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 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

6/05/2021

El Consejo de la Abogacía Europea (CCBE) representa a las Abogacías de 45 países y, a través de ellos, a más de un millón de profesionales de la abogacía en Europa. CCBE responde regularmente en nombre de sus miembros sobre cuestiones políticas que afectan a la ciudadanía y la abogacía europeas.

En diciembre de 2020, la Comisión Europea publicó una propuesta de Reglamento 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.

La propuesta establece las nuevas competencias que se otorgarán a Europol para tratar datos personales "*no incluidos en las categorías de interesados enumeradas en el anexo II para apoyar una investigación penal*" (artículo 18 bis), para comunicar datos personales operativos a otra institución, órgano, organismo o agencia de la Unión "*si los datos son necesarios para el legítimo desempeño de las funciones de la otra institución, órgano u organismo*" (artículo 24), para recibir datos personales directamente de partes privadas y tratar esos datos personales "*para evitar la difusión de contenidos en línea relacionados con el terrorismo o el extremismo violento en situaciones de crisis*" (artículo 26 bis), y para tratar datos personales con fines de investigación e innovación (art. 33a).

El objetivo del presente documento es que CCBE exponga su posición en relación con una serie de aspectos de la propuesta.

A. Comentarios generales

En primer lugar, CCBE observa que los conceptos de "seguridad nacional", "lucha contra el terrorismo" y prevención del "extremismo violento", así como la invocación de una supuesta necesidad de hacer frente a situaciones de crisis, son utilizados a menudo por los Estados y otras autoridades como motivo para justificar una supuesta necesidad de obtener acceso a datos personales. Un problema importante a este respecto es la falta de una definición común internacionalmente aceptada de estos términos ("seguridad nacional", "terrorismo", "extremismo", etc.), lo que dificulta que los tribunales puedan garantizar eficazmente que las medidas de vigilancia se ajusten a un control estricto de necesidad y proporcionalidad. Esta cuestión ya ha sido abordada por CCBE en sus Recomendaciones sobre la protección de los derechos fundamentales en el contexto de la seguridad nacional[1].

[1] Recomendaciones sobre la protección de los derechos fundamentales en el contexto de la seguridad nacional,

CCBE considera que todo acceso directo o indirecto a los datos personales de la ciudadanía realizado por un Estado debe estar dentro de los límites del Estado de Derecho y, dado que constituiría una injerencia en los derechos fundamentales, debe ser proporcional y, en particular, limitarse al mínimo en lo que respecta al alcance de la vigilancia y al período de conservación de los datos[2].

A este respecto, CCBE recuerda que el Tribunal Europeo de Derechos Humanos (en adelante, "TEDH") ha dictaminado que el mero almacenamiento de datos relativos a la vida privada de una persona, independientemente de su uso posterior, equivale a una injerencia en el sentido del artículo 8 del Convenio Europeo de Derechos Humanos, que garantiza el derecho al respeto de la vida privada y familiar, del domicilio y de la correspondencia[3]. Por su parte, el Tribunal de Justicia de la Unión Europea (en adelante, "TJUE") considera que el acceso a los datos personales con vistas a su conservación o utilización afecta al derecho fundamental al respeto de la vida privada garantizado en el artículo 7 de la Carta de los Derechos Fundamentales de la UE (en adelante, "la Carta"). Este tratamiento de datos personales también está comprendido en el ámbito de aplicación del artículo 8 de la Carta, ya que constituye un tratamiento de datos personales en el sentido de dicho artículo y, por consiguiente, debe cumplir necesariamente los requisitos de protección de datos establecidos en dicho artículo[4]. Además, ambos tribunales consideran que el acceso a los datos personales por parte de una autoridad pública constituye una injerencia adicional[5]. En consecuencia, el acceso, la conservación y la utilización ulterior de datos personales por parte de las autoridades públicas, como las autoridades policiales, en el marco de las medidas de vigilancia, no deben sobrepasar los límites de lo estrictamente necesario, evaluados a la luz de la Carta, para estar justificados en una sociedad democrática.

