CEPD-SEPD

Dictamen conjunto 5/2021

sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial)

18 de junio de 2021

Resumen ejecutivo

El 21 de abril de 2021, la Comisión Europea presentó su propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (en lo sucesivo, la «propuesta»). El CEPD y el SEPD acogen con satisfacción la preocupación del legislador a la hora de abordar el uso de la inteligencia artificial (IA) en la Unión Europea (UE) y subrayan que la propuesta tiene importantes **implicaciones en materia de protección de datos**.

El CEPD y el SEPD observan que la **base jurídica** de la propuesta es, en primer lugar, el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE). Además, la propuesta también se basa en el artículo 16 del TFUE en la medida en que contiene normas específicas sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, en particular las restricciones al uso de sistemas de IA para la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley. El CEPD y el SEPD recuerdan que, en consonancia con la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE), el artículo 16 del TFUE proporciona una base jurídica adecuada cuando la protección de los datos personales es una de las finalidades o uno de los componentes esenciales de las normas adoptadas por el legislador de la Unión. La aplicación del artículo 16 del TFUE también implica la **necesidad de garantizar un control independiente del cumplimiento** de los requisitos relativos al tratamiento de datos personales, como también exige el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

En cuanto al **ámbito de aplicación de la propuesta**, el CEPD y el SEPD acogen con gran satisfacción el hecho de que se extienda a la puesta a disposición y el uso de sistemas de IA por parte de las instituciones, organismos o agencias de la UE. Sin embargo, la **exclusión de la cooperación internacional con fines de aplicación de la ley del ámbito de aplicación** de la propuesta suscita serias preocupaciones para el CEPD y el SEPD, ya que tal exclusión crea un riesgo significativo de elusión (por ejemplo, terceros países u organizaciones internacionales que gestionan aplicaciones de alto riesgo a las que recurren las autoridades públicas de la UE).

El CEPD y el SEPD **acogen con satisfacción el enfoque basado en los factores de riesgo** que sustenta la propuesta. Sin embargo, este enfoque deberá aclararse y el concepto de «riesgo para los derechos fundamentales» debe armonizarse con el RGPD y el Reglamento (UE) 2018/1725 (RPDUE), ya que entran en juego aspectos relacionados con la protección de los datos personales.

El CEPD y el SEPD están de acuerdo con la propuesta cuando afirma que el hecho de que un **sistema de IA sea considerado de alto riesgo no significa necesariamente que sea legal** *per se* y que pueda ser desplegado por el usuario como tal. **Es posible** que la persona responsable del tratamiento **tenga que cumplir otros requisitos derivados de la legislación de la UE en materia de protección de datos.** Además, el cumplimiento de las obligaciones legales derivadas de la legislación de la Unión (incluida la protección de datos personales) deberá ser una condición previa para poder entrar en el mercado europeo como producto con el marcado CE. A tal fin, el CEPD y el SEPD consideran que **el requisito de garantizar el cumplimiento del RGPD y del RPDUE deberá incluirse en el capítulo 2 del título III.** Además, el CEPD y el SEPD consideran necesario adaptar el procedimiento de evaluación de la conformidad de la

propuesta para que las terceras partes realicen siempre evaluaciones *ex ante* de la conformidad de los sistemas de IA de alto riesgo.

Habida cuenta del gran riesgo de discriminación, la propuesta prohíbe la «clasificación social» cuando se realiza «durante un determinado período de tiempo» o «por las autoridades públicas o en su nombre». Sin embargo, las empresas privadas, como las redes sociales y los proveedores de servicios en la nube, también pueden tratar grandes cantidades de datos personales y realizar clasificaciones sociales. Por consiguiente, **el futuro Reglamento sobre la IA deberá prohibir cualquier tipo de clasificación social.**

La identificación biométrica remota de las personas en espacios de acceso público supone un riesgo elevado de intrusión en la vida privada de las personas, con graves efectos en las expectativas de la población de conservar el anonimato en los espacios públicos. Por estas razones, el CEPD y el SEPD **piden una prohibición general del uso de la IA para el reconocimiento automatizado de rasgos humanos en espacios de acceso público**, como los rostros, pero también la marcha, las huellas dactilares, el ADN, la voz, las pulsaciones de teclas y otras señales biométricas o conductuales, en cualquier contexto. También se recomienda **prohibir los sistemas de IA que clasifiquen a las personas a partir de sus datos biométricos en grupos** por razón de su origen étnico, sexo, orientación política o sexual u otros motivos de discriminación con arreglo al artículo 21 de la Carta. Además, el CEPD y el SEPD consideran que el uso de la IA para **inferir emociones de una persona física es altamente indeseable y deberá prohibirse.**

El CEPD y el SEPD acogen con satisfacción la **designación del SEPD como autoridad competente y de vigilancia del mercado para la supervisión de las instituciones, órganos y organismos de la Unión.** No obstante, deberá aclararse en mayor medida el papel y las funciones del SEPD, en particular por lo que se refiere a su papel como autoridad de vigilancia del mercado. Además, el futuro Reglamento sobre la IA deberá establecer claramente la **independencia de las autoridades de supervisión** en el ejercicio de sus funciones de supervisión y ejecución.

La designación de las autoridades de protección de datos (APD) como autoridades nacionales de supervisión garantizaría un enfoque regulador más armonizado, contribuiría a una interpretación coherente de las disposiciones sobre tratamiento de datos y evitaría contradicciones en su aplicación entre los Estados miembros. En consecuencia, el CEPD y el SEPD consideran que **las autoridades de protección de datos deberán ser designadas autoridades nacionales de supervisión de conformidad con el artículo 59 de la propuesta**.

La propuesta asigna un papel predominante a la Comisión en el «Comité Europeo de Inteligencia Artificial» (CEIA). Este papel entra en conflicto con la necesidad de que un organismo europeo de IA sea independiente de cualquier influencia política. Para garantizar su independencia, el futuro Reglamento sobre la IA deberá otorgar **más autonomía al CEIA** y garantizar que pueda actuar por propia iniciativa.

Teniendo en cuenta la dispersión de los sistemas de IA en el mercado único y la probabilidad de que se produzcan casos transfronterizos, existe una necesidad crucial de una aplicación armonizada y una asignación adecuada de competencias entre las autoridades nacionales de supervisión. El CEPD y el SEPD sugieren que se prevea un **mecanismo que garantice un punto de contacto único para las personas físicas afectadas por la legislación, así como para las empresas, para cada sistema de IA**.

Por lo que respecta a los **espacios de pruebas**, el CEPD y el SEPD **recomiendan que se aclare su ámbito de aplicación y sus objetivos**. La propuesta también deberá indicar claramente que la base jurídica de dichos espacios de pruebas deberá cumplir los requisitos establecidos en el marco de protección de datos existente.

El **sistema de certificación** descrito en la propuesta **carece de una relación clara con la legislación de la UE en materia de protección de datos**, así como con la legislación de la UE y de los Estados miembros aplicable a cada «ámbito» de sistema de IA de alto riesgo, y no tiene en cuenta los **principios de minimización de datos y protección de datos desde el diseño** como uno de los aspectos que deben tenerse en cuenta **antes de obtener el marcado CE**. Por consiguiente, el CEPD y el SEPD recomiendan que se modifique la propuesta para aclarar la relación entre los certificados expedidos en virtud de dicho Reglamento y los certificados, sellos y marcas de protección de datos. Por último, las APD deberán participar en la elaboración y el establecimiento de normas armonizadas y especificaciones comunes.

Por lo que respecta a los **códigos de conducta**, el CEPD y el SEPD consideran **necesario aclarar** si la protección de los datos personales debe considerarse entre los «requisitos adicionales» que pueden ser abordados por estos códigos de conducta y garantizar que las «especificaciones y soluciones técnicas» no entren en conflicto con las normas y principios del actual marco de protección de datos de la UE.

ÍNDICE

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

Visto el artículo 42, apartado 2, del Reglamento 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 deroga el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE ([1]),

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

Vista la solicitud de dictamen conjunto del Supervisor Europeo de Protección de Datos y del Comité Europeo de Protección de Datos, de 22 de abril de 2021, sobre la propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial),

HAN ADOPTADO EL SIGUIENTE DICTAMEN CONJUNTO

1 INTRODUCCIÓN

1. La llegada de los sistemas de inteligencia artificial («IA») es un paso muy importante en la evolución de las tecnologías y en la manera en que los seres humanos interactúan con ellas. La IA es un conjunto de tecnologías clave que alterarán profundamente nuestra vida cotidiana, ya sea desde un punto de vista social o económico. En los próximos años, se esperan decisiones fundamentales para la IA a medida que nos ayude a superar algunos de los mayores retos a los que nos enfrentamos hoy en día en muchos ámbitos, desde la salud hasta la movilidad, o desde la administración pública hasta la educación.

