EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

Council of Bars and Law Societies of Europe
The voice of European Lawyers

Rue Joseph II, 40/8 - B-1000 Brussels
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

Posicionamiento de CCBE sobre la propuesta de Reglamento por el que se establecen normas para prevenir y combatir los abusos sexuales a los niños

25/11/2022

Introducción y resumen

El 11 de mayo de 2022, la Comisión Europea presentó una propuesta de Reglamento por el que se establecen normas para prevenir y combatir el abuso sexual infantil[1]. La propuesta establece obligaciones para los proveedores de servicios de alojamiento, servicios de comunicación interpersonal, tiendas de aplicaciones informáticas, servicios de acceso a internet y otros servicios pertinentes en materia de detección, notificación, retirada y bloqueo de material en línea conocido y nuevo de abuso sexual infantil ("CSAM"), así como de captación de menores (lo que se denomina "grooming").

El CCBE considera que los abusos sexuales a menores son delitos especialmente graves y atroces y apoya plenamente los objetivos de lucha contra este tipo de delitos y la adopción de medidas específicas para prevenirlos y combatirlos; sin embargo, el CCBE tiene serias preocupaciones, compartidas por la Junta Europea de Protección de Datos ("JEPD") y el Supervisor Europeo de Protección de Datos ("SEPD")[2] , por las amenazas que plantea la propuesta sobre el derecho a la intimidad, la protección del secreto profesional y la prerrogativa del secreto profesional en el ámbito jurídico ("PS/LPP").

En concreto, el CCBE concluye que:

- **En la propuesta se han descartado las salvaguardias necesarias para garantizar la protección de los derechos fundamentales, incluida la confidencialidad de las comunicaciones. La esencia misma del derecho a la confidencialidad se ve socavada por la propuesta, que carece de claridad jurídica, como base legal de la obligación de detección, y de proporcionalidad en cuanto a las injerencias y limitaciones a los derechos fundamentales.**
- **Las garantías procesales y la complejidad del proceso que conduce a la adopción de una orden de detección no pueden sustituir a las garantías sustantivas para asegurar la confidencialidad de las comunicaciones y la protección de los PS/LPP.**
- **El legislador de la UE tiene que adoptar disposiciones legales claras y salvaguardias para garantizar que los derechos fundamentales de todos los ciudadanos estén debidamente asegurados y bien equilibrados. A este respecto, el CCBE se opone firmemente al planteamiento según el cual la protección de los derechos fundamentales se delega parcial o totalmente en partes privadas.**
- **Las medidas propuestas que permiten la detección e identificación de contenidos por parte de los proveedores de servicios deben eliminarse de la propuesta, a falta de disposiciones legales claras y salvaguardias adecuadas que garanticen el respeto y el equilibrio de los derechos fundamentales de las personas.**
- **La propuesta no debe impedir que los abogados protejan adecuadamente la confidencialidad de sus comunicaciones mediante métodos de cifrado. El legislador de la UE debe prever la protección del "cifrado de extremo a extremo" ("E2EE") y garantizar que las disposiciones de la propuesta no puedan debilitar en modo alguno el E2EE.**

[1] COM(2022) 2096 final

[2] Dictamen conjunto 4/2022 del SEPD sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen disposiciones para prevenir y combatir los abusos sexuales contra los niños, 28 de julio de 2022, página 5.

- **La propuesta debería especificar y limitar las circunstancias y los fines en virtud de los cuales el Centro de la UE puede transmitir informes a Europol. Toda transferencia de datos personales a Europol deberá ser adecuada, pertinente y limitada a lo estrictamente necesario, garantizando al mismo tiempo la calidad y fiabilidad de los datos. Además, el intercambio de datos personales entre el Centro de la UE y Europol sólo debería tener lugar caso por caso, previa solicitud explícita y debidamente evaluada.**

I. Obligación de detección

El CCBE observa que los artículos 7 a 10 de la propuesta de Reglamento prevén la obligación para los prestadores de servicios de alojamiento y de comunicación interpersonal de detectar la comunicación CSAM y grooming cuando una autoridad judicial o una autoridad administrativa independiente haya emitido una orden de detección en las condiciones previstas en los artículos 7 y 8. A este respecto, los proveedores deberán utilizar tecnologías que permitan detectar la difusión de CSAM o de comunicación de grooming en las condiciones especificadas en el artículo 10.

