibles, y en especial las usadas para detectar material nuevo de abuso sexual de menores o captación de menores, tienen unas tasas de error relativamente elevadas[49]. Asimismo, existe el riesgo de ser denunciado al Centro de la UE en virtud del artículo 12, apartado 1, y el artículo 48, apartado 1, de la propuesta a raíz de la detección de «posible» material de abuso sexual de menores.

53. Del mismo modo, las condiciones generales que se plantean en la propuesta para la emisión de una orden de detección, como que se aplique a todo un servicio y no solo a determinadas comunicaciones[50] o que tenga un período de vigencia de veinticuatro meses para el material de abuso sexual de menores conocido o nuevo y de doce meses en el caso del embaucamiento de menores[51], pueden llevar a que, en la práctica, la orden tenga un alcance muy amplio. Como consecuencia de esto, el seguimiento sería en realidad general e indiscriminado, en lugar de selectivo en la práctica.

54. En vista de lo anterior, el CEPD y el SEPD también manifiestan su preocupación por los posibles efectos paralizadores para el ejercicio de la libertad de expresión. El CEPD y el SEPD recuerdan que dicho efecto paralizador se considera más probable cuanto menos clara es la normativa.

55. Dado que carece de la especificidad, precisión y claridad exigidas para cumplir la exigencia de seguridad jurídica[52] y habida cuenta de su amplio alcance, ya que se aplica a todos los prestadores de servicios de la sociedad de la información pertinentes que ofrezcan tales servicios en la Unión[53], la propuesta no garantiza que la detección de material de abuso sexual de menores y captación de menores solo se vaya a abordar efectivamente con un enfoque selectivo. Por consiguiente, el CEPD y el SEPD consideran que, en la práctica, la propuesta podría convertirse en el fundamento para un escaneo generalizado e indiscriminado *de facto* del contenido de prácticamente todos los tipos de comunicaciones electrónicas de todos los usuarios de la UE/el EEE. En consecuencia, la legislación

---

[47] Véase también SEPD, *Opinion 7/2020 on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online* [«Dictamen 7/2020 sobre la propuesta relativa a la aplicación de excepciones temporales a la Directiva 2002/58/CE para combatir el abuso sexual de menores en línea», documento no disponible en español], 10 de noviembre de 2020, p. 9 y siguientes.

[48] SEPD, *Directrices para la evaluación de la proporcionalidad de las medidas que limitan los derechos fundamentales a la intimidad y a la protección de los datos personales*, 19 de diciembre de 2019, p. 20.

[49] Pueden consultarse más detalles al respecto en el apartado 4.5 y en el subapartado 4.8.2.

[50] Véase el artículo 7, apartado 1, de la propuesta.

[51] Véase el artículo 7, apartado 9, párrafo tercero, de la propuesta.

[52] TJUE, asunto C-197/96, Comisión de las Comunidades Europeas/República Francesa, apartado 15.

[53] Véase el artículo 1, apartado 2, de la propuesta.

podría llevar a la población a abstenerse de compartir contenido legal por temor a ser objeto de una orden de detección.

56. Dicho esto, el CEPD y el SEPD reconocen que las distintas medidas para combatir el abuso sexual de menores en línea pueden conllevar diferentes niveles de intrusión. Como cuestión preliminar, el CEPD y el SEPD observan que es probable que el análisis automatizado de locuciones o textos con vistas a identificar posibles casos de embaucamiento de menores suponga una mayor injerencia que el cotejo de imágenes o vídeos sobre la base de anteriores materiales de abuso sexual de menores confirmados para detectar la difusión de este tipo de contenidos. Asimismo, es preciso diferenciar entre la detección de material de abuso sexual de menores «conocido» y «nuevo». Del mismo modo, también hay que diferenciar el impacto de las medidas dirigidas a los prestadores de servicios de alojamiento de datos del que tienen las impuestas a los prestadores de servicios de comunicaciones interpersonales.

4.5.4 Detección de material de abuso sexual de menores conocido

57. Aunque según el considerando 4 la propuesta sería «tecnológicamente neutra», tanto la eficacia de las medidas de detección propuestas como su impacto para las personas dependerán en gran medida de la tecnología que se decida aplicar y de los indicadores seleccionados. Así lo reconoce la Comisión en la evaluación de impacto, anexo 8[54], y lo confirman otros estudios, tales como la evaluación de impacto sustitutiva específica del Servicio de Estudios del Parlamento Europeo, de febrero de 2021, relativa a la propuesta de la Comisión por la que se establece una excepción temporal a la Directiva sobre la privacidad y las comunicaciones electrónicas con fines de lucha contra el abuso sexual de menores en línea[55].

58. El artículo 10 de la propuesta establece una serie de requisitos que deben cumplir las tecnologías que se usarán con fines de detección, los cuales se refieren en particular a su eficacia, a su fiabilidad y a su carácter mínimamente intrusivo en lo que respecta a su impacto en los derechos de los usuarios a la vida privada y familiar, lo que incluye la confidencialidad de las comunicaciones, y a la protección de los datos personales.

59. En este contexto, el CEPD y el SEPD señalan que, en la actualidad, las únicas tecnologías que parecen poder cumplir en general estas condiciones son las que se utilizan para detectar material conocido de abuso sexual de menores, es decir, las tecnologías de correspondencia que toman como referencia una base de datos de valores resumen.

[54] Véase la información sobre las tasas de falsos positivos que figura en la evaluación de impacto, anexo 8, p. 279 y siguientes.
[55] Véase Servicio de Estudios del Parlamento Europeo, *Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse: Targeted substitute impact assessment* [«Evaluación de impacto sustitutiva específica sobre la propuesta de la Comisión por la que se establece una excepción temporal a la Directiva sobre la privacidad y las comunicaciones electrónicas con fines de lucha contra el abuso sexual de menores en línea», documento no disponible en español], febrero de 2021, p. 14 y siguientes.

4.5.5 Detección de material de abuso sexual de menores previamente desconocido

60. La evaluación de las medidas destinadas a detectar material de abuso sexual de menores previamente desconocido (es decir, nuevo) lleva a conclusiones diferentes en lo que respecta a su eficacia, fiabilidad y limitación del impacto en los derechos fundamentales a la privacidad y la protección de datos.

61. En primer lugar, tal y como se explica en la evaluación de impacto relativa a la propuesta, los clasificadores y la IA son algunas de las tecnologías que se usan actualmente para detectar material de abuso sexual de menores previamente desconocido. Un clasificador es cualquier algoritmo que, mediante el reconocimiento de patrones, ordena los datos por clases claramente identificadas o categorías de información[56]. Por consiguiente, estas tecnologías tienen distintos resultados y repercusiones en términos de precisión, eficacia y nivel de intrusión y, al mismo tiempo, también son más propensas a cometer errores.

62. Las técnicas utilizadas para detectar material de abuso sexual de menores previamente desconocido son similares a las usadas para detectar embaucamiento de menores, dado que ninguna de ellas se basa en simples tecnologías de correspondencia, sino en modelos predictivos que emplean tecnologías de IA. El CEPD y el SEPD consideran que es preciso proceder con suma cautela a la hora de detectar material de abuso sexual de menores previamente desconocido, ya que un error del sistema tendría graves consecuencias para los interesados, a los que automáticamente se señalaría como posibles autores de un delito muy grave, además de denunciar sus datos personales y los detalles de sus comunicaciones.

63. En segundo lugar, los indicadores de rendimiento que figuran en los estudios, algunos de los cuales se ponen de relieve en la evaluación de impacto que acompaña a la propuesta[57], aportan muy poca información sobre las condiciones en que se calcularon y su adecuación a las condiciones de la vida real, lo que significa que en la práctica su rendimiento podría ser muy inferior al esperado, de modo que podrían ser menos precisos y presentar un mayor porcentaje de «falsos positivos».