2. Sin embargo, los avances prometidos no están exentos de riesgos. De hecho, los riesgos son muy importantes teniendo en cuenta que, en gran medida, los efectos individuales y sociales de los sistemas de IA no se han observado antes. La generación de contenidos, la realización de predicciones o la toma de decisiones de forma automatizada que los sistemas de IA realizan mediante técnicas de aprendizaje automático o reglas de inferencia lógica y probabilística no son las mismas que las que llevan a cabo los seres humanos mediante un razonamiento creativo o teórico, con plena responsabilidad por las consecuencias.

3. La IA ampliará la cantidad de predicciones que pueden hacerse en muchos ámbitos, empezando por las correlaciones mensurables entre datos invisibles para los ojos humanos, pero visibles para las máquinas, facilitando nuestras vidas y resolviendo un gran número de problemas. Sin embargo, al mismo tiempo, erosionará nuestra capacidad de dar una interpretación causal a los

([1]) DO L 295 de 21.11.2018, pp. 39-98.
([2]) Las referencias a los «Estados miembros» realizadas en el presente documento deben entenderse como referencias a los «Estados miembros del EEE».

resultados, de modo que los conceptos de transparencia, control humano, rendición de cuentas y responsabilidad por los resultados se verán seriamente cuestionados.

4. Los datos (personales y no personales) en la IA son, en muchos casos, la premisa clave de las decisiones autónomas, lo que inevitablemente afectará a la vida de las personas a distintos niveles. Esta es la razón por la que el CEPD y el SEPD, ya en esta fase, afirman firmemente que la propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (en lo sucesivo, «Ley de Inteligencia Artificial») (en lo sucesivo, «la propuesta») ([3]) tiene **importantes implicaciones en materia de protección de datos**.

5. Asignar a las máquinas la tarea de decidir a partir de datos creará riesgos para los derechos y libertades de las personas, afectará a su vida privada y podría perjudicar a algunos grupos o incluso a las sociedades en su conjunto. El CEPD y el SEPD subrayan que el derecho a la vida privada y a la protección de los datos personales, que contradicen con la asunción de la autonomía de decisión de las máquinas que subyace al concepto de IA, es un pilar de los valores de la UE reconocidos en la Declaración Universal de Derechos Humanos (artículo 12), el Convenio Europeo de Derechos Humanos (artículo 8) y la Carta de los Derechos Fundamentales de la UE (en lo sucesivo, «la Carta») (artículos 7 y 8). Conciliar la perspectiva de crecimiento que ofrecen las aplicaciones de IA y la centralidad y primacía de los seres humanos frente a las máquinas es un objetivo muy ambicioso, pero necesario.

6. El CEPD y el SEPD acogen con satisfacción la participación en la regulación de todas las partes interesadas de la cadena de valor de la IA y la introducción de requisitos específicos para los proveedores de soluciones, ya que desempeñan un papel importante en los productos que utilizan sus sistemas. Sin embargo, las responsabilidades de las distintas partes (usuario, proveedor, importador o distribuidor de un sistema de IA) deben estar claramente definidas y asignadas. En particular, en el tratamiento de datos personales deberá prestarse especial atención a la coherencia de estas funciones y responsabilidades con los conceptos de responsable y encargado del tratamiento contenidos en el marco de protección de datos, ya que ambas normas no son congruentes.

7. La propuesta otorga un lugar importante al concepto de vigilancia humana (artículo 14) que el CEPD y el SEPD acogen favorablemente. Sin embargo, como se ha indicado anteriormente, debido al fuerte impacto potencial de determinados sistemas de IA para personas físicas o grupos de personas, la verdadera centralidad humana deberá aprovechar la vigilancia humana altamente cualificada y un tratamiento lícito en la medida en que dichos sistemas se basen en el tratamiento de datos personales o traten datos personales para cumplir su cometido, a fin de garantizar que se respete el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado.

8. Además, debido al carácter intensivo de datos de muchas aplicaciones de IA, la propuesta deberá promover la adopción de un enfoque de protección de datos desde el diseño y por defecto a todos los niveles, fomentando la aplicación efectiva de los principios de protección

([3]) COM(2021) 206 final.

de datos (tal como se prevé en el artículo 25 del RGPD y en el artículo 27 del RPDUE) mediante tecnologías de vanguardia.

9. Por último, el CEPD y el SEPD subrayan que este dictamen conjunto se emite únicamente como análisis preliminar de la propuesta, sin perjuicio de cualquier otra evaluación y dictamen sobre sus efectos y compatibilidad con la legislación de la UE en materia de protección de datos.

2 ANÁLISIS DE LOS PRINCIPIOS CLAVE DE LA PROPUESTA

2.1 Ámbito de aplicación de la propuesta y relación con el marco jurídico vigente

10. Según la exposición de motivos, la **base jurídica** de la propuesta es, en primer lugar, el artículo 114 del TFUE, que prevé la adopción de medidas para garantizar el establecimiento y el funcionamiento del mercado interior ([4]). Además, la propuesta se basa en el artículo 16 del TFUE *en la medida en que contiene normas específicas sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales*, en particular, restricciones al uso de sistemas de IA para la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley ([5]).

11. El CEPD y el SEPD recuerdan que, en consonancia con la jurisprudencia del TJUE, el artículo 16 del TFUE proporciona una base jurídica adecuada cuando la protección de los datos personales es una de las finalidades o uno de los componentes esenciales de las normas adoptadas por el legislador de la Unión ([6]). La aplicación del artículo 16 del TFUE también implica la necesidad de garantizar una supervisión independiente del cumplimiento de los requisitos relativos al tratamiento de datos personales, como también exige el artículo 8 de la Carta.

12. El SEPD y el CEPD recuerdan que ya existe un marco general de protección de datos adoptado sobre la base del artículo 16 del TFUE, consistente en el Reglamento general de protección de datos (RGPD) ([7]), el Reglamento de protección de datos para las instituciones, órganos y organismos de la Unión Europea (RPDUE) ([8]) y la Directiva sobre protección de datos en el

([4]) Exposición de motivos, p. 5.
([5]) Exposición de motivos, p. 6. Véase también el considerando 2 de la propuesta.
([6]) Dictamen de 26 de julio de 2017, *PNR Canadá*, Procedimiento de dictamen 1/15, ECLI:EU:C:2017:592, apartado 96.
([7]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119 de 4.5.2016, pp. 1-88).
([8]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, pp. 39-98).

ámbito penal (LED) ([9]). Según la propuesta, solo las restricciones adicionales relativas al tratamiento de datos biométricos contenidas en la misma pueden considerarse basadas en el artículo 16 del TFUE y, por lo tanto, tener la misma base jurídica que el RGPD, el RPDUE o la LED. Esto tiene importantes implicaciones para la relación de la propuesta con el RGPD, el RPDUE y la LED en general, como se expone a continuación.

13. Por lo que se refiere al **ámbito de aplicación de la propuesta**, el CEPD y el SEPD acogen con gran satisfacción el hecho de que la propuesta incluya el uso de sistemas de IA por parte de las instituciones, órganos y organismos de la UE. Dado que el uso de sistemas de IA por parte de estas entidades también puede tener un impacto significativo en los derechos fundamentales de las personas, similar al uso en los Estados miembros de la UE, es indispensable que el nuevo marco regulador de IA se aplique tanto a los Estados miembros como a las instituciones, órganos y organismos de la UE, a fin de garantizar un enfoque coherente en toda la Unión. Dado que las instituciones, órganos y organismos de la UE pueden actuar tanto como proveedores como como usuarios de sistemas de IA, el SEPD y el CEPD consideran plenamente apropiado incluir a estas entidades en el ámbito de aplicación de la propuesta sobre la base del artículo 114 del TFUE.

14. Sin embargo, el CEPD y el SEPD albergan serias dudas en cuanto a la exclusión de la cooperación internacional con fines de aplicación de la ley del ámbito de aplicación establecido en el artículo 2, apartado 4, de la propuesta. Esta exclusión crea un riesgo significativo de elusión (por ejemplo, terceros países u organizaciones internacionales que gestionan aplicaciones de alto riesgo a las que recurren las autoridades públicas de la UE).