Esta interferencia se vuelve especialmente peligrosa cuando se accede a datos y comunicaciones a los que la ley ha concedido una protección especial. Este es claramente el caso en relación con las comunicaciones entre la abogacía y sus clientes, ya que, en todos los Estados miembros de la UE, la ley protege la información comunicada de forma confidencial entre la abogacía y sus clientes[6]. Además, esta protección es, en los asuntos judiciales, un componente esencial para garantizar el derecho a un juicio justo del artículo 6 del CEDH, que es un derecho absoluto, y un principio fundamental del Estado de Derecho. En consecuencia, CCBE está especialmente preocupado por el impacto que cualquier medida de la UE sobre el acceso de Europol a los datos personales pueda tener sobre el secreto profesional.

Un problema adicional en relación con cualquier acceso a los datos de la abogacía almacenados en línea es la dificultad para identificar de antemano si los datos están cubiertos por el secreto profesional. CCBE reconoce que los proveedores de servicios de Internet todavía no tienen los medios, o, si los tienen, sólo de forma muy limitada, para reconocer si los datos solicitados por las autoridades policiales están cubiertos por el secreto profesional[7]; por lo tanto, es posible que se dé acceso a los

---

páginas 2 y 22.

[2] El TJUE ha dictado recientemente sentencias en los asuntos *La Quadrature du Net e.a. y Privacy International* (C-511/18, 512/18, 520/18 y 623/17), que confirman la importancia que el Tribunal concede a la protección de datos y la interpretación estricta de la posibilidad de derogar la obligación del Estado de garantizar la confidencialidad de los datos por motivos de seguridad nacional. El Tribunal confirmó que cualquier excepción debe limitarse siempre a lo estrictamente necesario e ir acompañada de garantías efectivas. En particular, se dictaminó que el Derecho de la UE se opone a una normativa nacional que obligue a un proveedor de servicios de comunicaciones electrónicas a realizar una transmisión o conservación general e indiscriminada de datos con el fin de luchar contra la delincuencia.
Véanse también las Recomendaciones 02/2020 del SEPD sobre las Garantías Esenciales Europeas para las medidas de vigilancia, párrafos 20-22.

[3] TEDH, 4 de diciembre de 2008, *S. and Marper contra Reino Unido*, demandas 30562/04 and 30566/04, §67.

[4] TJUE, 16 de julio de 2020, *Data Protection Commissioner contra Facebook Ireland Limited and Maximillian Schrems*, asunto C-311/18, §170.

[5] TJUE, 8 de abril de 2014, Digital Rights Ireland, casos C-293/12 and C-594/12; TEDH, 26 de marzo de 1987, Leander contra Suecia, demanda nº 9248/81, §48.

[6] Recomendaciones de CCBE sobre la protección de la confidencialidad de los clientes en el contexto de las actividades de vigilancia, p. 9.

[7] Conversaciones entre CCBE y EURO-ISPA (Asociación Europea de Asociaciones de Proveedores de Servicios de

datos protegidos, lo que llevaría a violaciones del secreto profesional.

Sobre esta cuestión, el TJUE reconoció que "*la transmisión de datos de tráfico y de localización a autoridades públicas con fines de seguridad puede vulnerar en sí misma el derecho al respeto de las comunicaciones, consagrado en el artículo 7 de la Carta, y provocar efectos disuasorios en el ejercicio por los usuarios de los medios de comunicaciones electrónicas de su libertad de expresión, garantizada en el artículo 11 de la Carta. Tales efectos disuasorios pueden repercutir, en particular, en las personas cuyas comunicaciones estén sujetas, según las normas nacionales, al secreto profesional*"[8].

A este respecto, CCBE subraya que debería exigirse a los proveedores de servicios de Internet y/o a las autoridades policiales y a Europol que la tecnología utilizada para la recogida, el tratamiento y el intercambio de datos personales entre ellos garantice que no haya interferencias con ningún tipo de datos protegidos por el secreto profesional. En cualquier caso, debería exigirse a las autoridades policiales que utilicen todos los medios tecnológicos disponibles para dejar el material protegido por el secreto profesional fuera del ámbito de las operaciones de vigilancia o de la recogida, almacenamiento, tratamiento y transferencia de datos personales. El desarrollo de dicha tecnología debería ser una prioridad absoluta.

Con el fin de informar a los legisladores y a los responsables políticos sobre las normas que deben respetarse para garantizar que los principios esenciales del secreto profesional no se vean socavados, se propone establecer las siguientes recomendaciones, basadas en las Recomendaciones de CCBE sobre la protección de la confidencialidad de los clientes en el contexto de las actividades de vigilancia[9].