A. La necesidad de garantizar PS/LPP

1. Una protección específica

El CCBE recuerda que para que los abogados sean eficaces en la defensa de los derechos de sus clientes, debe existir la confianza de que las comunicaciones entre ellos se mantienen confidenciales. La mayoría de los sistemas jurídicos comparten la idea de que, si se negara el derecho del ciudadano a salvaguardar la confidencialidad, es decir, el derecho del ciudadano a ser protegido contra cualquier divulgación de su comunicación con su abogado se podría negar a las personas el acceso al asesoramiento jurídico y a la justicia. Así pues, los PS/LPP se consideran instrumentos mediante los cuales se puede lograr el acceso a la justicia y el mantenimiento del Estado de Derecho.

El Tribunal Europeo de Derechos Humanos ("TEDH") ha vinculado reiteradamente el respeto de la PS/LPP a la observancia de **los artículos 6 y 8 del Convenio Europeo de Derechos Humanos** ("CEDH"), afirmando que "*el derecho de toda persona a un proceso equitativo*"[3] *depende de la "relación de confianza entre [el abogado y el cliente]*" y subrayando repetidamente que menoscabar la PS/LPP puede violar el artículo 8, que protege el derecho al respeto de la vida privada y familiar. En efecto, **el artículo 8 "*otorga una protección reforzada a los intercambios entre los abogados y sus clientes*"**. El Tribunal precisa que "*esto se justifica por el hecho de que los abogados tienen asignado un papel fundamental en una sociedad democrática, el de defender a los justiciables. Sin embargo, no pueden llevar a cabo esta tarea esencial si no pueden garantizar a aquellos a quienes defienden que sus intercambios seguirán* siendo confidenciales"[4] .

La protección de la confidencialidad de las comunicaciones entre abogado y cliente también ha sido reconocida como **principio general del Derecho de la UE** por el Tribunal de Justicia de las Comunidades Europeas[5] y tiene una **base jurídica en la Carta de los Derechos Fundamentales de la UE, en sus artículos 7 sobre el derecho a la intimidad y 47 sobre el derecho a un juicio justo**.

[3] TEDH, Michaud c. Francia (12323/11), 2012, §§117-118
[4] TEDH, Kopp contra Suiza (23224/94), 1998
[5] TJCE, AM&S contra Comisión, (155/79), 1982, §18

2. Interferencias limitadas

Según el apartado 1 del artículo 52 de la Carta de la UE, las injerencias en los derechos fundamentales deben estar previstas por la ley, respetar la esencia de esos derechos y, sin perjuicio del principio de proporcionalidad, sólo pueden limitarse si son necesarias y responden efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de proteger los derechos y libertades de los demás. Además, los derechos contenidos en la Carta correspondientes a los derechos garantizados por el CEDH deben tener el mismo significado y alcance. Esto se aplica al derecho a la confidencialidad de las comunicaciones, ya que está garantizado por el artículo 7 de la Carta y el artículo 8 del CEDH. El derecho protegido por el artículo 8 del CEDH puede ser objeto de injerencias que deben ser conformes a la ley, perseguir un objetivo legítimo y ser necesarias en una sociedad democrática para alcanzar el objetivo en cuestión.

Sin embargo, como se ha señalado anteriormente, el TEDH otorga una protección reforzada en virtud del artículo 8 del CEDH a las comunicaciones que recaen bajo la protección de PS/LPP. Además, el CCBE recuerda que, aunque el derecho del artículo 8 es cualificado, el derecho a un juicio justo según el artículo 6 CEDH es absoluto y no cualificado[6] . **Por lo tanto, si una comunicación legalmente privilegiada, o una comunicación protegida por una obligación de secreto profesional entra en el ámbito del artículo 6 CEDH, entonces, dado el carácter absoluto de la protección que ofrece este artículo, no debería existir la posibilidad de que se permita la interceptación**.