15. El desarrollo y la utilización de sistemas de IA implicarán en muchos casos el tratamiento de datos personales. Es de suma importancia garantizar la claridad de la relación de la presente propuesta con la legislación vigente de la UE en materia de protección de datos. La propuesta se entiende sin perjuicio y complementa el RGPD, el RPDUE y la LED. Si bien los considerandos de la propuesta aclaran que el uso de los sistemas de IA deberá seguir cumpliendo la legislación sobre protección de datos, **el CEPD y el SEPD recomiendan encarecidamente que se aclare en el artículo 1 de la propuesta que la legislación de la Unión en materia de protección de datos personales,** en particular el RGPD, el RPDUE, la Directiva sobre la privacidad y las comunicaciones electrónicas ([10]) y la Directiva LED, se aplicará a todo tratamiento de datos personales que entre en el ámbito de aplicación de la propuesta. El considerando pertinente deberá del mismo modo aclarar que la propuesta no persigue afectar a la aplicación de la legislación de la UE que regula el tratamiento de datos de

([9]) 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. 89-131).

([10]) 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), modificada por la Directiva 2006/24/CE y la Directiva 2009/136/CE.

carácter personal, incluidas las funciones y facultades de las autoridades de control independientes con competencias para supervisar el cumplimiento de dichos instrumentos.

2.2 Enfoque basado en los factores de riesgo

16. El CEPD y el SEPD **acogen con satisfacción el enfoque basado en los factores de riesgo** que sustenta la propuesta. La propuesta se aplicaría a todos los sistemas de IA, incluidos aquellos que no impliquen el tratamiento de datos personales, pero puedan seguir afectando a los intereses o a los derechos y libertades fundamentales.

17. El CEPD y el SEPD observan que algunas de las disposiciones de la propuesta excluyen los riesgos para grupos de personas o para la sociedad en su conjunto (por ejemplo, efectos colectivos de especial relevancia, como la discriminación de grupo o la expresión de opiniones políticas en espacios públicos). El CEPD y el SEPD recomiendan que los riesgos sociales o de grupo que plantean los sistemas de IA se evalúen y mitiguen por igual.

18. El CEPD y el SEPD opinan que deberá aclararse el enfoque basado en los factores de riesgo de la propuesta y que el concepto de «riesgo para los derechos fundamentales» **se ajusta al RGPD** en la medida en que entren en juego aspectos relacionados con la protección de los datos personales. Tanto si se trata de usuarios finales o como simplemente de personas interesadas o afectadas por el sistema de IA, la falta de referencia en el texto a la persona afectada por el sistema de IA aparece como ángulo muerto en la propuesta. De hecho, las obligaciones impuestas a los agentes frente a las personas afectadas deberán emanar más concretamente de la protección de la persona y de sus derechos. Así pues, el CEPD y el SEPD instan al legislador a que aborde explícitamente en la propuesta los **derechos y las vías de recurso de que disponen las personas** sujetas a sistemas de IA.

19. El CEPD y el SEPD toman nota de la decisión de proporcionar una lista exhaustiva de **sistemas de IA de alto riesgo**. Esta elección podría generar un efecto blanco y negro con escasa capacidad de atracción de situaciones de alto riesgo, lo que socavaría el enfoque general basado en factores de riesgo que subyace a la propuesta. Asimismo, esta lista de sistemas de IA de alto riesgo detallada en los anexos II y III de la propuesta carece de algunos tipos de casos de uso que entrañan riesgos significativos, como el uso de IA para determinar la prima de seguro, evaluar tratamientos médicos o con fines de investigación sanitaria. El CEPD y el SEPD también destacan que dichos anexos tendrán que actualizarse periódicamente para garantizar que su ámbito de aplicación es adecuado.

20. La propuesta exige que los **proveedores** de sistemas de IA realicen una evaluación de riesgos. Sin embargo, en la mayoría de los casos, los responsables del tratamiento (de datos) serán los **usuarios** en lugar de los proveedores de los sistemas de IA (por ejemplo, un usuario de un sistema de reconocimiento facial es un «responsable del tratamiento» y, por lo tanto, no está sujeto a los requisitos aplicables a los proveedores de IA de alto riesgo con arreglo a la propuesta).

21. Además, **un proveedor no siempre podrá evaluar todos los usos** del sistema de IA. Así pues, la evaluación de riesgos inicial será de carácter más general que la realizada por el usuario del sistema de IA. Aunque la evaluación de riesgos inicial por parte del proveedor no indique que

el sistema de IA sea «de alto riesgo» en el marco de la propuesta, esto no deberá excluir **una evaluación posterior (más detallada)** [evaluación de impacto relativa a la protección de datos (EIPD) en virtud del artículo 35 del RGPD, del artículo 39 del RPDUE o del artículo 27 de la LED] **que deberá realizar el usuario del sistema**, teniendo en cuenta el contexto de uso y los casos de uso específicos. La interpretación de si, con arreglo al RGPD, al RPDUE y a la LED, un tipo de tratamiento puede dar lugar a un riesgo elevado debe hacerse con independencia de la propuesta. Sin embargo, la clasificación de un sistema de IA como «de alto riesgo» debido a su impacto en los derechos fundamentales ([11]) **da lugar a una presunción de «alto riesgo» en el marco del RGPD, el RPDUE y la LED en la medida en que se tratan datos personales.**

22. **El CEPD y el SEPD están de acuerdo con la Propuesta cuando especifica que la clasificación de un sistema de IA como de alto riesgo no significa necesariamente que sea legal *per se* y que pueda ser desplegado por el usuario como tal. Es posible que el responsable del tratamiento tenga que cumplir otros requisitos derivados de la legislación de la UE en materia de protección de datos.** Además, el razonamiento subyacente al artículo 5 de la propuesta, según el cual, a diferencia de los sistemas prohibidos, los sistemas de alto riesgo pueden ser admisibles en principio, debe abordarse y eliminarse en la propuesta, especialmente porque el marcado CE propuesto no implica que el tratamiento asociado de datos personales sea lícito.

23. No obstante, el cumplimiento de las obligaciones legales derivadas de la legislación de la Unión (incluida la protección de datos personales) deberá ser una condición previa para poder entrar en el mercado europeo como producto con el marcado CE. A tal fin, el CEPD y el SEPD **recomiendan incluir en el capítulo 2 del título III de la propuesta el requisito de garantizar el cumplimiento del RGPD y del RPDUE.** Estos requisitos serán auditados (por auditoría de terceros) antes del marcado CE, de conformidad con el principio de rendición de cuentas. En el contexto de esta evaluación por terceros, la evaluación de impacto inicial que llevará a cabo el proveedor será especialmente pertinente.

24. Habida cuenta de las complejidades provocadas por el desarrollo de sistemas de IA, cabe señalar que las características técnicas de los sistemas de IA (por ejemplo, el tipo de enfoque de IA) podrían dar lugar a mayores riesgos. Por lo tanto, cualquier evaluación del riesgo del sistema de IA deberá tener en cuenta las **características técnicas**, junto con sus **casos de uso específicos y el contexto en el que opera el sistema**.

25. A la luz de lo anterior, el CEPD y el SEPD recomiendan especificar en la propuesta que el **proveedor** llevará a cabo una evaluación inicial del riesgo del sistema de IA en cuestión, **teniendo en cuenta los casos de uso** [que se especificarán en la propuesta, complementando,

([11]) La Agencia de los Derechos Fundamentales de la Unión Europea (FRA) ya ha abordado la necesidad de llevar a cabo evaluaciones de impacto en materia de derechos fundamentales en el uso de IA o de tecnologías conexas. En su informe de 2020 titulado «Construir correctamente el futuro. La inteligencia artificial y los derechos fundamentales»), la FRA identificó escollos en el uso de la IA, por ejemplo en la actuación policial predictiva, el diagnóstico médico, los servicios sociales y la publicidad dirigida, y subrayó que, para reducir los efectos negativos en las personas, las organizaciones públicas y privadas deberán llevar a cabo evaluaciones de cómo la IA podría dañar los derechos fundamentales.

por ejemplo, el anexo III, punto 1, letra a), cuando no se mencionen los casos de uso de los sistemas biométricos de IA], y que el usuario del sistema de IA, en su calidad de responsable del tratamiento de datos con arreglo a la legislación de protección de datos de la UE (si procede), también llevará a cabo la EIPD como se indica en al artículo 35 del RGPD, el artículo 39 del RPDUE y el artículo 27 de la LED, teniendo en cuenta no solo las características técnicas y **el caso de uso**, sino **también el contexto específico** en que operará la IA.