64. En tercer lugar, los indicadores de rendimiento deberían valorarse en el contexto específico en que se usan las herramientas de detección correspondientes y proporcionar información exhaustiva sobre el comportamiento de estas. Está demostrado que, cuando se aplican algoritmos de inteligencia artificial a imágenes o textos, pueden producirse sesgos y discriminación porque ciertos grupos demográficos no estaban representados en los datos utilizados para entrenar dichos algoritmos. Es preciso identificar, medir y reducir a un nivel aceptable estos sesgos, a fin de que los sistemas de detección realmente sean beneficiosos para la sociedad en su conjunto.

65. Aunque se ha realizado un estudio de las tecnologías usadas para la detección[58], el CEPD y el SEPD consideran que es necesario efectuar un análisis más profundo para evaluar la fiabilidad de las herramientas existentes. Este análisis debería basarse en indicadores del rendimiento exhaustivos y evaluar el impacto que tendrían posibles errores en condiciones reales para todos los interesados a los que afecta la propuesta.

66. Como se ha señalado anteriormente, el CEPD y el SEPD tienen serias dudas sobre si las garantías procesales previstas en el artículo 7, apartado 6, de la propuesta son suficientes para compensar estos riesgos. Asimismo, como se ha indicado previamente, señalan que la propuesta utiliza términos

[56] Evaluación de impacto, anexo 8, p. 281.
[57] Evaluación de impacto, anexo 8, pp. 281 a 283.
[58] Evaluación de impacto, p. 279 y siguientes.

bastante abstractos y vagos para describir el nivel aceptable de riesgo (p. ej., «en una medida apreciable»).

67. Al CEPD y el SEPD les preocupa que estos conceptos amplios y vagos den lugar a inseguridad jurídica y a unas divergencias considerables en la ejecución concreta de la propuesta en la Unión, pues dependerá de cómo interpreten las autoridades judiciales u otras autoridades administrativas independientes de los Estados miembros conceptos como «probabilidad» y «en una medida apreciable». Esto también resulta preocupante si se tiene en cuenta que las disposiciones de las órdenes de detección constituirán «limitaciones» al principio de confidencialidad establecido en el artículo 5 de la Directiva sobre la privacidad y las comunicaciones electrónicas. Por este motivo, resulta necesario mejorar su claridad y previsibilidad en el Reglamento propuesto.

4.5.6 Detección de embaucamiento de menores (captación de menores)

68. El CEPD y el SEPD señalan que es probable que las medidas propuestas para la detección de embaucamiento de menores (práctica también conocida como «captación de menores») que implican el análisis automatizado de locuciones o textos constituyan la mayor injerencia en los derechos de los usuarios a la vida privada y familiar, que engloba la confidencialidad de las comunicaciones, y a la protección de los datos personales.

69. Mientras que el alcance de la detección de material de abuso sexual de menores conocido, e incluso nuevo, puede limitarse al análisis de imágenes y vídeos, la detección de captación de menores abarcaría por definición todas las comunicaciones por escrito (y posiblemente de audio) que entren en el ámbito de aplicación de una orden de detección. En consecuencia, la intensidad de la injerencia en la confidencialidad de las comunicaciones afectadas es mucho mayor.

70. El CEPD y el SEPD consideran que el análisis automatizado generalizado e indiscriminado *de facto* de los mensajes escritos que se transmiten por medio de servicios de comunicaciones interpersonales con el objetivo de identificar posibles casos de embaucamiento de menores no respeta las condiciones de necesidad y proporcionalidad. Incluso aunque la tecnología utilizada se limite al uso de indicadores, el CEPD y el SEPD consideran que un análisis tan general e indiscriminado es excesivo y podría llegar a afectar a la esencia misma del derecho fundamental a la vida privada consagrado en el artículo 7 de la Carta.

71. Como ya se ha indicado, la ausencia de garantías sustantivas en el contexto de las medidas destinadas a detectar embaucamiento de menores no puede compensarse únicamente con garantías procesales. Además, el problema de la insuficiente claridad y seguridad jurídicas (p. ej., el uso de un lenguaje jurídico vago, como «en una medida apreciable») es aún más grave en el caso del análisis automatizado de las comunicaciones personales por escrito, en comparación con el cotejo de fotos basado en la tecnología de resumen.

72. Del mismo modo, el CEPD y el SEPD consideran que el «efecto paralizador» en la libertad de expresión es especialmente importante cuando se escanean y analizan a gran escala comunicaciones por escrito (o de audio) de particulares. El CEPD y el SEPD recuerdan que dicho efecto paralizador es más grave cuanto menos clara es la normativa.

73. Además, como se indica en la evaluación de impacto[59] y en el estudio del Servicio de Estudios del Parlamento Europeo[60], la tasa de precisión de las tecnologías usadas para detectar captación de menores en mensajes escritos es muy inferior a la de las tecnologías destinadas a detectar material de abuso sexual de menores conocido[61]. Las técnicas de detección de la captación de menores están diseñadas para analizar todos los aspectos de una conversación y asignarles puntuaciones de probabilidad, por lo que el CEPD y el SEPD también las consideran proclives a errores y vulnerables a usos indebidos.

4.5.7 Conclusión sobre la necesidad y proporcionalidad de las medidas previstas

74. En lo que respecta a la necesidad y proporcionalidad de las medidas de detección previstas, al CEPD y el SEPD les preocupan especialmente las medidas contempladas para detectar material de abuso sexual de menores desconocido y embaucamiento (o captación) de menores por su carácter intrusivo, al existir la posibilidad de que permitan acceder de forma generalizada al contenido de comunicaciones, por su naturaleza probabilística y por las tasas de error asociadas a dichas tecnologías.

75. Además, de la jurisprudencia del TJUE se puede inferir que las medidas que permiten a las autoridades públicas acceder de forma generalizada al contenido de una comunicación tienen más probabilidades de afectar al contenido esencial de los derechos garantizados en los artículos 7 y 8 de la Carta. Estas consideraciones son específicamente relevantes en lo que atañe a las medidas para la detección de embaucamiento de menores previstas en la propuesta.

76. Sea como fuere, el CEPD y el SEPD consideran que la injerencia que crean en particular las medidas para la detección de embaucamiento de menores va más allá de lo estrictamente necesario y proporcional. Por consiguiente, estas medidas deberían suprimirse de la propuesta.

4.6 Obligaciones de información

77. El CEPD y el SEPD recomiendan complementar la lista de requisitos específicos para la presentación de denuncias del artículo 13 de la propuesta con el requisito de incluir en la denuncia información sobre la tecnología concreta que el prestador utilizó para descubrir el contenido abusivo, en caso de que tomara conciencia del posible abuso sexual de menores tras adoptar medidas para ejecutar una orden de detección dictada de acuerdo con el artículo 7 de la propuesta.

4.7 Obligaciones de eliminación y bloqueo

78. Una de las medidas que contempla la propuesta para reducir el riesgo de que se difunda material de abuso sexual de menores es la emisión de órdenes de eliminación y bloqueo que obligarían a los prestadores a eliminar de sus servicios el material de abuso sexual de menores en línea, inhabilitar el acceso a él o bloquearlo[62].

79. Si bien las órdenes de eliminación tienen un impacto relativamente limitado en la protección de datos y la privacidad de las comunicaciones, el CEPD y el SEPD recuerdan, como observación

[59] Evaluación de impacto, anexo 8, pp. 281 a 283.
[60] Pp. 15 a 18.
[61] Véase el apartado 40.
[62] Propuesta, artículos 14 y 16.

general, el principio general que debe cumplirse: que cualquier medida de esta naturaleza debe ser lo más selectiva posible.

80. Al mismo tiempo, el CEPD y el SEPD señalan a la atención que los prestadores de servicios de acceso a internet solo pueden saber la URL precisa de un contenido si se ha publicado en texto no cifrado. Cuando el contenido se publique a través de HTTPS, el prestador de servicios de acceso a internet no tendrá forma de saber la URL exacta, a menos que descifre la comunicación. Por lo tanto, el CEPD y el SEPD albergan dudas con respecto a la eficiencia de las medidas de bloqueo, y consideran que sería desproporcionado exigir a los prestadores de servicios de acceso a internet que descifren las comunicaciones en línea para bloquear las relativas a material de abuso sexual de menores.