A este respecto, cabe señalar que en las disposiciones transitorias del **Reglamento (UE) 2021/1232**[7] , adoptado para modificar la Directiva sobre la privacidad y las comunicaciones electrónicas[8] para luchar contra el CSAM, a la espera de la adopción de la actual propuesta, el legislador de la UE ha previsto explícitamente una **cláusula sobre la protección de los PS/LPP**, considerando que **las normas temporales para detectar el abuso sexual infantil en línea deben entenderse "*sin perjuicio de las normas sobre el secreto profesional con arreglo al Derecho nacional", como las normas sobre la protección de las comunicaciones profesionales, entre médicos y sus pacientes, entre periodistas y sus fuentes, o entre abogados y sus clientes, en particular porque la confidencialidad de las comunicaciones entre los abogados y sus clientes es clave para garantizar el ejercicio efectivo de los derechos de la defensa como parte esencial del derecho a un juicio justo***". Lamentablemente, la Comisión Europea no ha repetido esta cláusula general en la nueva propuesta.

El siguiente análisis de la propuesta revela que se han descartado las salvaguardias necesarias para garantizar la protección de los derechos fundamentales, incluida la confidencialidad de las comunicaciones. El CCBE considera que la esencia misma del derecho a la confidencialidad se ve socavada por la propuesta, que carece de claridad jurídica, como base legal a la obligación de detección, y de proporcionalidad en cuanto a las injerencias y limitaciones a los derechos fundamentales.

[6] TEDH, Niemietz contra Alemania, (13710/88), 1992, §375.

[7] 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 parte de los proveedores de servicios de comunicaciones interpersonales independientes del número para el tratamiento de datos personales y de otro tipo con el fin de luchar contra los abusos sexuales a menores en línea, 14 de julio de 2021.

[8] Directiva 202/58/CE 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), 12 de julio de 2002.

B. La falta de salvaguardias suficientes en la propuesta

1. Las garantías procesales y el papel de los agentes privados

El CCBE señala que un complejo procedimiento conduce a la emisión de una orden de detección, empezando por una evaluación de riesgos realizada por el proveedor de servicios y las posibles medidas de mitigación. En caso de que persista un "*riesgo significativo*", la autoridad pública nacional afectada, la denominada autoridad de coordinación, iniciará el procedimiento para la adopción de una orden de detección. Antes de solicitar dicha orden a la autoridad judicial o administrativa competente, la autoridad de coordinación deberá intercambiar con el proveedor de servicios.

Las condiciones para solicitar la emisión de una orden de detección se establecen en el apartado 4 del artículo 7, que exige la existencia de un "*riesgo significativo*" de que el servicio se utilice con fines de abuso sexual infantil en línea. La evaluación de la existencia de dicho riesgo está prevista en los apartados 5, 6 y 7 del artículo 7 para cada categoría de orden de detección (relativa a la difusión de CSAM conocidos, CSAM nuevos y captación de niños).

A pesar de las disposiciones complementarias de los apartados 5 a 7 del artículo 7, los requisitos previos para la adopción de una orden de detección, basados en la demostración de un riesgo significativo, se basan en conceptos amplios y vagos, carentes de la claridad jurídica necesaria para la correcta aplicación de la propuesta y el equilibrio de los derechos en juego. En efecto, la emisión de una orden de detección no requiere una sospecha concreta y no está relacionada con casos individuales. Basta con la determinación de un "*riesgo significativo*" y éste "*se considerará que existe*" cuando el servicio se utilice "*probablemente*" para la difusión de CSAM o para el grooming. Como han indicado la SEPD y el SEPD, **estas disposiciones vagas y la inseguridad jurídica dificultan la aplicación de los requisitos jurídicos de la propuesta de manera previsible y no arbitraria, por parte de los proveedores de servicios interesados y de los tribunales o autoridades independientes que emitan la orden, y darán lugar a "*divergencias considerables sobre la aplicación concreta de la propuesta en toda la* Unión"**[9] .

El CCBE también está profundamente preocupado por la participación de agentes privados en la identificación, recopilación y transmisión de información sobre contenidos mientras no estén sujetos a ninguna obligación de secreto profesional ni a control democrático. Tal y como han planteado los organismos europeos de protección de datos, los proveedores de servicios y las autoridades gozan de un amplio margen de apreciación a la hora de equilibrar los derechos fundamentales de las personas. Los proveedores de servicios podrían tener una influencia consecuente en todo el proceso que conduce a la emisión de una orden de detección. Deberían llevar a cabo la evaluación inicial de riesgos (artículo 3), adoptar medidas paliativas teniendo "*debidamente en cuenta*" las "*posibles consecuencias*" para el ejercicio de los derechos fundamentales de todas las partes afectadas (artículo 4), antes de informar e interactuar con la autoridad de coordinación que decidirá solicitar o no una orden de detección.