1. Necesidad de control legislativo

CCBE considera que toda actividad de vigilancia emprendida por las autoridades policiales debe ser regulada con la debida especificidad y transparencia. Este principio debe aplicarse a Europol. Por lo tanto, cualquier medida europea sobre los poderes de Europol para acceder a los datos personales debe estar sujeta a un control legislativo efectivo dentro de un marco normativo claro[10].

A este respecto, CCBE subraya que los conceptos de seguridad nacional/extremismo/terrorismo/crisis como elementos justificativos en relación con el tratamiento de datos personales deben establecerse con la suficiente especificidad y claridad. La propuesta prevé que Europol intercambie datos personales con entidades privadas relacionadas con la respuesta a la crisis, de acuerdo con el nuevo artículo 26 bis. El objetivo de esta disposición es evitar la difusión de contenidos relacionados con el terrorismo o el extremismo violento en situaciones de crisis. Sin embargo, la propuesta no define en concreto qué es una situación de crisis, ni el terrorismo ni el extremismo violento. CCBE considera que la propuesta debería establecer disposiciones más claras y precisas en cuanto a las justificaciones de la recogida, el tratamiento y el intercambio de datos personales.

La facultad de acceder a los datos personales debe regularse con la misma especificidad y transparencia. CCBE considera que el acceso a los datos personales sólo debe permitirse cuando Europol, como organismo que desea llevar a cabo la vigilancia, pueda establecer que existen razones imperiosas que dan lugar a un grado de sospecha suficiente para justificar la interceptación[11]. Dichas

Internet, https://www.euroispa.org/about/).

[8] TJUE, 6 de octubre de 2020, Privacy International, caso C-623/17, §72.

[9] Recomendaciones del CCBE sobre la protección de la confidencialidad de los clientes en el contexto de las actividades de vigilancia, pp. 2 y 22.

[10] Esto está en consonancia con la posición del EDPB, como se indica en las Recomendaciones 02/2020 del EDPB sobre las garantías esenciales europeas para las medidas de vigilancia (párrafos 26-31).

[11] Del mismo modo, el Comité Europeo de Protección de Datos (CEPD) exige que "se demuestre la necesidad y la proporcionalidad con respecto a los objetivos legítimos que se persiguen" (Recomendaciones 02/2020 del CEPD

razones deberán estar claramente definidas.

A este respecto, CCBE se remite a la jurisprudencia más reciente del TJUE, según la cual "*en lo que atañe al objetivo de prevención, investigación, descubrimiento y persecución de delitos, de conformidad con el principio de proporcionalidad, solo la lucha contra la delincuentica grave y la prevención de las amenazas graves contra la seguridad pública pueden justificar las injerencias graves en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, como las que supone la conservación de los datos de tráfico y de los datos de localización. En consecuencia, solo las injerencias en tales derechos fundamentales que no presenten un carácter grave pueden estar justificadas por el objetivo de prevención, investigación, descubrimiento y persecución de delitos en general*"[12].

Más allá del marco normativo, CCBE considera que deberían existir controles legislativos eficaces y una supervisión democrática para evaluar políticamente la actividad de Europol y el tratamiento de datos personales o cubiertos por el secreto profesional. A este respecto, CCBE señala que, de conformidad con el artículo 88 del TFUE, el Reglamento de Europol prevé un Grupo de Control Parlamentario Conjunto (artículo 51, en adelante "el GCPC"), con miembros tanto de los parlamentos nacionales como del Parlamento Europeo. La propuesta refuerza este control al establecer que Europol debe proporcionar al GCPC información anual sobre el uso de sus herramientas y capacidades adicionales y el resultado de las mismas (considerando 40, modificación del artículo 51 §3).

Sin embargo, CCBE considera que el control legislativo actual y las disposiciones de refuerzo propuestas no son suficientes para garantizar un control democrático eficaz de las actividades de Europol. En lo que respecta a los riesgos y amenazas para los derechos fundamentales causados por el tratamiento de datos personales por parte de las autoridades policiales y de Europol, los poderes de control conferidos al GCPC deberían reforzarse para ir más allá de la facultad de interrogar o ser informado de las actividades de Europol. El reglamento debería prever competencias y responsabilidades más concretas para el GCPC, así como sanciones efectivas y otras consecuencias apropiadas en caso de que se constate una vulneración de los derechos fundamentales.