81. En términos más generales, cabe señalar también que bloquear (o inhabilitar) el acceso a un material digital es una operación que tiene lugar a nivel de la red y podría no ser efectiva si existen múltiples copias (posiblemente similares, pero no idénticas) del mismo material. Asimismo, dicha operación podría resultar desproporcionada si el bloqueo afecta a otros materiales digitales lícitos cuando están almacenados en el mismo servidor cuyo acceso se ha inhabilitado mediante comandos de red (p. ej., incluyendo en una lista negra direcciones IP o DNS). Del mismo modo, no todos los métodos de bloqueo a nivel de red son igual de efectivos, y algunos se pueden esquivar fácilmente con unas capacidades técnicas bastante básicas.

82. Por último, el Reglamento propuesto debería aclarar las facultades de las autoridades de coordinación en lo que respecta a la emisión de órdenes de bloqueo. Por ejemplo, con la redacción actual del artículo 16, apartado 1, y el artículo 17, apartado 1, no queda claro si las autoridades de coordinación están facultadas para emitir órdenes de bloqueo o solo para solicitar su emisión[63].

4.8 Tecnologías y garantías pertinentes

4.8.1 Protección de datos desde el diseño y por defecto

83. Los requisitos de la propuesta aplicables a las tecnologías que deben implementarse para detectar material de abuso sexual de menores y embaucamiento de menores no parecen lo suficientemente estrictos. En particular, el CEPD y el SEPD han observado que, al contrario de lo que ocurre en las disposiciones análogas del Reglamento provisional[64], la propuesta no hace referencia explícita al principio de la protección de datos desde el diseño y por defecto ni estipula que las tecnologías que se utilizan para escanear el texto de las comunicaciones no deben ser capaces de deducir la esencia del contenido de estas. La propuesta únicamente establece, en el artículo 10, apartado 3, letra b), que las tecnologías no deben ser capaces de «extraer» de las comunicaciones pertinentes ninguna otra información que no sea la estrictamente necesaria para la detección. No obstante, esta norma no

[63] El artículo 16, apartado 1, de la propuesta establece lo siguiente: «La autoridad de coordinación del país de establecimiento estará facultada para solicitar a la autoridad judicial competente del Estado miembro que la haya designado o a una autoridad administrativa independiente de dicho Estado miembro que dicte una orden de bloqueo […]». Por su parte, el artículo 17, apartado 1, dice lo siguiente: «La autoridad de coordinación del país de establecimiento emitirá las órdenes de bloqueo a que se refiere el artículo 16 […]» (subrayado añadido).
[64] Reglamento provisional, artículo 3, apartado 1, letra b).

parece lo suficientemente estricta, ya que podría ser posible *deducir* otra información de la esencia del contenido de una comunicación sin *extraer* información como tal de ella.

84. En consecuencia, el CEPD y el SEPD recomiendan introducir en la propuesta un considerando que estipule que el principio de la protección de datos desde el diseño y por defecto establecido en el artículo 25 del Reglamento (UE) 2016/679 se aplica por ley a las tecnologías reguladas por el artículo 10 de la propuesta, por lo que no era necesario repetirlo en el texto jurídico. Además, el artículo 10, apartado 3, letra b), debe modificarse para garantizar que no se pueda extraer ninguna otra información y tampoco pueda deducirse, como establece actualmente el artículo 3, apartado 1, letra b), del Reglamento provisional.

4.8.2 Fiabilidad de las tecnologías

85. La propuesta asume que los prestadores de servicios pueden utilizar varios tipos de soluciones tecnológicas para ejecutar las órdenes de detección. En particular, la propuesta parte de la base de que se cuenta con sistemas de inteligencia artificial que funcionan correctamente para detectar material de abuso sexual de menores desconocido y embaucamiento de menores[65], y que algunas autoridades de coordinación podrían considerarlos tecnologías punteras. Si bien la eficacia de la propuesta depende de la fiabilidad de estas soluciones tecnológicas, existe muy poca información sobre el uso generalizado y sistemático de estas técnicas, que merece ser estudiado con detenimiento.

86. Además, aunque el CEPD y el SEPD tuvieron que usarlos en su evaluación de la proporcionalidad porque no había alternativas, cabe señalar que los indicadores del rendimiento de las tecnologías de detección que se mencionan en la evaluación de impacto que acompaña a la propuesta aportan muy poca información sobre el modo en que se han evaluado y sobre si reflejan el rendimiento de las tecnologías pertinentes en la vida real. No hay información sobre las pruebas o los valores de referencia utilizados por los proveedores de estas tecnologías para medir sus rendimientos. Sin dicha información, es imposible replicar las pruebas o valorar la validez de las declaraciones de rendimiento. En este sentido, cabe señalar que, aunque se podría interpretar que los indicadores del rendimiento sugieren que algunas herramientas de detección son muy precisas (por ejemplo, algunas herramientas de detección de captación de menores tienen una precisión del 88 %)[66], estos indicadores deberían analizarse teniendo en cuenta el uso práctico previsto de las herramientas de detección y la gravedad de los riesgos que la evaluación incorrecta de un material acarrearía para los interesados correspondientes. Asimismo, el CEPD y el SEPD consideran que, al ser un tratamiento de tanto riesgo, una tasa de error del 12 % supone un riesgo elevado para los interesados que han sufrido falsos positivos, aun cuando existan garantías para evitar que se presenten denuncias falsas a las autoridades policiales. Es altamente improbable que los prestadores de servicios puedan destinar suficientes recursos a revisar un porcentaje tan alto de falsos positivos.

87. Como se ha mencionado previamente[67], los indicadores del rendimiento deberían proporcionar información exhaustiva sobre el comportamiento de las herramientas de detección. Está demostrado que, cuando se aplican algoritmos de inteligencia artificial a imágenes o textos, pueden producirse sesgos y discriminación porque ciertos grupos demográficos no estaban representados en los datos utilizados para entrenar dichos algoritmos. Es preciso identificar, medir y reducir a un nivel aceptable

[65] Véase la evaluación de impacto, pp. 281 y 282.
[66] Ibíd., p. 283.
[67] Véanse los apartados 63 y 64.

estos sesgos, a fin de que los sistemas de detección realmente sean provechosos para la sociedad en su conjunto.

88. Aunque se ha llevado a cabo un estudio de las tecnologías utilizadas para la detección[68], el CEDP y el SEPD consideran que es necesario realizar un análisis más pormenorizado, a fin de evaluar de manera independiente la fiabilidad de las herramientas existentes cuando se usan en el mundo real. Este análisis debería basarse en indicadores del rendimiento exhaustivos y evaluar el impacto que tendrían posibles errores en condiciones reales para todos los interesados a los que afecta la propuesta. Puesto que la propuesta se sustenta en estas tecnologías, el CEPD y el SEPD consideran que este análisis es crucial para valorar si la propuesta es adecuada.

89. El CEPD y el SEPD señalan también que la propuesta no define requisitos específicos para las tecnologías, ya sea en lo que respecta a las tasas de error, al uso de clasificadores y su validación, o a otras restricciones. De este modo, dichos criterios deben desarrollarse con la práctica cuando se evalúe la proporcionalidad de utilizar una tecnología concreta, lo que contribuye una vez más a la falta de precisión y claridad.

90. Dadas las importantes consecuencias que tienen los falsos positivos para los interesados, el CEPD y el SEPD consideran que es preciso reducir las tasas de falsos positivos al mínimo, y que dichos sistemas deben diseñarse sin olvidar que la gran mayoría de las comunicaciones electrónicas no contienen material de abuso sexual de menores ni embaucamientos de menores, y teniendo también presente que incluso una tasa de falsos positivos muy reducida implicará un número muy elevado de falsos positivos debido al volumen de los datos que se someterá a la detección. En términos más generales, al CEPD y el SEPD también les preocupa que el rendimiento de las herramientas disponibles que se indica en la evaluación de impacto no contiene indicadores precisos y comparables en relación con las tasas de falsos positivos y falsos negativos, y consideran que se deben crear indicadores del rendimiento comparables y significativos para dichas tecnologías antes de considerar que están disponibles y que son eficientes.