A este respecto, el CCBE señala que, en relación con la evaluación del riesgo, los proveedores deben tener en cuenta una lista de elementos con arreglo al artículo 3, apartado 2, letras a) a e), como lo que está prohibido o restringido en sus términos y condiciones; la forma en que los usuarios utilizan el servicio; la forma en que el servicio es utilizado o puede ser utilizado por niños; los grupos de edad y el riesgo de captación de grupos de edad; las funcionalidades existentes para establecer contactos. En cuanto a las medidas paliativas que deben adoptarse, el artículo 4 exige la adopción de medidas como la adaptación de los sistemas de moderación o recomendación de contenidos del proveedor.

Sin embargo, como indican el SEPD y el SEPD, los criterios de los artículos 3 y 4 pueden parecer pertinentes, pero dejan un amplio margen de interpretación y apreciación al utilizar términos abstractos, vagos y

[9] EDPB-EDPS Dictamen conjunto 4/2022, §37

genéricos. El CCBE está de acuerdo en que "***estos criterios no cumplen los criterios de seguridad jurídica y previsibilidad necesarios para justificar una injerencia en la confidencialidad de las comunicaciones entre particulares que constituya una clara injerencia en los derechos fundamentales a la intimidad y a la libertad de*** expresión"[10] .

Además, por lo que se refiere al considerando (17), que estipula que los proveedores deben poder indicar su voluntad y preparación para la emisión de una orden de detección, durante la fase de notificación del riesgo a la autoridad pública competente, parece que se escucharán sus opiniones sobre la posible adopción de una orden, mientras que "***no puede suponerse que todos y cada uno de los proveedores tratarán de evitar la emisión de una orden de detección para preservar la confidencialidad de las comunicaciones de sus usuarios aplicando las medidas más eficaces, pero menos intrusivas [...***]"[11] . Así pues, los proveedores a los que se dirige tendrán un papel importante en la ponderación de los derechos en juego, en particular la confidencialidad de las comunicaciones. Esta implicación resulta bastante inquietante tras las recientes filtraciones de datos y escándalos que demostraron la incapacidad de ciertos proveedores para procesar adecuadamente contenidos muy sensibles. A pesar de los marcos reguladores, supuestamente sólidos en Europa, las grandes plataformas han eludido durante años las leyes de protección de datos y privacidad, demostrando la ineficacia de los mecanismos reguladores para garantizar la confidencialidad de las comunicaciones y la protección de datos.

A este respecto, las garantías procesales y la complejidad del proceso que conduce a la adopción de una orden de detección no son suficientes ni pueden sustituir a las salvaguardias sustantivas[12] para garantizar la confidencialidad de las comunicaciones y la protección de los PS/LPP. Asimismo, el CCBE se opone firmemente a el planteamiento según el cual la protección de los derechos fundamentales se delega parcial o totalmente en partes privadas.

Corresponde a los legisladores de la UE adoptar disposiciones jurídicas claras y salvaguardias para garantizar que los derechos fundamentales de los ciudadanos sean respetados.

2. Tecnologías utilizadas para detectar CSAM y grooming

De conformidad con el artículo 10 de la propuesta, los proveedores de servicios dirigidos que reciban una orden de detección deberán ejecutarla instalando y haciendo funcionar tecnologías para detectar la difusión de CSAM o grooming conocidos o nuevos. Dichas tecnologías no podrán extraer más información de las comunicaciones pertinentes que la estrictamente necesaria para la detección, de acuerdo con el estado de la técnica en el sector y lo menos intrusiva posible en términos de impacto sobre los derechos de los usuarios a la intimidad y la confidencialidad de las comunicaciones.

Sin embargo, el CCBE observa que, como señalan el SEPD y la SEPB, "*las tecnologías actualmente disponibles se basan en el* ***tratamiento automatizado de los datos de contenido de todos los usuarios afectados*** [...]. *Además, se sabe que las tecnologías actualmente disponibles, especialmente las destinadas a detectar nuevos CSAM o grooming, presentan tasas de* ***error relativamente elevadas****"*[13] . Esto es tanto más alarmante cuanto que "*las condiciones generales para la emisión de una orden de detección con arreglo a la Propuesta, es decir, aplicada a todo un servicio y no sólo a comunicaciones seleccionadas, la duración de hasta 24 meses para CSAM conocido o nuevo y de hasta 12 meses para grooming, etc. pueden llevar a un alcance muy amplio de la orden en la práctica. En consecuencia,* ***el control sería en realidad de carácter general e indiscriminado, y no selectivo en la práctica****".*