26. Por otra parte, deberán aclararse algunos de los términos mencionados en el anexo III de la propuesta, por ejemplo, los servicios privados esenciales o los sistemas de IA destinados a utilizarse para evaluar la solvencia por parte de proveedores a pequeña escala para su uso propio.

2.3 Usos prohibidos de la IA

27. El CEPD y el SEPD consideran que las **formas intrusivas de IA**, especialmente las que pueden afectar a la dignidad humana, deben considerarse sistemas de IA prohibidos con arreglo al artículo 5 de la propuesta, en lugar de clasificarse simplemente como «de alto riesgo» en el anexo III de la propuesta, como las del artículo 6. Esto se aplica, en particular, a las comparaciones de datos que, a gran escala, afectan también a personas que no hayan dado ninguna causa o solo hayan dado una causa limitada a la observación policial, o a un tratamiento que atente contra el principio de limitación de la finalidad en virtud de la legislación en materia de protección de datos. El uso de la IA en el ámbito policial y de aplicación de la ley requiere normas específicas, precisas, previsibles y proporcionadas, que deben tener en cuenta los intereses de las personas afectadas y los efectos sobre el funcionamiento de una sociedad democrática.

28. El artículo 5 de la propuesta corre el riesgo de ser meramente declarativo respecto a los «valores» y a la prohibición de los sistemas de IA contrarios a dichos valores. En efecto, los criterios mencionados en el artículo 5 para «calificar» los sistemas de IA prohibidos **limitan el ámbito de aplicación de la prohibición** hasta el punto de que pueden resultar carentes de sentido en la práctica [por ejemplo, «que provoque o sea probable que provoque perjuicios físicos o psicológicos» en el artículo 5, apartado 1, letras a) y b); la limitación a las autoridades públicas en el artículo 5, apartado 1, letra c); la redacción ambigua en los incisos (i) y (ii) del apartado c); la limitación a la identificación biométrica remota «en tiempo real» únicamente sin una definición clara, etc.].

29. En particular, el uso de la IA para la «clasificación social», tal como se prevé en el artículo 5, apartado 1, letra c), de la propuesta puede dar lugar a discriminación y es contrario a los valores fundamentales de la UE. La propuesta solo prohíbe estas prácticas cuando se realizan «durante un período determinado de tiempo» o «por parte de las autoridades públicas o en representación de estas». Las empresas privadas, principalmente las redes sociales y los proveedores de servicios en la nube, pueden tratar grandes cantidades de datos personales y realizar clasificaciones sociales. Por consiguiente, **la propuesta deberá prohibir cualquier tipo de clasificación social**. Cabe señalar que, en el ámbito de la aplicación de la ley, el artículo 4 de la LED ya limita significativamente (o incluso prohíbe en la práctica) este tipo de actividades.

30. La **identificación biométrica remota** de las personas en espacios de acceso público supone un riesgo elevado de intrusión en la vida privada. Por consiguiente, el CEPD y el SEPD **consideran que es necesario un enfoque más estricto**. El uso de sistemas de IA podría plantear graves problemas de proporcionalidad, ya que podría implicar el tratamiento de datos de un número indiscriminado y desproporcionado de personas para la identificación de solo unas pocas (por ejemplo, pasajeros en aeropuertos y estaciones de tren). La naturaleza **sin fricciones** de los sistemas de identificación biométrica remota plantea, además, problemas de transparencia y cuestiones relacionadas con la base jurídica del tratamiento con arreglo a la legislación de la UE (LED, RGPD, RPDUE y otra legislación aplicable). Todavía no se ha resuelto el problema relativo a la manera de informar adecuadamente a las personas sobre este tratamiento, así como el ejercicio efectivo y oportuno de los derechos de las personas. Lo mismo se aplica a sus **graves efectos irreversibles en las expectativas** (razonables) **de la población de conservar el anonimato en los espacios públicos** y esto repercute negativamente en el ejercicio de la libertad de expresión, de reunión, de asociación y de circulación.

31. El artículo 5, apartado 1, letra d), de la propuesta establece una amplia **lista de casos excepcionales** en los que se permite la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley. El CEPD y el SEPD consideran que **este enfoque adolece de defectos** en varios aspectos. En primer lugar, no está claro qué deberá entenderse por «demora significativa» ni cómo deberá considerarse un factor atenuante, teniendo en cuenta que un sistema de identificación masiva es capaz de identificar a miles de personas en solo unas horas. Además, la intrusión del tratamiento no siempre depende de que la identificación se realice en tiempo real o no. Es probable que la identificación biométrica a distancia en el contexto de una protesta política tenga un efecto disuasorio significativo en el ejercicio de los derechos y libertades fundamentales, como la libertad de reunión y asociación y, más en general, en los principios fundacionales de la democracia. En segundo lugar, el carácter intrusivo del tratamiento no depende necesariamente de su finalidad. El uso de este sistema para otros fines, como la seguridad privada, representa las mismas amenazas para los derechos fundamentales al respeto de la vida privada y familiar y a la protección de los datos personales. Por último, incluso con las limitaciones previstas, el número potencial de personas sospechosas o autoras de delitos será casi siempre «lo suficientemente elevado» como para justificar el uso continuo de sistemas de IA para la detección de sospechosos, a pesar de las condiciones adicionales del artículo 5, apartados 2 a 4, de la propuesta. El razonamiento que subyace a la propuesta parece omitir que, a la hora de supervisar los espacios abiertos, las obligaciones derivadas de la legislación de la UE en materia de protección de datos deben cumplirse no solo para las personas sospechosas, sino para todas aquellas que son objeto de seguimiento en la práctica.

32. Por todas estas razones, el CEPD y el SEPD **piden una prohibición general del uso de la IA para el reconocimiento automatizado de rasgos humanos en espacios de acceso público, como los rostros, pero también la marcha, las huellas dactilares, el ADN, la voz, las pulsaciones de teclas y otras señales biométricas o conductuales, en cualquier contexto**. El enfoque actual de la propuesta es identificar y enumerar todos los sistemas de IA que deberán prohibirse. Así pues, por razones de coherencia, los **sistemas de IA para la identificación**

remota a gran escala en espacios en línea deberán prohibirse en virtud del artículo 5 de la propuesta. Teniendo en cuenta la LED, el RPDUE y el RGPD, el SEPD y el CEPD no pueden discernir en qué medida esta práctica podría cumplir los requisitos de necesidad y proporcionalidad y que, en última instancia, se deriva de lo que el TJUE y el TEDH consideran injerencias aceptables de los derechos fundamentales.

33. Además, el CEPD y el SEPD **recomiendan la prohibición**, tanto para las autoridades públicas como para las entidades privadas, de los **sistemas de IA que clasifican a las personas a partir de datos biométricos (por ejemplo, el reconocimiento facial) en grupos por razón de su origen étnico, sexo, orientación política o sexual u otros motivos de discriminación prohibidos en virtud del artículo 21 de la Carta**, o los sistemas de IA cuya validez científica no está demostrada o que están en conflicto directo con los valores esenciales de la UE [por ejemplo, el polígrafo, anexo III, apartado 6, letra b), y apartado 7, letra a)]. En consecuencia, la «**clasificación biométrica**» deberá **prohibirse en virtud del artículo 5**.

34. **La determinación o clasificación por un ordenador de la conducta futura con independencia de la voluntad propia** también **afecta a la dignidad humana.** Los sistemas de IA destinados a ser utilizados por las autoridades encargadas de la aplicación de la ley para llevar a cabo evaluaciones de riesgos individuales de personas físicas con el objetivo de determinar el riesgo de que cometan infracciones penales [véase el anexo III, apartado 6, letra a)], o para predecir la frecuencia o reiteración de una infracción penal real o potencial con base en la elaboración de perfiles de personas físicas o en la evaluación de rasgos y características de la personalidad o conductas delictivas pasadas [véase el anexo III, apartado 6, letra e)] utilizados según su finalidad prevista conducirán a la dominación fundamental de la toma de decisiones policiales y judiciales, con la consiguiente cosificación de la persona afectada. Dichos sistemas de IA, que afectan a la esencia del derecho a la dignidad humana, deberán prohibirse en virtud del artículo 5.