4.8.3 Escaneo de comunicaciones de audio

91. Al contrario que el Reglamento provisional[69], la propuesta no excluye de su ámbito de aplicación el escaneo de las comunicaciones de audio en el contexto de la detección de captación de menores[70]. El CEPD y el SEPD creen que el escaneo de comunicaciones de audio resulta especialmente intrusivo, ya que normalmente habría que interceptarlas de manera activa, continua y «en directo». Es más, en algunos Estados miembros, la privacidad del discurso oral goza de una protección especial[71]. Además, como en principio habría que analizar todo el contenido de las comunicaciones de audio, es probable que esta medida afecte a la esencia de los derechos garantizados en los artículos 7 y 8 de la Carta. Por este motivo, este método de detección debe quedar fuera del ámbito de las obligaciones de detección establecidas en el Reglamento propuesto en lo que respecta tanto a los mensajes de voz como a las comunicaciones en directo, especialmente habida cuenta de que la evaluación de impacto que

[68] Véase la evaluación de impacto, p. 279 y siguientes.
[69] Véase el Reglamento provisional, artículo 1, apartado 2.
[70] Véase la propuesta, artículo 1.
[71] Véase, por ejemplo, el Código Penal alemán, apartado 201.

acompaña a la propuesta no identificó ningún riesgo específico ni cambios en el panorama de amenazas que pudieran justificar su uso[72].

4.8.4 Verificación de la edad

92. La propuesta anima a los prestadores a utilizar medidas de verificación y evaluación de la edad para identificar a los usuarios menores en sus servicios[73]. Sobre esta cuestión, el CEPD y el SEPD señalan que en la actualidad no existe ninguna solución tecnológica capaz de evaluar con exactitud la edad de un usuario en un contexto virtual sin basarse en una identidad digital oficial, algo que en estos momentos no está al alcance de todos los ciudadanos europeos[74]. Por lo tanto, el uso de medidas de verificación de la edad que se contempla en la propuesta podría hacer que, por ejemplo, adultos que parecen más jóvenes de lo que son no puedan acceder a servicios en línea, o llevar a la implantación de herramientas de verificación de la edad muy intrusivas que podrían dificultar o desalentar el uso de los servicios afectados con fines legítimos.

93. En este sentido, y aunque el considerando 16 de la propuesta menciona las herramientas de control parental como posibles medidas de reducción del riesgo, el CEPD y el SEPD recomiendan que el Reglamento propuesto se modifique para permitir expresamente a los prestadores recurrir a mecanismos de control parental como medida adicional o alternativa a la verificación de la edad.

4.9 Conservación de la información

94. El artículo 22 de la propuesta limita las finalidades para las que los prestadores sujetos a la propuesta pueden conservar los datos de contenido y otros datos tratados en relación con las medidas adoptadas para cumplir las obligaciones establecidas en la propuesta. Sin embargo, la propuesta indica que los prestadores también podrán conservar esta información con el fin de mejorar la eficacia y exactitud de las tecnologías de detección de abusos sexuales de menores en línea para la ejecución de una orden de detección, pero que no podrán almacenar ningún dato personal a tal efecto[75].

95. El CEPD y el SEPD consideran que únicamente los prestadores que utilicen sus propias tecnologías de detección deberían poder conservar datos con el fin de mejorar la eficacia y exactitud de las tecnologías, mientras que los que usen las tecnologías que les facilite el Centro de la UE no deberían tener esta posibilidad. Del mismo modo, el CEPD y el SEPD señalan que, en la práctica, podría resultar difícil garantizar que no se almacene ningún dato personal a tal efecto, pues es probable que la mayoría de los datos de contenido y otros datos tratados con fines de detección sean datos personales.

4.10 Impacto en el cifrado

96. Las autoridades europeas de protección de datos han defendido sistemáticamente la disponibilidad generalizada de herramientas sólidas de cifrado y han luchado contra cualquier tipo de puerta trasera[76], ya que el cifrado es importante para garantizar el disfrute de todos los derechos humanos

[72] Véase la evaluación de impacto
[73] Véase la propuesta, artículo 4, apartado 3; artículo 6, apartado 1, letra c), y considerando 16.
[74] Véase, por ejemplo, la recomendación 7 del CNIL: «Comprobar la edad del menor y el consentimiento parental respetando, al mismo tiempo, la privacidad del menor» (9 de agosto de 2021).
[75] Propuesta, artículo 22, apartado 1.
[76] Véase, por ejemplo, Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, *Statement of the WP29 on encryption and their impact on the protection of individuals with regard*

tanto fuera como dentro de internet[77]. Asimismo, las tecnologías de cifrado contribuyen de una manera fundamental al respeto de la vida privada y la confidencialidad de las comunicaciones, así como a la innovación y al crecimiento de la economía digital, que se fundamenta en el elevado nivel de seguridad y confianza que proporcionan dichas tecnologías.

97. En el contexto de las comunicaciones interpersonales, el cifrado de extremo a extremo es una herramienta crucial para garantizar la confidencialidad de las comunicaciones electrónicas, ya que proporciona potentes medidas técnicas de seguridad para que nadie, salvo el emisor y los destinatarios, pueda acceder al contenido de las comunicaciones, incluido el prestador. Si se evitase o desalentase de alguna manera el uso del cifrado de extremo a extremo, se impusiera a los prestadores de servicios la obligación de tratar los datos de comunicaciones electrónicas con fines distintos de la prestación de sus servicios o se los obligase a remitir de manera proactiva comunicaciones electrónicas a terceros, se correría el riesgo de que los prestadores ofreciesen servicios menos cifrados para cumplir mejor sus obligaciones, lo que debilitaría la función del cifrado en general y socavaría el respeto por los derechos fundamentales de los ciudadanos europeos. Conviene señalar que, aunque el cifrado de extremo a extremo es una de las medidas de seguridad más utilizadas en el contexto de las comunicaciones electrónicas, es posible que otras soluciones técnicas (p. ej., la utilización de otros sistemas criptográficos) sean igualmente importantes para garantizar y proteger la confidencialidad de las comunicaciones digitales o lleguen a serlo. Por lo tanto, su uso tampoco debería evitarse ni desalentarse.

98. La implementación de herramientas para interceptar y analizar comunicaciones electrónicas interpersonales se opone fundamentalmente a cifrado de extremo a extremo, pues este último busca garantizar por medios técnicos que una comunicación siga siendo confidencial entre el emisor y el destinatario.

99. Por consiguiente, aunque la propuesta no impone una obligación de interceptación sistemática a los prestadores, es probable que la mera posibilidad de que se dicte una orden de protección influya enormemente en las decisiones técnicas de los prestadores, en especial debido al plazo reducido que tendrán para cumplir dicha orden y las duras sanciones a las que se enfrentarían si no lo hicieran[78]. En la práctica, esto podría hacer que ciertos prestadores dejen de utilizar el cifrado de extremo a extremo.

100. Es preciso evaluar adecuadamente las consecuencias que podría tener degradar o desalentar el uso del cifrado de extremo a extremo a raíz de la propuesta. Todas las técnicas para eludir el objetivo de preservar la privacidad del cifrado de extremo a extremo que se presentan en la evaluación de impacto que acompaña a la propuesta introducirían lagunas de seguridad[79]. Por ejemplo, los escaneos desde

---

to the processing of their personal data in the EU [«Declaración del Grupo de Trabajo del Artículo 29 sobre el cifrado y su impacto en la protección de las personas en lo que respecta al tratamiento de sus datos personales en la UE», documento no disponible en español], 11 de abril de 2018.

[77] Véase Consejo de Derechos Humanos, Resolución 47/16 sobre la promoción, protección y disfrute de los derechos humanos en Internet, documento de las Naciones Unidas A/HRC/RES/47/16, 26 de julio de 2021.

[78] Véase la propuesta, artículo 35.