Asimismo, en la anterior evaluación de impacto elaborada por el Servicio de Estudios del Parlamento Europeo ("EPRS") sobre las normas temporales para luchar contra el CSAM y la captación de menores del

[10] *Ibídem*, §27
[11] *Ibídem*, §29
[12] *Ibid., §30*
[13] *Ibídem*, §52

Reglamento (UE) 2021/1232, el EPRS concluyó que "***las técnicas de detección de la captación de menores basadas en texto implican el análisis automatizado y el escaneo indiscriminado del contenido de las comunicaciones y los datos de tráfico relacionados, y son propensas a errores y vulnerables a abusos. Sin salvaguardias adicionales claras y precisas, estas tecnologías no podrían cumplir la prueba de necesidad y proporcionalidad prevista en el artículo 52, apartado 1, de la*** *Carta*"[14] .

El CCBE comparte las conclusiones de EPDB-EDPS en el sentido de que "*la propuesta podría convertirse en la base de un escaneo generalizado e indiscriminado de facto del contenido de prácticamente todos los tipos de comunicaciones electrónicas de todos los usuarios de la UE/EEE. Como* ***resultado, la legislación podría llevar a las personas a abstenerse de compartir contenidos legales por temor a que puedan ser objeto de una persecución basada en su*** acción"[15] .

El CCBE considera que las tecnologías en cuestión, así como las condiciones de su utilización, no prevén garantías suficientes para asegurar la protección de la PS/PVL y la confidencialidad de las comunicaciones. Al aplicarse a todos los usuarios y realizar un análisis automatizado de todas las comunicaciones, de forma desproporcionada, dichas tecnologías pueden permitir el señalamiento y la interceptación de comunicaciones privilegiadas compartidas por los clientes y sus abogados, dando lugar a violaciones de los PS/PLP. **Más allá de su falta de proporcionalidad, el CCBE subraya que en todos los casos debería exigirse a los proveedores de servicios que se aseguren de que la tecnología que utilizan garantiza que no se interfiere con ningún tipo de dato o comunicación protegido por PS/LPP. Se les debe exigir que desplieguen medios tecnológicos que garanticen que no se accederá a material privilegiado**.

A la vista de lo anterior, el CCBE concluye que las medidas propuestas que permiten la detección e identificación de contenidos por parte de los proveedores de servicios deben eliminarse de la propuesta, en la ausencia de disposiciones legales claras y salvaguardias adecuadas que garanticen el respeto y el equilibrio de los derechos fundamentales de las personas.

Impedir los intentos de poner en peligro el cifrado

Además, el CCBE observa que, tal como han planteado el SEPD y el SEPD, la propuesta podría repercutir en el uso del cifrado de extremo a extremo ("E2EE"). El considerando 26 de la propuesta establece que los proveedores pueden elegir las tecnologías utilizadas para cumplir las órdenes de detección, lo que no debe entenderse como un incentivo o desincentivo al uso de una tecnología determinada, siempre que las tecnologías y las medidas de acompañamiento cumplan los requisitos del Reglamento propuesto, incluida la tecnología de cifrado de extremo a extremo. Como explican la SEPD y el SEPD, "es *probable que la mera posibilidad de que se emita una orden de detección tenga un gran peso en las decisiones técnicas que tomen los proveedores, sobre todo teniendo en cuenta el limitado plazo de que dispondrán para cumplir dicha orden y las fuertes sanciones a las que se enfrentarían en caso de no hacerlo. En la práctica, esto podría llevar a algunos proveedores a dejar de utilizar E2EE*".

Además, es sorprendente observar que la **cláusula sobre la protección del cifrado de extremo a extremo**, prevista en el Reglamento (UE) 2021/1232, no se ha repetido en la propuesta de la Comisión Europea, al igual que la cláusula sobre la protección del secreto profesional[16] .

[14] EPRS Study on the Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse - Targeted substitute impact assessment, February 2021, page 37.