35. Además, el CEPD y el SEPD consideran que el uso de la IA para **inferir emociones de una persona física es muy indeseable y deberá prohibirse**, excepto en determinados casos de uso bien especificados, a saber, con fines de salud o investigación (por ejemplo, pacientes para quienes el reconocimiento emocional es importante), siempre con las salvaguardias adecuadas y, por supuesto, con sujeción a todas las demás condiciones y límites de protección de datos, incluida la limitación de la finalidad.

2.4 Sistemas de IA de alto riesgo

2.4.1 Necesidad de una evaluación *ex ante* de la conformidad por parte de terceros externos

36. El CEPD y el SEPD acogen con satisfacción que los sistemas de IA que plantean un riesgo elevado deban someterse a una evaluación *ex ante* de la conformidad antes de poder ser introducidos en el mercado o puestos en funcionamiento en la UE. En principio, se acoge con satisfacción este modelo regulador, ya que ofrece un buen equilibrio entre la facilidad para la innovación y un alto nivel de protección proactiva de los derechos fundamentales. Para poder utilizarlo en entornos específicos, como los procesos de toma de decisiones de las instituciones

de servicio público o las infraestructuras críticas, deben establecerse las formas de investigar el código fuente completo.

37. Sin embargo, el CEPD y el SEPD abogan por adaptar el procedimiento de evaluación de la conformidad previsto en el artículo 43 de la propuesta a fin de que, **por lo general, se lleve a cabo una evaluación *ex ante* de la conformidad por parte de terceros para la IA de alto riesgo**. Aunque la evaluación por terceros de la conformidad para el tratamiento de datos personales de alto riesgo no es un requisito del RGPD ni del RPDUE, aún no se comprenden del todo los riesgos que plantean los sistemas de IA. La inclusión general de la obligación de una evaluación de la conformidad por terceros reforzaría, por tanto, la seguridad jurídica y la confianza en todos los sistemas de IA de alto riesgo.

2.4.2 El ámbito de aplicación del reglamento también debe abarcar los sistemas de IA ya en uso

38. De conformidad con el artículo 43, apartado 4, de la propuesta, los sistemas de IA de alto riesgo deberán someterse a un nuevo procedimiento de evaluación de la conformidad cada vez que se produzca un cambio significativo. Es correcto garantizar que los sistemas de IA cumplan los requisitos del Reglamento sobre la IA a lo largo de todo su ciclo de vida. Los sistemas de IA introducidos en el mercado o puestos en servicio antes de la aplicación del reglamento propuesto (o 12 meses después para los sistemas informáticos de gran magnitud enumerados en el anexo IX) quedan excluidos de su ámbito de aplicación, a menos que dichos sistemas se vean sometidos a «cambios significativos» en su diseño o finalidad prevista (artículo 83).

39. Sin embargo, el umbral para dichos «cambios significativos» no está claro. El considerando 66 de la propuesta especifica un umbral más bajo para la reevaluación de la conformidad «cada vez que se produzca un cambio que pueda afectar al cumplimiento». Un umbral similar sería adecuado para el artículo 83, al menos para los sistemas de IA de alto riesgo. Además, para colmar las lagunas de protección, es necesario que los sistemas de IA ya establecidos y en funcionamiento (tras determinada fase de aplicación) cumplan también todos los requisitos del Reglamento sobre la IA.

40. Las múltiples posibilidades de tratamiento de datos personales y los riesgos externos también afectan a la seguridad de los sistemas de IA. El enfoque del artículo 83 sobre el «cambio significativo en el diseño o la finalidad prevista» no incluye ninguna referencia a los cambios en los riesgos externos. Por lo tanto, deberá incluirse en el artículo 83 de la propuesta una referencia a los cambios en el escenario de las amenazas derivadas de riesgos externos, como los ciberataques, los ataques adversarios y las reclamaciones justificadas de los consumidores.

41. Además, dado que la aplicación está prevista veinticuatro meses después de la entrada en vigor del futuro Reglamento, el SEPD y el CEPD no consideran apropiado eximir los sistemas de IA ya introducidos en el mercado durante un período de tiempo aún más largo. Si bien la propuesta también establece que los requisitos del Reglamento se tendrán en cuenta en la evaluación de cada sistema informático de gran magnitud según lo dispuesto en los actos jurídicos enumerados en el anexo IX, el CEPD y el SEPD consideran que los requisitos relativos a la

puesta en servicio de los sistemas de IA deberán ser aplicables a partir de la fecha de aplicación del futuro Reglamento.

2.5 Gobernanza y Comité Europeo de IA

2.5.1 Gobernanza

42. El CEPD y el SEPD acogen con satisfacción la designación del SEPD como autoridad competente y de vigilancia del mercado para la supervisión de las instituciones, órganos y organismos de la Unión dentro del ámbito de aplicación de la propuesta. El SEPD está dispuesto a desempeñar su nuevo papel de regulador de la IA para la administración pública de la UE. Además, el papel y las funciones del SEPD no se describen con suficiente detalle y deberán aclararse en la propuesta, en particular por lo que se refiere a su papel como autoridad de vigilancia del mercado.

43. El CEPD y el SEPD reconocen la asignación de recursos financieros, prevista para el Comité y el SEPD, en su calidad de organismo notificante, en la propuesta. Sin embargo, el cumplimiento de las nuevas funciones previstas para el SEPD, incluso cuando actúe como organismo notificado, requerirá recursos financieros y humanos significativamente mayores.

44. Esto se debe, en primer lugar, a que la redacción del artículo 63, apartado 6, establece que el SEPD actuará como autoridad de vigilancia del mercado para las instituciones, agencias y organismos de la Unión dentro del ámbito de aplicación de la propuesta, que no aclara si el SEPD debe considerarse una «autoridad de vigilancia del mercado» plenamente incorporada, tal como se prevé en el Reglamento (UE) 2019/1020. Esto plantea dudas sobre las obligaciones y las competencias del SEPD en la práctica. En segundo lugar, y siempre que se responda afirmativamente a la pregunta anterior, no está claro de qué forma el papel del SEPD, tal como se prevé en el RPDUE, puede acomodar la tarea prevista en el artículo 11 del Reglamento (UE) 2019/1020, que incluye «la vigilancia eficaz del mercado en su territorio de los productos comercializados en línea» o las comprobaciones físicas y de laboratorio basadas en muestras adecuadas. Existe el riesgo de que asumir el nuevo conjunto de tareas sin más aclaraciones en la propuesta ponga en peligro el cumplimiento de sus obligaciones como supervisor de protección de datos.

45. Sin embargo, el CEPD y el SEPD subrayan que algunas disposiciones de la propuesta que definen las funciones y competencias de las diferentes autoridades competentes en virtud del Reglamento sobre la IA, sus relaciones, su naturaleza y la garantía de su independencia parecen poco claras en esta fase. Mientras que el Reglamento (UE) 2019/1020 establece que la autoridad de vigilancia del mercado debe ser independiente, el proyecto de reglamento no exige que las autoridades de supervisión sean independientes e incluso les obliga a informar a la Comisión sobre determinadas tareas llevadas a cabo por las autoridades de vigilancia del mercado, que pueden ser instituciones diferentes. Dado que la propuesta también establece que las APD serán las autoridades de vigilancia del mercado para los sistemas de IA utilizados con fines de aplicación de la ley (artículo 63, apartado 5), eso significa también que estarán sujetas, posiblemente a través de su autoridad nacional de supervisión, a obligaciones de información a la Comisión (artículo 63, apartado 2), lo que parece incompatible con su independencia.

46. Por consiguiente, el CEPD y el SEPD consideran que estas disposiciones deben aclararse para ser coherentes con el Reglamento (UE) 2019/1020, el RPDUE y el RGPD, y la propuesta deberá establecer claramente que las autoridades supervisoras en virtud del Reglamento sobre la IA deben ser totalmente independientes en el desempeño de sus funciones, ya que ello constituiría una garantía esencial para la correcta supervisión y cumplimiento del futuro Reglamento.