[79] Véase Abelson, Harold, Ross J. Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague y Carmela Troncoso, *Bugs in our Pockets: The Risks of Client-Side Scanning* [«Micrófonos en nuestros bolsillos: los riesgos del escaneo desde el cliente», documento no disponible en español], ArXiv abs/2110.07450, 2021, apartado 4.2.

el cliente[80] desembocarían, con toda probabilidad, en el acceso considerable y generalizado a contenido no cifrado en los dispositivos de los usuarios finales y en su tratamiento. Una degradación tan importante de la confidencialidad afectaría especialmente a los menores, pues es más probable que los servicios que usan sean objeto de órdenes de detección, lo que los hace vulnerables a controles o escuchas. Al mismo tiempo, el escaneo *desde el servidor* también es incompatible en esencia con el paradigma del cifrado de extremo a extremo dado que habría que acceder al canal de comunicación, cifrado entre iguales, lo que se traduciría en el tratamiento en masa de los datos personales almacenados en los servidores de los prestadores.

101. Aunque la propuesta afirma que «deja en manos del prestador afectado la elección de las tecnologías que deben utilizarse para cumplir eficazmente las órdenes de detección y no debe entenderse en el sentido de que incentiva o desincentiva el uso de una tecnología determinada»[81], la incompatibilidad estructural de ciertas órdenes de detección con el cifrado de extremo a extremo constituye, en la práctica, un fuerte desincentivo para usar el cifrado de extremo a extremo. La imposibilidad de acceder a servicios con cifrado de extremo a extremo (actualmente los más punteros en términos de protección técnica de la confidencialidad) y utilizarlos podría tener un efecto paralizador en la libertad de expresión y el uso privado de los servicios de comunicaciones electrónicas con fines lícitos. La Comisión también reconoce la mala relación entre la detección de material de abuso sexual de menores o de la captación de menores y el cifrado de extremo a extremo al señalar, en la evaluación de impacto[82], la probabilidad de que, una vez que Facebook implante el cifrado de extremo a extremo en 2023, dejará de hacer escaneos voluntarios.

102. Para garantizar que el Reglamento propuesto no socave la seguridad o confidencialidad de las comunicaciones electrónicas de los ciudadanos europeos, el CEPD y el SEPD consideran que en la parte dispositiva de la propuesta se debería dejar claro que ninguna de las disposiciones del Reglamento propuesto debe interpretarse en el sentido de que prohíbe o debilita el cifrado, en línea con lo que se indica en el considerando 25 del Reglamento provisional.

4.11 Supervisión, ejecución y cooperación

4.11.1 Función de las autoridades de control nacionales conforme al RGPD

103. La propuesta prevé el establecimiento de una red de autoridades nacionales de coordinación, que tendrá la responsabilidad de aplicar y hacer cumplir el Reglamento propuesto[83]. Aunque el considerando 54 de la propuesta indica que «no debe entenderse que las normas del presente Reglamento sobre supervisión y ejecución afectan a las facultades y competencias de las autoridades de protección de datos en virtud del Reglamento (UE) 2016/679», el CEPD y el SEPD opinan que se debería regular mejor la relación entre las funciones de las autoridades de coordinación y las de las autoridades de protección de datos, y que a estas últimas se les debería otorgar un papel más destacado en el Reglamento propuesto.

[80] «Escaneo desde el cliente» se refiere de manera amplia a los sistemas que escanean los contenidos de los mensajes para cotejarlos con una base de datos de contenido inadmisible antes de que se envíen a sus destinatarios.
[81] Propuesta, considerando 26.
[82] Evaluación de impacto, p. 27.
[83] Propuesta, artículo 25.

104. En particular, se debería exigir a los prestadores que consulten a las autoridades de protección de datos mediante un procedimiento de consulta previa, como se menciona en el artículo 36 del RGPD, antes de implantar cualquier medida de detección de material de abuso sexual de menores o de captación de menores, y no exclusivamente en relación con el uso de medidas para detectar el embaucamiento de menores, como contempla actualmente la propuesta[84]. Se debería considerar por defecto que todas las medidas de detección conllevan un «riesgo alto», de modo que habría que someterlas a un procedimiento de consulta previa con independencia de si se refieren a la captación de menores o a material de abuso sexual de menores, como ya ocurre en el marco del Reglamento provisional[85]. Además, las autoridades de protección de datos competentes designadas en virtud del RPGD deberían estar siempre facultadas para dar su opinión sobre las medidas de detección previstas, en vez de solo en circunstancias concretas[86].

105. Del mismo modo, el Reglamento propuesto debería establecer un sistema para abordar y resolver los desacuerdos entre las autoridades competentes y las autoridades de protección de datos en lo que respecta a las órdenes de detección. En particular, se debería otorgar a las autoridades de protección de datos el derecho a impugnar una orden de detección ante los órganos jurisdiccionales del Estado miembro de la autoridad judicial o la autoridad administrativa independiente competente que la haya emitido. Sobre esta cuestión, el CEPD y el SEPD señalan que, con arreglo a la versión actual de la propuesta, la autoridad competente puede ignorar la opinión de las autoridades de protección de datos competentes cuando dicte una orden de detección. Esto podría dar lugar a decisiones contradictorias, dado que, como confirma el artículo 36, apartado 2, del RGPD, las autoridades de protección de datos conservarían todos los poderes correctivos que les concede el artículo 58 del RGPD, incluido el poder de imponer la prohibición del tratamiento.

4.11.2 Función del CEPD

106. El CEPD y el SEPD señalan que la propuesta establece, en el artículo 50, apartado 1, párrafo tercero, que «el Centro de la UE solicitará el dictamen de su Comité de Tecnología y del Comité Europeo de Protección de Datos» antes de incluir tecnologías específicas en las listas de tecnologías que los prestadores de servicios de alojamiento de datos o de servicios de comunicaciones interpersonales puedan plantearse utilizar para ejecutar órdenes de detección. También indica que el CEPD emitirá sus dictámenes en un plazo de ocho semanas, que podría prorrogarse seis semanas más cuando sea necesario, teniendo en cuenta la complejidad del asunto. Por último, exige al CEDP que informe al Centro de la UE de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, junto con los motivos de la dilación.

107. Las actuales funciones del CEPD están definidas en el artículo 70 del RGPD y el artículo 51 de la Directiva (UE) 2016/680 (en lo sucesivo, la «Directiva DAP»)[87]. En estas funciones, se establece que el CEPD asesorará a la Comisión y emitirá dictámenes a petición de esta, una autoridad nacional de control o su Presidencia. Aunque el artículo 1, apartado 3, letra d), de la propuesta afirma que esta no

[84] Propuesta, artículo 7, apartado 3, segundo párrafo, letra b).
[85] Reglamento provisional, artículo 3, apartado 1, letra c).
[86] Propuesta, artículo 7, apartado 3, segundo párrafo, letra c).
[87] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (DO L 119 de 4.5.2016, pp. 89 a 131).

afecta a las normas recogidas en el RGPD y la Directiva DAP, el hecho de facultar al Centro de la UE para que solicite dictámenes al CEPD sobrepasa las funciones que el RGPD y la Directiva DAP atribuyen al CEPD. Por lo tanto, se debería dejar claro en el Reglamento propuesto —al menos en un considerando— que la propuesta amplía las funciones del CEDP. En este sentido, el CEPD y el SEPD agradecen la importante labor que la propuesta atribuye al CEPD, al requerir que participe en la implementación práctica del Reglamento propuesto. En la práctica, la Secretaría del CEPD desempeña una función crucial al brindar el apoyo analítico, administrativo y logístico necesario para la adopción de los dictámenes del CEDP. De este modo, para garantizar que el CEPD y sus miembros puedan desempeñar sus funciones, resulta esencial asignar suficiente presupuesto y personal al CEPD. Sin embargo, lamentablemente, la ficha de financiación legislativa de la propuesta no indica que se vayan a facilitar recursos adicionales para el ejercicio de las funciones adicionales que la propuesta asigna al CEPD[88].