2. Autorización judicial previa, control independiente y recursos efectivos

Según los nuevos artículos 26.6.a, y 26bis.5 propuestos, Europol podrá solicitar a los Estados miembros que obtengan datos personales de entidades privadas con arreglo a su legislación aplicable, con el fin de compartirlos con Europol, a condición de que los datos personales solicitados se limiten estrictamente a lo necesario para Europol. Se especifica que "*los Estados miembros se asegurarán de que sus autoridades nacionales competentes puedan tramitar legalmente dichas solicitudes de conformidad con su legislación nacional con el fin de proporcionar a Europol la información necesaria para cumplir sus objetivos*".

A este respecto, CCBE observa que debe exigirse la autorización previa de un tribunal para cualquier acceso a los datos personales por parte de las autoridades policiales. El TEDH y el TJUE han especificado en numerosas ocasiones que toda injerencia en el derecho a la intimidad y a la protección de datos debe estar sujeta a un sistema de supervisión eficaz, independiente e imparcial[13].

La legislación debe garantizar que los datos personales obtenidos sin una autorización judicial específica previa sean inadmisibles en un tribunal. Asimismo, debe exigirse la destrucción de todo el material interceptado que se considere adquirido ilegalmente. Además, cualquier dato personal interceptado legalmente debe utilizarse únicamente para el fin para el que se concedió la autorización.

A este respecto, CCBE subraya que la propuesta no debe permitir a Europol eludir ni la necesidad de autorización judicial previa ni el sistema de control independiente e imparcial, que son garantías

sobre las Garantías Esenciales Europeas para las medidas de vigilancia, párrafo. 32-38).

[12] TJUE, 6 octubre de 2020, La Quadrature du Net e.a., casos C-511/18, C-512/18 and C-520/18, §140. Veáse también: TJUE, 2 de marzo de 2021, H.K. v Prokuratuur, caso C-746/18, §45.

[13] TEDH, 1978, Klass y otros contra Alemania, demanda nº 5029/71; TJUE, La Quadrature du Net, §189

esenciales[14]

Además, para proporcionar una protección jurídica eficaz contra la vigilancia ilegal, es necesario que los ciudadanos cuyos datos han sido tratados dispongan de recursos legales[15]. En particular, una vez que se ha revelado que se han emprendido medidas de vigilancia, los ciudadanos deben tener derecho a ser informados de los datos que se han recogido y procesado y deben poder impugnar la legalidad de dichas medidas ante un juez. Además, deben imponerse sanciones adecuadas a las personas y organismos que hayan realizado una vigilancia ilegal.

CCBE observa que el Reglamento de Europol establece que las personas afectadas pueden presentar una reclamación ante el SEPD en caso de tratamiento irregular de datos personales por parte de Europol (artículo 47). Además, cualquier persona que haya sufrido un daño por una operación de tratamiento de datos ilegal tendrá derecho a recibir una indemnización de Europol, de conformidad con el artículo 340 del TFUE, y tendrá derecho a interponer una acción contra Europol ante el TJUE o ante los tribunales nacionales contra los Estados miembros.

Sin embargo, CCBE considera que estos recursos deberían reforzarse, dentro de la propia Europol, para que las personas afectadas puedan ejercer sus derechos, en virtud de los artículos 7 y 8 de la Carta, a ser informados del tratamiento de sus datos, a solicitar el acceso a sus datos personales que hayan sido objeto de un tratamiento y, en su caso, a su rectificación o supresión, así como a disponer de un recurso efectivo ante un tribunal.

El respeto al Estado de Derecho y al secreto profesional debe ser un principio general en el contexto de cualquier medida de la UE sobre vigilancia y, en particular, sobre el acceso a los datos con fines de seguridad y de aplicación de la ley. Además, la ley debe prever una protección explícita del secreto profesional, otorgándole siempre el máximo nivel de protección.

En caso de que se conceda el acceso a los datos relativos a las comunicaciones entre la abogacía y sus clientes en circunstancias excepcionales, CCBE subraya que debe haber una supervisión judicial independiente[16] en todas las etapas del procedimiento de vigilancia, en función de cada caso. El juez que supervise la ejecución de la interceptación debe ser diferente del juez que la autorizó.