47. El CEPD y el SEPD también desean recordar que las autoridades de protección de datos ya están aplicando el RGPD, el RPDUE y la LED a los sistemas de IA que implican datos personales con el fin de garantizar la protección de los derechos fundamentales y, más concretamente, el derecho a la protección de datos. Por lo tanto, las APD ya conocen, hasta cierto punto, como exige la propuesta para las autoridades nacionales de supervisión, las tecnologías de IA, datos y computación de datos, los derechos fundamentales, y tienen conocimientos especializados en la evaluación de los riesgos que plantean las nuevas tecnologías para los derechos fundamentales. Además, cuando los sistemas de IA se basan en el tratamiento de datos personales o tratan datos personales, las disposiciones de la propuesta están directamente interrelacionadas con el marco jurídico de protección de datos, que será el caso de la mayoría de los sistemas de IA en el ámbito de aplicación del Reglamento. Como consecuencia de ello, habrá interconexiones de competencias entre las autoridades de supervisión en virtud de la propuesta y las APD.

48. Por lo tanto, la designación de las APD como autoridades nacionales de supervisión garantizaría un enfoque regulador más armonizado, contribuiría a una interpretación coherente de las disposiciones sobre tratamiento de datos y evitaría contradicciones en su aplicación entre los Estados miembros. También sería beneficioso para todas las partes interesadas de la cadena de valor de la IA disponer de un punto de contacto único para todas las operaciones de tratamiento de datos personales incluidas en el ámbito de aplicación de la propuesta y limitar las interacciones entre dos organismos reguladores diferentes para el tratamiento a los que afectan la propuesta y el RGPD. En consecuencia, el CEPD y el SEPD consideran que las APD **deberán ser designadas autoridades nacionales de supervisión de conformidad con el artículo 59 de la propuesta.**

49. En cualquier caso, en la medida en que la propuesta contiene normas específicas sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales adoptadas sobre la base del artículo 16 del TFUE, el cumplimiento de estas normas, en particular las restricciones al uso de sistemas de IA para la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley **deberá estar sujeto al control de autoridades independientes.**

50. Sin embargo, la propuesta no contiene ninguna disposición explícita que atribuya competencias al control de autoridades independientes para garantizar el cumplimiento de estas normas . La única referencia a las autoridades de control competentes en materia de protección de datos con arreglo al RGPD, o a la LED, figura en el artículo 63, apartado 5, de la propuesta, pero solo como organismos de «vigilancia del mercado» y, alternativamente, con otras autoridades. El CEPD y el SEPD consideran que este sistema no garantiza el cumplimiento del requisito de

control independiente establecido en el artículo 16, apartado 2, del TFUE y en el artículo 8 de la Carta.

2.5.2 El Comité Europeo de IA

51. La Propuesta establece un «Comité Europeo de Inteligencia Artificial» (CEIA). El CEPD y el SEPD reconocen la necesidad de una aplicación coherente y armonizada del marco propuesto, así como de la participación de personas expertas independientes en el desarrollo de la política de la UE en materia de IA. Al mismo tiempo, la propuesta prevé otorgar un papel preponderante a la Comisión. De hecho, esta última no solo formaría parte del CEIA, sino que también lo presidiría y tendría derecho de veto para la adopción del Reglamento interno del CEIA. Esto entra en conflicto con la necesidad de que un organismo europeo de IA sea independiente de cualquier influencia política. Por consiguiente, el CEPD y el SEPD consideran que el futuro Reglamento sobre la IA deberá otorgar **más autonomía al CEIA**, a fin de permitirle garantizar realmente la aplicación coherente del Reglamento en todo el mercado único.

52. El CEPD y el SEPD también señalan que no se confiere ningún poder al CEIA en relación con la ejecución del Reglamento propuesto. Aun así, teniendo en cuenta la dispersión de los sistemas de IA en el mercado único y la probabilidad de que se produzcan casos transfronterizos, existe una necesidad crucial de una aplicación armonizada y una asignación adecuada de competencias entre las autoridades nacionales de supervisión. Por consiguiente, el CEPD y el SEPD recomiendan que los mecanismos de cooperación entre las autoridades nacionales de supervisión se especifiquen en el futuro Reglamento sobre la IA. El CEPD y el SEPD sugieren que se imponga un mecanismo que garantice un punto de contacto único para las personas afectadas por la legislación, así como para las empresas, para cada sistema de IA, y que, en el caso de las organizaciones cuya actividad abarque más de la mitad de los Estados miembros de la UE, el CEIA pueda designar a la autoridad nacional responsable de hacer cumplir el Reglamento sobre la IA para este sistema de IA.

53. Además, teniendo en cuenta el carácter independiente de las autoridades que formarán el Comité, este estará facultado para actuar por iniciativa propia y no solo para prestar asesoramiento y asistencia a la Comisión. Por consiguiente, el CEPD y el SEPD subrayan la necesidad de una ampliación de la misión asignada al Comité, que además no corresponde a las tareas enumeradas en la propuesta.

54. Para cumplir estos objetivos, **el CEIA dispondrá de facultades suficientes y adecuadas**, y deberá aclararse su estatuto jurídico. En particular, para que el ámbito de aplicación material del futuro Reglamento siga siendo pertinente, parece necesario implicar en su evolución a las autoridades encargadas de su aplicación. Por consiguiente, el CEPD y el SEPD recomiendan que se faculte al CEIA para proponer a la Comisión modificaciones del anexo I, en el que se definen las técnicas y enfoques de IA, y del anexo III, en el que se enumeran los sistemas de IA de alto riesgo a que se refiere el artículo 6, apartado 2. El CEIA también deberá ser consultado por la Comisión antes de cualquier modificación de dichos anexos.

55. El artículo 57, apartado 4, de la propuesta prevé intercambios entre el Comité y otros órganos, oficinas, agencias y grupos consultivos de la Unión. Teniendo en cuenta su trabajo previo en

el ámbito de la IA y sus conocimientos especializados en materia de derechos humanos, el CEPD y el SEPD recomiendan considerar a la Agencia de los Derechos Fundamentales como una de los observadoras del Comité.

3 INTERACCIÓN CON EL MARCO DE PROTECCIÓN DE DATOS

3.1 Relación de la propuesta con la legislación vigente de la UE en materia de protección de datos

56. La relación claramente definida entre la propuesta y la legislación vigente en materia de protección de datos es un requisito previo esencial para garantizar y mantener el respeto y la aplicación del acervo de la UE en el ámbito de la protección de datos personales. Dicha legislación de la UE, en particular el RGPD, el RPDUE y la LED, debe considerarse un requisito previo en el que pueden basarse otras propuestas legislativas sin afectar a las disposiciones existentes ni interferir con ellas, también en lo que se refiere a la competencia de las autoridades de control y la gobernanza.

57. En opinión del CEPD y del SEPD, es importante, por tanto, evitar claramente en la propuesta cualquier incoherencia y posible conflicto con el RGPD, el RPDUE y la LED. Esto no solo en aras de la seguridad jurídica, sino también para evitar que la propuesta tenga por efecto poner en peligro directa o indirectamente el derecho fundamental a la protección de los datos de carácter personal, tal como se establece en el artículo 16 del TFUE y en el artículo 8 de la Carta.

58. En particular, las máquinas de autoaprendizaje solo podrían proteger los datos personales de las personas si se integran en la concepción. También es esencial la posibilidad inmediata de ejercer los derechos de las personas en virtud del artículo 22 (Decisiones individuales automatizadas, incluida la elaboración de perfiles) del RGPD o del artículo 23 del RPDUE, independientemente de los fines del tratamiento. A este respecto, los sistemas de IA deben ofrecer desde el principio otros derechos de las personas interesadas relacionados con el derecho de supresión, el derecho de rectificación con arreglo a la legislación sobre protección de datos, cualquiera que sea el enfoque de IA elegido o la arquitectura técnica.

59. El uso de datos personales para el aprendizaje de sistemas de IA puede conducir a la generación de patrones de toma de decisiones sesgados en el núcleo del sistema de IA. Así pues, deberán exigirse diversas salvaguardias y, en particular, una vigilancia humana cualificada en tales procesos para garantizar el respeto y la garantía de los derechos de los interesados, así como para evitar cualquier efecto negativo para las personas. Las autoridades competentes también deberán poder proponer directrices para evaluar los sesgos en los sistemas de IA y ayudar al ejercicio de la vigilancia humana.

60. Siempre deberá informarse a las personas interesadas, cuando sus datos se utilicen para la formación o predicción en materia de IA, de la base jurídica de dicho tratamiento, una explicación general de la lógica (procedimiento) y el alcance del sistema de IA. A este respecto, en esos casos deberá garantizarse siempre el derecho de las personas físicas a restringir el

tratamiento (artículo 18 del RGPD y artículo 20 del RPDUE), así como a la supresión o el borrado de datos (artículo 16 del RGPD y artículo 19 del RPDUE). Además, la persona responsable del tratamiento deberá tener la obligación explícita de informar al interesado de los plazos aplicables para formular objeciones, limitaciones, supresión de datos, etc. El sistema de IA debe ser capaz de cumplir todos los requisitos de protección de datos mediante medidas técnicas y organizativas adecuadas. Un derecho a la explicación ofrecerá una mayor transparencia.