108. Por otra parte, el CEPD y el SEPD señalan que el artículo 50 de la propuesta no especifica cómo procederá el Centro de la UE tras recibir un dictamen del CEPD[89]. El considerando 27 de la propuesta únicamente indica que el Centro de la UE y la Comisión Europea deben tener en cuenta el asesoramiento del CEPD. Por consiguiente, conviene aclarar qué finalidad tendrá el dictamen solicitado en el proceso previsto en el artículo 50 de la propuesta y cómo actuará el Centro de la UE una vez que reciba un dictamen del CEPD.

109. Además, el CEPD y el SEPD consideran que, si bien las directrices o los posibles dictámenes del CEPD respecto al uso de tecnologías de detección valorarán la utilización de dichas tecnologías en términos generales, para realizar una consulta previa con arreglo al artículo 36 del RGPD, la autoridad de control nacional deberá tener en cuenta las circunstancias particulares y evaluar caso por caso el tratamiento previsto por el responsable pertinente. El CEPD y el SEPD señalan que las autoridades de control deben aplicar y aplicarán los criterios establecidos en el artículo 36 del RGPD para decidir si es necesario prorrogar el plazo establecido en el RGPD para formular un dictamen en respuesta a una consulta previa, y que no es necesario aplicar criterios diferentes cuando la consulta previa se refiera al uso de una tecnología de detección[90].

110. Por último, al aplicar el artículo 11 («Directrices relativas a las obligaciones de detección»), la propuesta estipula que la Comisión podrá emitir directrices sobre la aplicación de los artículos 7 a 10 de la propuesta. Resulta preciso modificar el artículo 11 de la propuesta para aclarar que, antes de emitir directrices relativas a las obligaciones de detección, la Comisión deberá consultar, además de a las autoridades de coordinación y al Centro de la UE, al CEPD en relación con el borrador de las directrices al margen del proceso de consulta pública previsto.

111. Por lo tanto, es necesario que el legislador evalúe en mayor profundidad esta función del CEPD y su papel en el marco jurídico que introduciría la propuesta.

4.11.3 Función del Centro de la UE sobre Abuso Sexual de Menores

112. El capítulo IV de la propuesta establecería el Centro de la UE, como la nueva agencia descentralizada para permitir la aplicación de la propuesta. Entre otras funciones, el Centro de la UE debe facilitar el acceso de los prestadores a tecnologías de detección fiables; poner a disposición indicadores creados

[88] Véase la propuesta, p. 105 y siguientes.
[89] Véase, en cambio, el artículo 51, apartado 4, de la Directiva DAP.
[90] Véase la propuesta, considerando 24.

sobre la base de los abusos sexuales de menores en línea verificados por órganos jurisdiccionales o autoridades administrativas independientes de los Estados miembros a efectos de detección; prestar cierta asistencia, previa solicitud, en relación con la realización de evaluaciones de riesgos, y prestar apoyo en la comunicación con las autoridades nacionales pertinentes[91].

113. En ese sentido, el CEPD y el SEPD aplauden el artículo 77, apartado 1, de la propuesta, que confirma que el tratamiento de datos personales por parte del Centro de la UE estará sujeto al RPDUE e indica que las medidas para la aplicación de dicho Reglamento por parte del Centro de la UE, incluidas las relativas al nombramiento de un responsable de la protección de datos del Centro de la UE, se establecerán previa consulta con el SEPD. No obstante, el CEPD y el SEPD opinan que varias disposiciones de este capítulo merecen un examen más a fondo.

114. En primer lugar, el CEPD y el SEPD señalan que el artículo 48 de la propuesta ordena transmitir cualquier denuncia que no sea «manifiestamente infundada»[92] a las autoridades policiales nacionales y a la Agencia de la Unión Europea para la Cooperación Policial (Europol). Este umbral para que el Centro de la UE transmita denuncias a las autoridades policiales y Europol («no es manifiestamente infundada») parece demasiado bajo, sobre todo si se tiene en cuenta que el Centro de la UE se crea con el objetivo, según la evaluación de impacto de la Comisión, de aliviar la carga que supone para las autoridades policiales y Europol filtrar el contenido que se clasifica erróneamente como material de abuso sexual de menores[93]. En este sentido, no queda claro por qué el Centro de la UE, en tanto que centro de conocimientos especializados, no podría llevar a cabo un análisis jurídico y fáctico más exhaustivo a fin de limitar los riesgos de que los datos de personas inocentes se transfieran a las autoridades policiales.

115. En segundo lugar, la disposición relativa a la duración del almacenamiento de datos personales por parte del Centro de la UE parece relativamente abierta, dada la sensibilidad de los datos en cuestión. Aunque no sea posible establecer un período máximo de conservación para el almacenamiento de dichos datos, el CEPD y el SEPD recomiendan que en la propuesta se establezca, al menos, un plazo máximo para revisar la necesidad de continuar almacenándolos y se exija una justificación para seguir conservándolos una vez transcurrido dicho plazo.

116. Además, dada la gran sensibilidad de los datos personales que debe tratar el Centro de la UE, el CEPD y el SEPD opinan que su tratamiento debería estar sujeto a unas garantías adicionales, en particular para garantizar un control efectivo. Una de ellas podría ser la obligación para el Centro de la UE de llevar registros de las operaciones de tratamiento en sistemas de tratamiento automatizado referentes a los datos, que replicaría el requisito aplicable a los datos personales operativos recogido en el capítulo IX del RPDUE. Esto implicará consignar la inclusión, modificación, consulta, comunicación, combinación y supresión de datos personales, así como cualquier acceso a ellos. Los registros de operaciones de consulta y comunicación harán posible determinar la justificación, así como la fecha y la hora, de tales operaciones y el nombre de la persona que consultó o comunicó datos personales operativos, así como, en la medida de lo posible, la identidad de los destinatarios. Estos registros se utilizarán con el fin de verificar la licitud del tratamiento, ejercer un autocontrol y

[91] Véase COM(2022) 209 final, p. 8.

[92] El término «manifiestamente infundada» se define en el considerando 65 de la propuesta del siguiente modo: «cuando sea inmediatamente evidente, sin ningún análisis jurídico o fáctico sustancial, que las actividades denunciadas no constituyen abusos sexuales de menores en línea».

[93] Véase, por ejemplo, la página 349 de la evaluación de impacto.

garantizar su integridad y seguridad, y se pondrán a disposición del delegado de protección de datos del Centro de la UE y el SEPD cuando así lo soliciten.

117. Asimismo, la propuesta alude a la obligación de los prestadores de informar a los usuarios de que se ha detectado material de abuso sexual de menores mediante una orden de detección, así como al derecho a presentar una denuncia a la autoridad de coordinación[94]. Sin embargo, la propuesta no establece procedimientos para que los interesados ejerzan sus derechos que tengan en cuenta también los múltiples lugares donde se pueden transferir y almacenar datos personales en virtud de la propuesta (Centro de la UE, Europol, autoridades policiales nacionales). El requisito de informar a los usuarios debería incluir la obligación de informarlos de que sus datos han sido transmitidos y están siendo tratados por distintas entidades, cuando corresponda (p. ej., por las autoridades policiales nacionales y Europol). Del mismo modo, debería existir un procedimiento centralizado para recibir y coordinar solicitudes relacionadas con el derecho de acceso, rectificación y supresión, o bien la obligación de que la entidad que reciba la solicitud de un interesado se coordine con el resto de las entidades implicadas.

118. El CEPD y el SEPD señalan que, con arreglo al artículo 50 de la propuesta, el Centro de la UE tiene la función de especificar la lista de tecnologías que pueden utilizarse para ejecutar órdenes de detección. No obstante, en virtud del artículo 12, apartado 1, de la propuesta, los prestadores tienen la obligación de denunciar cualquier información que indique un posible abuso sexual de menores en línea en sus servicios, no solo la que obtengan mediante la ejecución de órdenes de detección. Es sumamente probable que gran parte de esa información proceda de las medidas de reducción del riesgo que apliquen los prestadores, de acuerdo con el artículo 4 de la propuesta. Por tanto, parece crucial definir en qué podrían consistir estas medidas, su eficacia, sus tasas de error a la hora de denunciar posibles abusos sexuales de menores y su impacto en los derechos y las libertades de las personas. A pesar de que el artículo 4, apartado 5, de la propuesta indica que la Comisión, en cooperación con las autoridades de coordinación y el Centro de la UE y tras haber llevado a cabo una consulta pública, podrá publicar directrices relevantes, al CEPD y el SEPD les parece importante que el legislador también asigne al Centro de la UE, en el artículo 50, la función de proporcionar una lista de las medidas de reducción recomendadas y de las mejores prácticas pertinentes que sean en particular efectivas para identificar posibles abusos sexuales de menores en línea. Puesto que dichas medidas podrían suponer una injerencia en los derechos fundamentales a la protección de los datos y la vida privada, también se recomiende que el Centro de la UE consulte al CEPD antes de facilitar dicha lista.