Además, cuando los datos protegidos por el secreto profesional sean interceptados erróneamente sin autorización, dichos datos deberán ser borrados inmediatamente, independientemente de que estén o no relacionados con el caso en cuestión. En caso de duda sobre el carácter privilegiado de los datos, Europol deberá separar los datos en cuestión y realizar los controles necesarios antes de cualquier tratamiento.

3. Garantías esenciales aplicables a la transferencia de datos personales a entidades privadas

Según los nuevos artículos 26 §5 y 26 §6 propuestos, Europol podrá transmitir o transferir datos personales a partes privadas, establecidas dentro o fuera de la UE, en función de cada caso, en varias situaciones y cumpliendo los requisitos de absoluta y estricta necesidad. Se solicitará una autorización específica del director ejecutivo de Europol si la entidad privada de que se trate no está establecida en la Unión, y deberán cumplirse las condiciones necesarias para conceder esta autorización. En particular, los datos personales no se transferirán si el director ejecutivo determina que los derechos y libertades fundamentales de la persona afectada prevalecen sobre el interés público de la transferencia. Asimismo, las transferencias no serán sistemáticas, masivas o estructurales. Las

[14] Comité Europeo de Protección de Datos (CEPD), Recomendaciones 02/2020 sobre las Garantías Esenciales Europeas para las medidas de vigilancia, 10 de noviembre de 2020.

[15] CEPD, Recomendaciones 02/2020 sobre las Garantías Esenciales Europeas para las medidas de vigilancia, 10 de noviembre de 2020, párrafos 43-47.

[16] CEPD, Recomendaciones 02/2020 sobre las Garantías Esenciales Europeas para las medidas de vigilancia, 10 de noviembre de 2020, párrafo 39.

salvaguardias específicas previstas en la propuesta fueron acogidas con satisfacción por el SEPD[17].

CCBE recuerda que la persona interesada cuyos datos personales se transfieren a un tercer país debe gozar de un nivel de protección esencialmente equivalente al que se garantiza en la Unión Europea[18]. Por lo tanto, cualquier transferencia de datos personales a entidades privadas realizada por Europol, dentro o fuera de la UE, debe respetar las mencionadas garantías esenciales europeas reconocidas por el Comité Europeo de Protección de Datos:

- **La transferencia debe basarse en normas claras, precisas y accesibles.**
- **Es necesario demostrar la necesidad y la proporcionalidad con respecto a los objetivos legítimos que se persiguen.**
- **Debe garantizarse una supervisión judicial independiente.**
- **El sujeto de los datos debe disponer de recursos efectivos.**

Además, CCBE considera que deben incluirse en la propuesta salvaguardias adicionales en relación con la transferencia o transmisión de datos personales a entidades privadas por parte de Europol, más allá de las previstas en la propuesta de reglamento y en la ley de protección de datos de la UE. CCBE subraya que cualquier transferencia de datos personales a partes privadas debe tener debidamente en cuenta los derechos de la defensa y el derecho a un juicio justo. En cualquier caso, Europol velará por que no se transfieran datos personales protegidos por el secreto profesional.

Asimismo, antes de cualquier transmisión de datos personales a entidades privadas, Europol deberá asegurarse de que los datos son adecuados, pertinentes y están actualizados. Esto es de gran importancia cuando, por ejemplo, los datos se refieren a información relacionada con una infracción penal de la que el interesado ha sido absuelto.

Como recomendó el SEPD en su dictamen sobre la propuesta, estas garantías deben aplicarse a las transmisiones a particulares dentro o fuera de la UE[19].

B. Nuevas competencias de Europol en materia de investigación e innovación

CCBE considera que el poder de investigación e innovación propuesto debería estar vinculado a fuertes salvaguardias, en particular sobre la transparencia y la supervisión, especialmente por parte del SEPD.

1. Desarrollo de tecnologías basadas en la IA para las autoridades policiales

[17] Dictamen del SEPD sobre la propuesta de modificación del Reglamento de Europol, Dictamen 4/2021, 8 de marzo de 2021, punto 18.

[18] TJUE, 16 julio de 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, C-311/18, párrafo 96.

[19] Dictamen del SEPD sobre la propuesta de modificación del Reglamento de Europol, Dictamen 4/2021, 8 de marzo de 2021, punto 18.