[15] Dictamen conjunto 4/202, §55

[16] Considerando (25) del Reglamento (UE) 2021/1232: "*El cifrado de extremo a extremo es una herramienta importante para garantizar la seguridad y confidencialidad de las comunicaciones de los usuarios, incluidas las de los niños. Cualquier debilitamiento del cifrado podría ser objeto de abuso por parte de terceros malintencionados.*

El CCBE considera que la propuesta no debería impedir a los abogados proteger adecuadamente la confidencialidad de sus comunicaciones mediante métodos de cifrado. El CCBE ha subrayado la especial vulnerabilidad de los abogados a los ataques ilícitos por parte de la Administración o de piratas informáticos privados, debido al hecho de que guardan confidencialmente información sensible que les proporcionan los clientes y que no puede divulgarse[17] . Esto requiere una protección criptográfica adecuada. Por lo tanto, el CCBE pide al legislador de la UE que prevea la protección de la E2EE y que garantice que las disposiciones de la propuesta no puedan debilitar la E2EE en modo alguno.

II. La cooperación entre el nuevo Centro de la UE y Europol

Por último, el CCBE toma nota de que el capítulo IV establece un Centro de la UE sobre abusos sexuales a menores como nuevo organismo descentralizado para garantizar la aplicación de sus disposiciones. El Centro de la UE debería trabajar en estrecha cooperación con Europol, con una sede compartida y un amplio acceso a las bases de datos y a los sistemas de información. Según el artículo 48, el Centro de la UE debe remitir a Europol y a las autoridades nacionales competentes los informes que no sean manifiestamente infundados para investigar o perseguir posibles abusos sexuales a menores. Asimismo, el artículo 53 establece *que* "*Europol y el Centro de la UE se facilitarán mutuamente el* ***máximo acceso posible a la información y a los sistemas de información pertinentes****, cuando sea necesario para el desempeño de sus respectivas funciones y de conformidad con los actos del Derecho de la Unión que regulen dicho acceso*".

El CCBE ha comentado y expresado anteriormente su preocupación por los poderes otorgados a Europol en su nuevo mandato en relación con la recogida, el tratamiento y el intercambio de datos personales. Consideraba que las justificaciones para la recogida, el tratamiento y el intercambio de datos personales por parte de Europol debían regirse por disposiciones claras y precisas, que no pasaran por alto garantías esenciales como la necesidad de autorización judicial previa, así como el sistema de supervisión independiente e imparcial. En su posición, el CCBE precisó que toda transferencia de datos personales a particulares efectuada por Europol debe respetar las garantías esenciales (clara base jurídica, necesidad y proporcionalidad, supervisión judicial independiente y recursos efectivos)[18] . Además, tal como plantearon la SEPD y el SEPD, el mandato de Europol se limita a apoyar y reforzar las actuaciones de las autoridades nacionales competentes y su cooperación mutua en la prevención y la lucha contra la delincuencia grave transfronteriza[19] , y los organismos de la Unión que faciliten información a Europol deberán determinar la finalidad o finalidades para las que esta última deba tratar dicha información y en qué condiciones[20] .

[17] Recomendaciones del CCBE sobre la protección de la confidencialidad de los clientes en el contexto de las actividades de vigilancia, p. 20

[18] CCBE Position Paper on the Proposal for Regulation amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, 6 de mayo de 2021.

[19] Reglamento (UE) 2016/794, artículo 3

[20] *Ibídem*, artículo 19

Por consiguiente, el CCBE considera que la transmisión de informes a Europol no puede tener lugar de forma general y automatizada. La CCBE apoya la recomendación de la SEPD y del SEPD de que la propuesta especifique y limite las circunstancias y los fines para los que el Centro de la UE puede remitir informes a Europol. También debería exigir que toda transferencia de datos personales a Europol sea adecuada, pertinente y limitada a lo estrictamente necesario, garantizando al mismo tiempo la calidad y fiabilidad de los datos[21]. En cuanto al acceso mutuo a los sistemas de información pertinentes entre el Centro de la UE y Europol, el CCBE observa que la propuesta no especifica los criterios ni las salvaguardias específicas para permitir dicho acceso a datos personales muy sensibles. A este respecto, el CCBE apoya las recomendaciones de la SEPD y del SEPD, que consideran que el intercambio de datos personales entre el Centro de la UE y Europol sólo debería tener lugar caso por caso, previa solicitud explícita y debidamente evaluada .[22]

[21] EDPB-EDPS Joint Opinion 4/2022, §126

[22] Ibid., §§129-133