119. Por último, los requisitos de seguridad definidos en el artículo 51, apartado 4, de la propuesta deberían ser más específicos. En este sentido, podrían servir de inspiración los requisitos de seguridad establecidos en otros Reglamentos relativos a sistemas a gran escala que implican tratamientos de alto riesgo, como el Reglamento (CE) n.º 767/2008 [95] (véase el artículo 32), el Reglamento (CE)

[94] Véase el artículo 10, apartado 6, y, tras la presentación de una denuncia al Centro de la UE, el artículo 12, apartado 2, de la propuesta.

[95] Reglamento (CE) n.º 767/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros (Reglamento VIS) (DO L 218 de 13.8.2008, pp. 60 a 81).

n.º 1987/2006[96] (véase el artículo 16), el Reglamento (UE) 2018/1862[97] (véase el artículo 16) y el Reglamento (UE) n.º603/2013[98] (véase el artículo 34).

4.11.4 La función de Europol

120. La propuesta contempla la estrecha cooperación entre el Centro de la UE y Europol. En virtud del capítulo IV de la propuesta, cuando reciba denuncias de los prestadores referentes a supuestos materiales de abuso sexual de menores, el Centro de la UE deberá comprobarlas para determinar cuáles son perseguibles (no manifiestamente infundadas) y se las remitirá a Europol y a las autoridades policiales nacionales[99]. El Centro de la UE dará a Europol acceso a sus bases de datos de indicadores y de denuncias, a fin de ayudar a Europol en su investigación de presuntos delitos de abuso sexual de menores[100]. Asimismo, se facilitará al Centro de la UE el acceso «más completo posible» a los sistemas de información de Europol [101] . Ambas agencias compartirán además locales y determinadas infraestructuras (no operativas)[102].

121. El CEPD y el SEPD observan que varios aspectos de la cooperación entre el Centro de la UE propuesto y Europol suscitan preocupación o deben especificarse en más detalle.

En lo que respecta a la transmisión de denuncias a Europol por parte del Centro de la UE (artículo 48)

122. El artículo 48 del Reglamento propuesto requiere que el Centro de la UE transmita las denuncias que no considere manifiestamente infundadas, junto con toda la información adicional pertinente de que disponga, a Europol y a las autoridades policiales competentes del Estado miembro que pueda ser competente para investigar o enjuiciar los posibles abusos sexuales de menores. Aunque este artículo atribuye a Europol la función de determinar cuál es la autoridad policial competente cuando no esté claro cuál es el Estado miembro competente, en realidad la disposición prevé que todas las denuncias

[96] Reglamento (CE) n.º 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 381 de 28.12.2006, pp. 4 a 23).
[97] Reglamento (UE) 2018/1862 del Parlamento Europeo y del Consejo, de 28 de noviembre de 2018, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen (SIS) en el ámbito de la cooperación policial y de la cooperación judicial en materia penal, por el que se modifica y deroga la Decisión 2007/533/JAI del Consejo, y se derogan el Reglamento (CE) n.º 1986/2006 del Parlamento Europeo y del Consejo y la Decisión 2010/261/UE de la Comisión (DO L 312 de 7.12.2018, pp. 56 a 106).
[98] Reglamento (UE) n.º 603/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013 , relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento (UE) n ° 604/2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida, y a las solicitudes de comparación con los datos de Eurodac presentadas por los servicios de seguridad de los Estados miembros y Europol a efectos de aplicación de la ley, y por el que se modifica el Reglamento (UE) n ° 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (DO L 180 de 29.6.2013, pp. 1 a 30).
[99] Véase el artículo 48 de la propuesta.
[100] Véase el artículo 46, apartados 4 y 5, de la propuesta.
[101] Véase el artículo 53, apartado 2, de la propuesta.
[102] En especial las relacionadas con la gestión de los recursos humanos; las tecnologías de la información, incluida la ciberseguridad; el edificio, y las comunicaciones.

se transmitan a Europol con independencia de si se ha identificado a la autoridad nacional competente y de si el Centro de la UE ya ha transferido la denuncia a esta.

123. Sin embargo, la propuesta no aclara qué valor añadido aportaría la implicación de Europol ni la función que se espera que desempeñe una vez que reciba las denuncias, especialmente en aquellos casos en que se haya identificado a la autoridad policial nacional y esta haya sido informada en paralelo[103].

124. El CEPD y el SEPD recuerdan que el mandato de Europol se limita a apoyar la actuación de las autoridades competentes de los Estados miembros y su cooperación mutua en la prevención y la lucha contra la delincuencia grave que afecte a dos o más Estados miembros[104]. El artículo 19 del Reglamento (UE) 2016/794[105], en su versión modificada por el Reglamento (UE) 2022/991[106] (el «Reglamento sobre Europol modificado»), estipula que un organismo de la Unión que facilite información a Europol tiene la obligación de determinar el fin o los fines para los que Europol deba tratar dicha información, así como las condiciones para dicho tratamiento. También tiene la responsabilidad de garantizar la exactitud de los datos personales transferidos[107].

125. Por consiguiente, la transmisión generalizada de denuncias a Europol contravendría el Reglamento sobre Europol modificado y acarrearía múltiples riesgos para la protección de los datos. La duplicación del tratamiento de los datos personales podría redundar en el almacenamiento paralelo de varias copias de los mismos datos personales altamente sensibles (p. ej., en el Centro de la UE, Europol y las autoridades policiales nacionales), lo que generaría riesgos para la exactitud de los datos debido a la posible desincronización de las bases de datos, así como para el disfrute de sus derechos por parte de los interesados. Asimismo, el bajo umbral que establece la propuesta para remitir denuncias a las autoridades policiales (aquellas «no manifiestamente infundadas») implica una alta probabilidad de que en los sistemas de información de Europol se almacenen falsos positivos (es decir, contenido que se ha clasificado por error como abuso sexual de menores), posiblemente durante largos períodos de tiempo[108].

126. En consecuencia, el CEPD y el SEPD recomiendan que la propuesta especifique y limite las circunstancias en las que el Centro de la UE podrá transmitir denuncias a Europol, de conformidad con el Reglamento sobre Europol modificado, y las finalidades con las que podrá hacerlo. Deberían quedar excluidas de forma explícita aquellas circunstancias en que las denuncias se hayan transmitido a las

---

[103] El considerando 71 de la propuesta únicamente se refiere de manera general a la experiencia de Europol en la identificación de las autoridades nacionales competentes en situaciones poco claras y a su base de datos de inteligencia criminal, que puede contribuir a identificar vínculos con investigaciones en otros Estados miembros.
[104] Véase el artículo 3 del Reglamento sobre Europol modificado.
[105] Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo (DO L 135 de 24.5.2016, pp. 53 a 114).
[106] Reglamento (UE) 2022/991 del Parlamento Europeo y del Consejo, de 8 de junio de 2022, por el que se modifica el Reglamento (UE) 2016/794 en lo que se refiere a la cooperación de Europol con entidades privadas, el tratamiento de datos personales por Europol en apoyo de investigaciones penales y el papel de Europol en materia de investigación e innovación (DO L 169 de 27.6.2022, pp. 1 a 42).
[107] Artículo 38, apartado 2, letra a), del Reglamento sobre Europol modificado.
[108] Según la evaluación de impacto de la Comisión, Europol solo ha podido examinar el 20 % de los 50 millones de imágenes y vídeos únicos de material de abuso sexual de menores que figuran en su base de datos, lo que implica que carece de los recursos necesarios para tomar medidas respecto de los materiales de abuso sexual de menores que recibe actualmente. Véase la evaluación de impacto que acompaña a la propuesta de Reglamento por el que se establecen normas para prevenir y combatir el abuso sexual de los menores, SWD(2022)209, pp. 47 y 48.

autoridades policiales del Estado miembro oportuno, siempre y cuando no tengan una dimensión transfronteriza. Además, la propuesta debería incluir el requisito de que el Centro de la UE únicamente transfiera a Europol datos personales cuando sea apropiado, relevante y estrictamente necesario. También deben establecerse garantías específicas que aseguren la calidad y fiabilidad de los datos.