Según el considerando 38, "*Europol debe desempeñar un papel clave a la hora de ayudar a los Estados miembros a desarrollar nuevas soluciones tecnológicas basadas en la inteligencia artificial, lo que redundaría en beneficio de las autoridades policiales nacionales en toda la Unión*".

CCBE considera que Europol no debe liderar el desarrollo de nuevas soluciones tecnológicas basadas en la IA para las autoridades policiales. De hecho, CCBE subraya que todavía es pronto para evaluar de forma crítica el papel que deben desempeñar las herramientas de IA en el ámbito de la aplicación de la ley y la justicia penal, si es que lo hacen. Si bien es posible que el uso de la IA contribuya a la prevención o resolución de delitos, los riesgos de sesgo y discriminación contra determinados grupos de la sociedad son elevados, y la amenaza de la vigilancia masiva por parte de los sistemas de IA supone un riesgo para las sociedades abiertas y plurales.

Por lo tanto, las herramientas basadas en la IA para la aplicación de la ley sólo deben introducirse cuando existan suficientes salvaguardias contra cualquier forma de sesgo o discriminación. Todas las medidas de aumento de la vigilancia deben equilibrarse cuidadosamente con el impacto que puedan tener en una sociedad abierta y plural. En este sentido, no corresponde a Europol, como Agencia Europea para el cumplimiento de la ley, desempeñar un papel clave en la promoción de una inteligencia artificial de carácter ético, fiable y centrada en el ser humano, sujeta a sólidas salvaguardias en términos de seguridad, protección y derechos fundamentales. Si hay que desarrollar tecnologías basadas en la IA para los sistemas de justicia y de aplicación de la ley a nivel europeo, debería ser el legislador europeo el que construyera primero las mencionadas salvaguardias de forma abierta y transparente.

2. Alcance de las actividades de investigación e innovación de Europol

En base al nuevo artículo 18.2 e), Europol podría tratar datos personales con el fin de desarrollar "*actividades de investigación e innovación relativas a los aspectos contemplados en el presente Reglamento con vistas al desarrollo, la formación, el ensayo y la validación de algoritmos para el desarrollo de herramientas*".

CCBE observa que el SEPD, en su dictamen sobre la propuesta de modificación del Reglamento de Europol, llegó a la conclusión de que el alcance de la finalidad de tratamiento de la investigación y la innovación está definido con demasiada amplitud en el nuevo artículo 18.2 e)[20]. CCBE está de acuerdo con esta conclusión.

Teniendo en cuenta los elevados riesgos de discrecionalidad y las amenazas de la vigilancia masiva, el ámbito de las actividades de investigación e innovación de Europol debería definirse claramente en la propuesta indicando, en particular, los objetivos que se persiguen, las actividades a las que se dirigen las autoridades policiales, las herramientas que se desarrollarán y sus usos previstos.

3. Garantías y control de las actividades de investigación e innovación de Europol (nuevo artículo 33 bis)

CCBE toma nota de que se han previsto salvaguardias adicionales en un nuevo artículo 33 bis relativo al tratamiento de datos personales por parte de Europol en el contexto de la investigación y la innovación. Además, Europol está obligada a mantener una descripción completa y detallada del tratamiento y de la justificación de la formación, las pruebas y la validación de los algoritmos para garantizar la transparencia y para verificar la exactitud de los resultados.

[20] Dictamen del SEPD sobre la propuesta de modificación del Reglamento de Europol, Dictamen 4/2021, 8 de marzo de 2021, punto 33.

Por lo que respecta al control de las actividades de investigación e innovación de Europol, la propuesta establece que todo proyecto estará sujeto a la autorización previa del Director Ejecutivo de Europol, basada en una descripción de la actividad de tratamiento prevista que establezca la necesidad del tratamiento; una descripción del período de conservación; las condiciones de acceso a los datos; una evaluación del impacto de la protección de datos sobre los riesgos para todos los derechos y libertades de las personas interesadas, incluida cualquier discrecionalidad en el resultado, y las medidas previstas para hacer frente a esos riesgos. Asimismo, antes de iniciar un proyecto de tratamiento de datos.

CCBE considera que las garantías establecidas en la propuesta son necesarias. Sin embargo, dichas salvaguardias no son suficientes y no constituyen más que un mínimo. En cuanto a la autorización previa de los proyectos de investigación e innovación, CCBE considera que dicha autorización debe proceder de una autoridad independiente. El director ejecutivo de Europol no debe ser el único que decida si un proyecto debe ponerse en marcha o no, ni el único que realice una evaluación del impacto de la protección de datos sobre los riesgos para los derechos y libertades de las personas interesadas, incluidos, entre otros, los riesgos de discrecionalidad.