3.2 Tratamiento ulterior y del espacio de pruebas (artículos 53 y 54 de la propuesta)

61. Dentro de los límites legales y morales existentes, es importante promover la innovación europea a través de instrumentos como un espacio de pruebas. Dicho espacio permite ofrecer las salvaguardias necesarias para generar confianza en los sistemas de IA. En entornos complejos, puede resultar difícil para los profesionales de la IA ponderar adecuadamente todos los intereses. Especialmente en el caso de las pequeñas y medianas empresas con recursos limitados, operar en un espacio controlado de pruebas puede aportar información más rápida y, por tanto, fomentar la innovación.

62. El artículo 53, apartado 3, de la Propuesta establece que el espacio de pruebas no afecta a las facultades de supervisión y correctoras. Si esta aclaración es útil, también es necesario elaborar directrices u orientaciones sobre cómo lograr un buen equilibrio entre ser una autoridad de supervisión, por una parte, y ofrecer orientaciones detalladas a través de un espacio de pruebas, por otra.

63. El artículo 53, sección 6, describe que las modalidades y condiciones de funcionamiento de los espacios de pruebas se determinarán en actos de ejecución. Es importante que se elaboren directrices específicas para garantizar la coherencia y el apoyo en el establecimiento y funcionamiento de los espacios de pruebas. Sin embargo, los actos de ejecución vinculantes podrían limitar la capacidad de cada Estado miembro para personalizar el espacio de pruebas en función de sus necesidades y prácticas locales. Así pues, el CEPD y el SEPD recomiendan que el CEIA proporcione directrices para los espacios de pruebas.

64. El artículo 54 de la propuesta aspira a proporcionar una base jurídica para el tratamiento ulterior de datos personales para desarrollar determinados sistemas de IA en aras del interés público en el espacio controlado de pruebas para la IA. Sigue sin estar clara la relación entre el artículo 54, apartado 1, de la propuesta y el artículo 54, apartado 2, y el considerando 41 de la propuesta y, por tanto, también con la legislación vigente de la UE en materia de protección de datos. Sin embargo, el RGPD y el RPDUE ya disponen de una base establecida para el «tratamiento ulterior». Especialmente en los casos en que sea de interés público permitir un tratamiento ulterior, el equilibrio entre los intereses del responsable del tratamiento y los intereses del interesado no tiene por qué obstaculizar la innovación. El artículo 54 de la propuesta no aborda actualmente dos cuestiones importantes: i) en qué circunstancias, utilizando qué criterios (adicionales), se sopesan los intereses de los interesados, y ii) si estos sistemas de IA solo se utilizarán dentro del espacio de pruebas. El CEPD y el SEPD acogen con satisfacción el requisito de legislación de la Unión o de los Estados miembros en el tratamiento de datos

personales recogidos en el marco del sistema LED en un espacio de pruebas, pero recomiendan que se especifique más en detalle lo que aquí se prevé, de manera que se ajuste al RGPD y al RPDUE, principalmente aclarando que la base jurídica de dichos espacios de pruebas deberá cumplir los requisitos establecidos en el artículo 23, apartado 2, del RGPD y en el artículo 25 del RPDUE, y precisa que todo uso del espacio de pruebas debe someterse a una evaluación exhaustiva. Esto también se aplica a la lista completa de condiciones del artículo 54, apartado 1, letras b) a j).

65. Algunas consideraciones adicionales relativas a la reutilización de datos en el artículo 54 de la propuesta indican que la explotación de un espacio de pruebas requiere un uso intensivo de recursos y, por lo tanto, es realista estimar que solo un pequeño número de empresas tendría la oportunidad de participar. La participación en el espacio de pruebas podría constituir una ventaja competitiva. Permitir la reutilización de los datos requeriría un examen minucioso de cómo seleccionar a los participantes para asegurarse de que están incluidos en el ámbito de aplicación y evitar un trato injusto. El CEPD y el SEPD temen que permitir la reutilización de datos en el marco del espacio de pruebas se aparte del enfoque de rendición de cuentas del RGPD, en el que la responsabilidad recae en el responsable del tratamiento de datos y no en la autoridad competente.

66. Además, el CEPD y el SEPD consideran que, habida cuenta de los objetivos del espacio de pruebas, que consisten en desarrollar, probar y validar sistemas de IA, los espacios de pruebas no pueden entrar en el ámbito de aplicación de la LED. Mientras que la LED prevé la reutilización de datos para la investigación científica, los datos tratados para ese fin secundario estarán sujetos al RGPD o al RPDUE y no al sistema LED.

67. No está claro qué abarcará un espacio controlado de pruebas. Se plantea la cuestión de si el espacio controlado de pruebas propuesto incluye una infraestructura informática en cada Estado miembro con fundamentos jurídicos adicionales para un tratamiento posterior, o si simplemente organiza el acceso a asesoramiento y orientación en materia de regulación. El CEPD y el SEPD instan al legislador a aclarar este concepto en la propuesta y a indicar claramente en ella que el espacio controlado de pruebas no implica la obligación de que las autoridades competentes proporcionen su infraestructura técnica. En cualquier caso, deberán ponerse a disposición de las autoridades competentes recursos financieros y humanos necesarios para dicha aclaración.

68. Por último, el CEPD y el SEPD desean hacer hincapié en el desarrollo de sistemas transfronterizos de IA que estarán a disposición del mercado único digital europeo en su conjunto. En el caso de estos sistemas de IA, el espacio controlado de pruebas como herramienta para la innovación no deberá convertirse en un obstáculo para el desarrollo transfronterizo. Por consiguiente, el CEPD y el SEPD recomiendan un enfoque transfronterizo coordinado que siga estando suficientemente disponible a nivel nacional para todas las pymes y ofrezca un marco común en toda Europa sin ser demasiado restrictivo. Debe alcanzarse un equilibrio entre la coordinación europea y los procedimientos nacionales a fin de evitar una aplicación contradictoria del futuro Reglamento sobre la IA, que obstaculizaría la innovación a escala de la UE.

3.3 Transparencia

69. El CEPD y el SEPD acogen con satisfacción que los sistemas de IA de alto riesgo se registren en una base de datos pública (contemplada en los artículos 51 y 60 de la propuesta). Esta base de datos deberá aprovecharse como una oportunidad para proporcionar información al público en general sobre el ámbito de aplicación del sistema de IA y sobre los defectos e incidentes conocidos que puedan comprometer su funcionamiento y las soluciones adoptadas por los proveedores para abordarlos y remediarlos.

70. Un principio democrático fundamental es el uso de controles y equilibrios. Por lo tanto, el hecho de que la obligación de transparencia no se aplique a los sistemas de IA utilizados para detectar, prevenir, investigar o enjuiciar infracciones penales es demasiado amplio como para considerarse una excepción. Es necesario distinguir entre los sistemas de IA que se utilizan para detectar o prevenir y los sistemas de IA destinados a investigar o colaborar en el enjuiciamiento de infracciones penales. Las salvaguardias para la prevención y detección tienen que ser más fuertes debido a la presunción de inocencia. Por otra parte, el CEPD y el SEPD lamentan la ausencia de advertencias precautorias en la propuesta, que puede interpretarse como una luz verde para el uso de sistemas o aplicaciones de IA de alto riesgo o incluso no demostrados.

71. En aquellos casos en los que, por razones de secreto, puede darse poca o ninguna transparencia al público, incluso en el marco de una democracia que funcione correctamente, deberán establecerse salvaguardias y estos sistemas de IA deberán registrarse y proporcionar transparencia a la autoridad de control competente.

72. Garantizar la transparencia de los sistemas de IA es un objetivo muy complicado. El enfoque íntegramente cuantitativo de la toma de decisiones de muchos sistemas de IA, que es intrínsecamente diferente del enfoque humano que se basa principalmente en el razonamiento causal y teórico, puede entrar en conflicto con la necesidad de obtener una explicación comprensible previa de los resultados de las máquinas. El Reglamento deberá promover formas nuevas, más proactivas y oportunas de informar a los usuarios de los sistemas de IA sobre la situación (de toma de decisiones) en que se encuentra el sistema en cualquier momento, proporcionando una alerta temprana de posibles resultados perjudiciales, de modo que las personas cuyos derechos y libertades puedan verse perjudicados por decisiones autónomas de las máquinas puedan reaccionar o corregir la decisión.