Artículo 53, apartado 2, sobre la cooperación entre el Centro de la UE y Europol

127. El artículo 53, apartado 2, de la propuesta exige que Europol y el Centro de la UE se faciliten mutuamente «el acceso más completo posible a los sistemas de información pertinentes cuando sea necesario para el desempeño de sus funciones respectivas y de conformidad con los actos del Derecho de la Unión que regulan dicho acceso».

128. El artículo 46, apartados 4 y 5, de la propuesta especifica además que Europol debe poder acceder a la base de datos de indicadores y la base de datos de denuncias del Centro de la UE, mientras que el artículo 46, apartado 6, establece el procedimiento para obtener dicho acceso: Europol deberá enviar una solicitud especificando el objetivo y el grado de acceso necesario para alcanzarlo, y el Centro de la UE deberá evaluar debidamente dicha solicitud.

129. No se especifican los criterios y las garantías que condicionan el acceso de Europol y el posterior uso que haga de los datos que obtenga de los sistemas de información del Centro de la UE. Tampoco se explica por qué es necesario que Europol acceda directamente a los sistemas de información de una autoridad no policial que contienen datos personales altamente sensibles cuyo vínculo con actividades delictivas y la prevención de delitos quizá no se haya determinado. A fin de garantizar un alto nivel de protección de datos y el cumplimiento del principio de limitación de la finalidad, el CEPD y el SEPD recomiendan que el Centro de la UE únicamente transmita datos personales a Europol tras valorar las características de cada caso, en respuesta a una solicitud debidamente evaluada y por medio de una herramienta de intercambio de comunicaciones segura, como SIENA[109].

130. En el artículo 53, apartado 2, figura la única referencia en la propuesta al acceso por parte del Centro de la UE a los sistemas de información de Europol. No está claro, por tanto, con qué finalidades y conforme a qué garantías específicas tendría lugar dicho acceso.

131. El CEPD y el SEPD recuerdan que Europol es un cuerpo de seguridad creado en virtud de los Tratados de la UE con el mandato fundamental de prevenir y luchar contra la delincuencia grave. En consecuencia, los datos personales operativos que trata Europol están sometidos a unas normas y unas garantías estrictas para el tratamiento de datos. El Centro de la UE propuesto no es una autoridad policial, por lo que no se le debería conceder acceso directo a los sistemas de información de Europol bajo ninguna circunstancia.

132. El CEPD y el SEPD señalan igualmente que gran parte de la información de interés común para el Centro de la UE y Europol incluirá datos personales sobre las víctimas de presuntos delitos, datos personales de menores y datos personales relativos a la vida sexual, los cuales constituyen categorías especiales de datos personales en virtud del Reglamento sobre Europol modificado. El Reglamento sobre Europol modificado impone condiciones estrictas para acceder a categorías especiales de datos personales. El artículo 30, apartado 3, del Reglamento sobre Europol modificado estipula que solo

[109] Aplicación de la Red de Intercambio Seguro de Información (SIENA).

Europol tendrá acceso directo a esos datos personales, y más concretamente un número limitado de miembros del personal de Europol autorizados por el director ejecutivo[110].

133. Por este motivo, el CEPD y el SEPD recomiendan aclarar la redacción del artículo 53, apartado 2, de la propuesta para reflejar adecuadamente las restricciones existentes en virtud del Reglamento sobre Europol modificado y especificar las modalidades de acceso para el Centro de la UE. En particular, todo acceso a los datos personales tratados en los sistemas de información de Europol, cuando se considere estrictamente necesario para el desempeño de las funciones del Centro de la UE, debe concederse tras valorar las características de cada caso y en respuesta a una solicitud explícita que documente el objetivo específico y la justificación. Se debe pedir a Europol que evalúe con diligencia dichas solicitudes y únicamente transfiera datos personales al Centro de la UE cuando sea estrictamente necesario y proporcional para el objetivo requerido.

Artículo 10, apartado 6, sobre la función de Europol a la hora de informar a los usuarios tras la ejecución de una orden de detección

134. El CEPD y el SEPD agradecen que, como se establece en el artículo 10, apartado 6, de la propuesta, se exija a los prestadores que informen a los usuarios cuyos datos personales puedan verse afectados por la ejecución de una orden de detección. Esta información no se facilitará a los usuarios hasta que Europol o las autoridades policiales nacionales de un Estado miembro que haya recibido la denuncia con arreglo al artículo 48 hayan confirmado que proporcionar información a los usuarios no interferirá en las actividades de prevención, detección, investigación y enjuiciamiento de delitos de abuso sexual de menores.

135. Sin embargo, falta precisión en lo que respecta a la ejecución práctica de esta disposición. La propuesta no estipula si, cuando se transfieran denuncias a Europol y las autoridades policiales de un Estado miembro, es necesario que uno o ambos destinatarios confirmen su recepción, y tampoco explica los procedimientos o modalidades para obtener dicha confirmación (p. ej., si deben transmitirse a través del Centro de la UE). Habida cuenta del elevado volumen de material de abuso sexual de menores que Europol y las autoridades policiales nacionales podrían tener que tratar, y dada la ausencia de un plazo preciso para cursar la confirmación («sin demora indebida»), el CEPD y el SEPD recomiendan aclarar los procedimientos aplicables a fin de asegurar que esta garantía se haga efectiva en la práctica. Además, la obligación de informar a los usuarios también debería incluir información relativa a los destinatarios de los datos personales afectados.

En lo que respecta a la recopilación de datos y la información sobre transparencia (artículo 83)

136. El artículo 83, apartado 3, de la propuesta indica que el Centro de la UE recopilará datos y generará estadísticas sobre varias de las funciones que le atribuye el Reglamento propuesto. A efectos de control, el CEPD y el SEPD recomiendan añadir a esta lista estadísticas sobre el número de denuncias transferidos a Europol en virtud del artículo 48, así como el número de solicitudes de acceso recibidas por Europol con arreglo al artículo 46, apartados 4 y 5, incluido el número de las solicitudes aceptadas y denegadas por el Centro de la UE.

[110] El Reglamento sobre Europol modificado contempla excepciones a esta prohibición para los organismos de la Unión establecidos sobre la base del título V del TFUE. Sin embargo, dada la base jurídica de la propuesta (artículo 114 del TFUE, relativo a la armonización del mercado interior), esta excepción no incluiría el Centro de la UE propuesto.

5. CONCLUSIÓN

137. Aunque el CEPD y el SEPD aplauden los esfuerzos realizados por la Comisión para garantizar la lucha efectiva contra el abuso sexual de menores en línea, consideran que la propuesta plantea serios problemas en lo que respecta a la protección de los datos y la vida privada. Por ese motivo, el CEPD y el SEPD invitan a los colegisladores a modificar el Reglamento propuesto, en particular para garantizar que las obligaciones de detección previstas cumplan los requisitos de necesidad y proporcionalidad aplicables y no debiliten ni degraden el cifrado en términos generales. El CEPD y el SEPD quedan a disposición para ofrecer su asistencia durante el proceso legislativo, en caso de que sus aportaciones se consideren necesarias para resolver los problemas destacados en el presente Dictamen conjunto.

En nombre del Supervisor Europeo de Protección de Datos	En nombre del Comité Europeo de Protección de Datos
El Supervisor Europeo de Protección de Datos	La presidenta
(Wojciech Wiewiorowski)	(Andrea Jelinek)