Esta tarea podría encomendarse al SEPD. CCBE observa que el Reglamento de Europol ya prevé, en su artículo 43, letra f), que el SEPD imponga una prohibición temporal o definitiva de las operaciones de tratamiento de Europol que infrinjan las disposiciones que regulan el tratamiento de datos personales. Sin embargo, teniendo en cuenta los riesgos y amenazas que se plantean para los derechos y libertades, dicha evaluación no debería ser posterior al lanzamiento de un nuevo proyecto de investigación e innovación por parte de Europol.

Además, CCBE subraya que, por las razones expuestas anteriormente, el GCPC debe ser informado caso por caso antes del lanzamiento de cualquier proyecto de investigación e innovación. Dichos proyectos también deberían llevarse a cabo de forma transparente, no sólo en lo que respecta a los resultados de la investigación, sino también a todo el proceso. Las partes interesadas, incluida la profesión jurídica, a las que afecta el uso de las herramientas para las autoridades policiales deben ser informadas de cada proyecto previsto y ser consultadas al respecto.

C. Observaciones finales

Por último, CCBE llama la atención sobre el informe del Supervisor Europeo de Protección de Datos (SEPD) de 17 de septiembre de 2020, que dio lugar a una "amonestación" formal contra Europol, basada en el tratamiento potencialmente ilegal de datos personales de un gran número de personas inocentes.

Según el informe, Europol recibe enormes cantidades de datos de las fuerzas de seguridad nacionales y de otros lugares, y con el fin de utilizar esos datos para las investigaciones penales, ha adoptado medios y métodos que no se ajustan a la legislación por la que se rige la agencia.

El resultado, dice el SEPD, es:

"…una situación en la que se almacenan en los sistemas de Europol durante varios años grandes cantidades de datos personales cuya conformidad con los requisitos establecidos por... el Reglamento de Europol es incierta. Como tal, el almacenamiento continuado de datos personales que podrían ir más allá de los límites contenidos en estos artículos socava el principio de minimización de datos…"

El informe subraya que lo más probable es que Europol esté tratando ilegalmente los datos personales de un gran número de personas -cuyo número, de hecho, se desconoce: *"…es muy probable que Europol procese continuamente datos personales de personas para las que no está autorizado a hacerlo y conserve categorías de datos personales que van más allá de la lista restrictiva prevista en... el Reglamento de Europol. Aunque no se puede cuantificar la cantidad exacta, el aumento del uso [...] observado durante los últimos años muestra claramente que la cantidad de conjuntos de datos compartidos por los Estados miembros con Europol está creciendo rápidamente."*

El informe también expone lo que esto significa para los individuos: *"El tratamiento de datos sobre personas en una base de datos policial de la UE puede tener profundas consecuencias para los implicados. Sin una aplicación adecuada del principio de minimización de datos y de las salvaguardias específicas contenidas en el Reglamento de Europol, los interesados corren el riesgo de ser vinculados erróneamente a una actividad delictiva en toda la UE, con todos los perjuicios potenciales para su vida personal y familiar, su libertad de circulación y su profesión que ello supone."*

CCBE insta a Europol y a las instituciones europeas competentes a que, antes de cualquier otro proceso legislativo o de adopción de medidas, aborden las cuestiones anteriores dando una respuesta adecuada, indicando especialmente las medidas y políticas necesarias que tienen previsto emprender para abordar la cuestión del tratamiento ilícito de datos personales que se ha planteado.

Además, CCBE señala que el reglamento de Europol debe ser evaluado por la Comisión Europea, antes del 1 de mayo de 2022. El artículo 68 establece que esta evaluación debe valorar, en particular, el impacto, la eficacia y la eficiencia de Europol y de sus prácticas de trabajo. Esta evaluación es la mejor ocasión para llevar a cabo una valoración profunda del reglamento en cuanto a la compatibilidad de las actividades de Europol con los derechos fundamentales. Por lo tanto, CCBE considera que la adopción de la propuesta de reforzar el mandato de Europol, tras la advertencia del SEPD, es prematura y precipitada.