3.4 Tratamiento de categorías especiales de datos y datos relativos a infracciones penales

73. El tratamiento de categorías especiales de datos en el ámbito de la aplicación de la ley se rige por las disposiciones del marco de protección de datos de la UE, incluido el sistema LED y su aplicación nacional. La propuesta afirma no proporcionar un fundamento jurídico general para el tratamiento de datos personales, incluidas las categorías especiales de datos personales (véase el considerando 41). Al mismo tiempo, el artículo 10, apartado 5, de la propuesta dice lo siguiente: «Los proveedores de dichos sistemas podrán tratar las categorías especiales de datos personales». Además, la misma disposición requiere salvaguardias adicionales, también con ejemplos. De este modo, la propuesta parece interferir en la aplicación del RGPD, la LED y el RPDUE. Aunque el

CEPD y el SEPD acogen con satisfacción el intento de establecer garantías adecuadas, es necesario un enfoque regulador más coherente, ya que las disposiciones actuales no parecen lo suficientemente claras como para crear una base jurídica para el tratamiento de las categorías especiales de datos, y deben complementarse con medidas de protección adicionales que aún deben evaluarse. Además, cuando los datos personales se hayan recogido mediante tratamiento dentro del ámbito de aplicación de la LED, deberán tenerse en cuenta las posibles salvaguardias y limitaciones adicionales derivadas de las transposiciones nacionales de la LED.

3.5 Mecanismos de cumplimiento

3.5.1 Certificación

74. Uno de los principales pilares de la propuesta es la certificación. El sistema de certificación descrito en la propuesta se basa en una estructura de entidades (autoridades notificantes/organismos notificados/Comisión) y un mecanismo de evaluación/certificación de la conformidad que abarca los requisitos obligatorios aplicables a los sistemas de IA de alto riesgo, y se basa en normas europeas armonizadas con arreglo al Reglamento (UE) n.º 1025/2012 y en especificaciones comunes que debe establecer la Comisión. Este mecanismo es diferente del sistema de certificación destinado a garantizar el cumplimiento de las normas y principios de protección de datos, descritos en los artículos 42 y 43 del RGPD. Sin embargo, no está claro cómo pueden interactuar los certificados expedidos por los organismos notificados de conformidad con la propuesta con las certificaciones, sellos y marcas de protección de datos previstos en el RGPD, a diferencia de lo que se prevé para otros tipos de certificados (véase el artículo 42, apartado 2, en relación con las certificaciones expedidas en virtud del Reglamento (UE) 2019/881).

75. En la medida en que los sistemas de IA de alto riesgo se basan en el tratamiento de datos personales o tratan datos personales para cumplir su cometido, estos desajustes pueden generar inseguridad jurídica para todos los organismos afectados, ya que pueden dar lugar a situaciones en las que los sistemas de IA, certificados con arreglo a la propuesta y provistos de un marcado CE de conformidad, una vez introducidos en el mercado o puestos en servicio, podrían utilizarse de una forma no acorde con las normas y principios de protección de datos.

76. La propuesta carece de una relación clara con la legislación en materia de protección de datos, así como con la legislación de la UE y de los Estados miembros aplicable a cada uno de los «ámbitos» de los sistemas de IA de alto riesgo enumerados en el anexo III. En particular, la propuesta deberá incluir los principios de minimización y protección de datos desde el diseño como uno de los aspectos que deben tenerse en cuenta antes de obtener el marcado CE, teniendo en cuenta el posible alto nivel de interferencia de los sistemas de IA de alto riesgo con los derechos fundamentales a la privacidad y a la protección de los datos personales, y la necesidad de garantizar un alto nivel de confianza en el sistema de IA. Por consiguiente, el CEPD y el SEPD recomiendan que se modifique la propuesta para aclarar la relación entre los certificados expedidos en virtud de dicho Reglamento y los certificados, sellos y marcas de protección de datos. Por último, las autoridades de protección de datos deberán participar en la elaboración y el establecimiento de normas armonizadas y especificaciones comunes.

77. En relación con el artículo 43 de la propuesta, relativo a la evaluación de la conformidad, la excepción al procedimiento de evaluación de la conformidad establecida en el artículo 47 parece muy amplia e incluye demasiadas excepciones, como las razones excepcionales de seguridad pública o protección de la vida y la salud de las personas, protección del medio ambiente y protección de activos industriales e infraestructuras clave. Proponemos al legislador que los reduzca.

3.5.2 Códigos de conducta

78. De conformidad con el artículo 69 de la propuesta, la Comisión y los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta destinados a promover la aplicación voluntaria, por parte de los proveedores de sistemas de IA que no son de alto riesgo, de los requisitos aplicables a los sistemas de IA de alto riesgo, así como requisitos adicionales. En consonancia con el considerando 78 del RGPD, el CEPD y el SEPD recomiendan identificar y definir sinergias entre estos instrumentos y los códigos de conducta previstos en el RGPD que apoyan el cumplimiento de la protección de datos. En este contexto, es importante aclarar si la protección de los datos personales debe considerarse entre los «requisitos adicionales» que pueden cumplir los códigos de conducta a que se refiere el artículo 69, apartado 2. También es pertinente garantizar que las «especificaciones y soluciones técnicas», abordadas por los códigos de conducta a que se refiere el artículo 69, apartado 1, diseñadas para fomentar el cumplimiento de los requisitos del proyecto de Reglamento sobre la IA, no entren en conflicto con las normas y principios del RGPD y del RPDUE. De este modo, la adhesión a estas herramientas por parte de los proveedores de sistemas de IA que no son de alto riesgo, en la medida en que dichos sistemas se basan en el tratamiento de datos personales o tratan datos personales para cumplir su cometido, representaría un valor añadido, ya que esto garantizará que las personas responsables y encargadas del tratamiento puedan cumplir sus obligaciones en materia de protección de datos en el uso de dichos sistemas.

79. Al mismo tiempo, el marco jurídico para una IA fiable se complementaría con la integración de los códigos de conducta, con el fin de fomentar la confianza en el uso de esta tecnología de manera segura y conforme con la legislación, incluido el respeto de los derechos fundamentales. No obstante, el diseño de estos instrumentos deberá reforzarse previendo mecanismos destinados a verificar que dichos códigos ofrecen «especificaciones y soluciones técnicas» eficaces y establecer «objetivos claros e indicadores clave de resultados para medir la consecución de dichos objetivos» como parte integrante de los códigos en cuestión. Además, la ausencia de referencias a los mecanismos de control (obligatorios) de los códigos de conducta destinados a verificar que los proveedores de sistemas de IA que no son de alto riesgo cumplen sus disposiciones, así como la posibilidad de que los proveedores individuales elaboren (y apliquen ellos mismos) dichos códigos (véase la sección 5.2.7 de la exposición de motivos) pueden debilitar aún más la eficacia y la aplicabilidad de estos instrumentos.

80. Por último, el CEPD y el SEPD solicitan aclaraciones sobre los tipos de iniciativas que la Comisión puede formular, de conformidad con el considerando 81 de la propuesta, «encaminadas a facilitar la reducción de las barreras técnicas que obstaculizan el intercambio transfronterizo de datos para el desarrollo de IA».

4 CONCLUSIÓN

81. Aunque el CEPD y el SEPD acogen con satisfacción la propuesta de la Comisión y consideran que dicho Reglamento es necesario para garantizar los derechos fundamentales de la ciudadanía de la UE y de la población residente, consideran que la propuesta debe adaptarse en varias cuestiones, a fin de garantizar su aplicabilidad y eficiencia.

82. Dada la complejidad de la propuesta, así como de las cuestiones que pretende abordar, queda mucho trabajo por hacer hasta que la propuesta pueda dar lugar a un marco jurídico que funcione correctamente y complemente de manera eficaz el RGPD en lo que respecta a la protección de los derechos humanos fundamentales, fomentando al mismo tiempo la innovación. El CEPD y el SEPD seguirán estando disponibles para ofrecer su apoyo en este recorrido.

Bruselas, 18 de junio de 2021

Por el Comité Europeo de Protección de Datos	Por el Supervisor Europeo de Protección de Datos
La Presidenta	El Supervisor
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI