

Bruselas, 12 de septiembre de 2022  
(OR. en)

12302/22

LIMITE

JUR 579  
TELECOM 364  
COSI 217  
JAI 1155  
ENFOPOL 451

---

---

**Expediente interinstitucional:  
2021/0106(COD)**

---

---

## **DICTAMEN DEL SERVICIO JURÍDICO<sup>1</sup>**

|         |                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| De:     | Servicio Jurídico                                                                                                                                                                                                                                                                                                                                                                                       |
| Asunto: | Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial <ul style="list-style-type: none"><li>– Adecuación de los artículos 114 y 16 del TFUE como bases jurídicas en relación con las disposiciones aplicables a las autoridades encargadas de la aplicación de la ley y a las autoridades judiciales</li></ul> |

### **I. INTRODUCCIÓN**

1. La propuesta de Reglamento establece normas armonizadas para la introducción en el mercado y la puesta en servicio de sistemas de inteligencia artificial («sistemas de IA») en la Unión («propuesta de Reglamento»)<sup>2</sup>.

---

<sup>1</sup> El presente documento contiene asesoramiento jurídico protegido en virtud del artículo 4, apartado 2, del Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión, que el Consejo de la Unión Europea no ha divulgado. El Consejo se reserva todos sus derechos respecto de cualquier publicación no autorizada.

<sup>2</sup> 8115/21.

2. En la reunión del Grupo «Telecomunicaciones y Sociedad de la Información» celebrada el 7 de abril de 2022, el Servicio Jurídico del Consejo intervino sobre la cuestión de la adecuación de la doble base jurídica [artículos 16 y 114 del Tratado de Funcionamiento de la Unión Europea (TFUE)] para la propuesta de Reglamento sobre sistemas de IA. Las explicaciones confirmaron que los artículos 16 y 114 del TFUE son las bases jurídicas correctas para la propuesta y que no resulta adecuado invocar el artículo 87, apartado 2, del TFUE en lugar de su artículo 114. A petición del Grupo, el presente dictamen establece por escrito y desarrolla la intervención del representante del Servicio Jurídico del Consejo en dicha reunión.
3. En el artículo 3, apartado 1, de la propuesta de Reglamento se definen los sistemas de IA. En general, corresponden a determinados tipos de *software*. La propuesta de Reglamento es aplicable tanto a los proveedores que introduzcan sistemas de IA en el mercado como a los proveedores que pongan dichos sistemas en servicio. Además, la propuesta de Reglamento también es aplicable a los usuarios. Puede ser proveedor toda persona física o jurídica o autoridad u organismo público que desarrolle un sistema de IA o para el que se haya desarrollado un sistema de IA con vistas a introducirlo en el mercado o ponerlo en servicio con su propio nombre o marca comercial. Puede ser usuario toda persona física o jurídica, autoridad pública, agencia u organismo de otra índole que utilice un sistema de IA bajo su propia autoridad.

4. De acuerdo con las definiciones del artículo 3, las autoridades encargadas de la aplicación de la ley y las autoridades judiciales podrían ser tanto proveedores como usuarios de un sistema de IA. Los sistemas de IA cuya finalidad prevista, definida por el proveedor, sea la aplicación de la ley o la administración de justicia se consideran de alto riesgo con arreglo al anexo III. En cuanto tales, están sujetos a requisitos esenciales (gestión de riesgos, pruebas, gobernanza de datos, documentación técnica, transparencia, vigilancia humana, precisión, solidez y ciberseguridad) y a obligaciones (por ejemplo, sistemas de gestión de la calidad, documentación técnica, evaluación de la conformidad, medidas correctoras, obligación de información, obligaciones de los importadores y distribuidores), así como a normas y a evaluación de la conformidad. Estas normas armonizadas se inspiran en las que se aplican a la seguridad de los productos en la Directiva 2006/42/CE (máquinas)<sup>3</sup> y el Reglamento 2017/745 (productos sanitarios)<sup>4</sup>.
5. Por su parte, los sistemas de IA que implican el uso de sistemas para la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley entran en la categoría de sistemas de IA prohibidos. No obstante, esta prohibición del uso de sistemas de IA está sujeta a excepciones. De hecho, los Estados miembros pueden autorizar o no el uso de estos sistemas. Si se autorizan, los sistemas se someten a restricciones y salvaguardias detalladas para limitar su uso a lo estrictamente necesario y para preservar el derecho fundamental a la protección de datos de carácter personal. Estas restricciones y salvaguardias están previstas en la propuesta de Reglamento con arreglo al artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) y tienen que ser complementadas por el Derecho interno. El artículo 5, apartado 1, letra d), y apartados 2, 3 y 4, de la propuesta de Reglamento constituye una *lex specialis* de la Directiva 2016/680 (Directiva sobre protección de datos en el ámbito penal), que se adoptó con arreglo al artículo 16, apartado 2, del TFUE.

<sup>3</sup> Directiva 2006/42/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a las máquinas y por la que se modifica la Directiva 95/16/CE (DO L 157 de 9.6.2006, p. 24).

<sup>4</sup> Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo (DO L 117 de 5.5.2017, p. 1).

De conformidad con el artículo 5, apartado 1, letra d), los objetivos de dichos sistemas se limitan a los siguientes:

- i) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos;
- ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista;
- iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos a que hace referencia el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI del Consejo<sup>5</sup>, para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro.

De conformidad con el artículo 5, apartado 3, el uso de estas tecnologías por parte de las autoridades encargadas de la aplicación de la ley debe estar supeditado a la concesión de una autorización previa por parte de una autoridad judicial o administrativa. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar el sistema antes de obtener la autorización correspondiente, que podrá solicitarse durante el uso o después de este.

Con arreglo al artículo 5, apartado 4, los Estados miembros podrán decidir autorizar el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley y definir las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de la autorización previa, así como los delitos correspondientes.

6. Las bases jurídicas de la propuesta de Reglamento son los artículos 16 (protección de datos de carácter personal) y 114 (funcionamiento del mercado interior) del TFUE. Por tanto, se plantea la cuestión de la adecuación de dichas bases jurídicas en relación con las normas armonizadas aplicables a los sistemas de IA facilitados o utilizados por las autoridades encargadas de la aplicación de la ley y las autoridades judiciales.

---

<sup>5</sup> Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (DO L 190 de 18.7.2002, p. 1).

7. El presente dictamen se centra, en primer lugar, en la adecuación del artículo 114 del TFUE como base jurídica, en el contexto particular de las autoridades encargadas de la aplicación de la ley que se mencionan en varias disposiciones de la propuesta de Reglamento, esto es, con respecto a los sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público, y los sistemas de IA de alto riesgo a que hace referencia el punto 6 del anexo III. Por tanto, en el dictamen se examina la cuestión de si el artículo 87, apartado 2, del TFUE (cooperación policial) constituiría una base jurídica más adecuada para abarcar la facilitación y el uso de sistemas de IA por parte de las autoridades encargadas de la aplicación de la ley, en lugar del artículo 114 del TFUE (sección II). Por analogía, la conclusión de la presente nota puede aplicarse a las autoridades judiciales a que hace referencia el anexo III en relación con los sistemas de IA de alto riesgo.
8. La presente nota también examina la adecuación del artículo 16 del TFUE como base jurídica adicional y la aplicación de los Protocolos n.º 21 y n.º 22 en el contexto del uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público por parte de las autoridades encargadas de la aplicación de la ley (sección III).

## II. ADECUACIÓN DEL ARTÍCULO 114 DEL TFUE COMO BASE JURÍDICA

9. Según jurisprudencia reiterada, la base jurídica de un acto de la Unión no depende de la convicción de una institución respecto al fin perseguido, sino que debe determinarse con arreglo a criterios objetivos susceptibles de control jurisdiccional, entre los que figuran, en especial, el objetivo y el contenido del acto. Si el examen de un acto muestra que este persigue un doble objetivo o que tiene un componente doble, y si uno de dichos objetivos o componentes puede calificarse de principal o preponderante, mientras que el otro solo es accesorio, dicho acto debe fundarse en una sola base jurídica, a saber, aquella que exige el objetivo o el componente principal o preponderante. Únicamente con carácter excepcional, si se establece que el acto persigue a la vez varios objetivos relacionados de modo indisoluble, sin que uno de ellos sea secundario e indirecto respecto del otro, dicho acto podrá fundarse en las distintas bases jurídicas correspondientes, salvo que los procedimientos previstos por estas bases jurídicas sean incompatibles entre sí. Conviene señalar, asimismo, que la primera frase del artículo 114, apartado 1, del TFUE precisa que las disposiciones de dicho artículo se aplican «[s]alvo que los Tratados dispongan otra cosa». En consecuencia, la invocación de dicho artículo solo está justificada si no existe una disposición más específica que pueda constituir la base jurídica para la adopción del acto de que se trate<sup>6</sup>. Cuando existe en el Tratado una disposición más específica que puede constituir la base jurídica del acto en cuestión, este debe fundarse en esa disposición<sup>7</sup>.

---

<sup>6</sup> Dictamen del Servicio Jurídico del Consejo de 17 de mayo de 2016, 9007/16, apartado 6.

<sup>7</sup> Sentencia de 29 de abril de 2004, Comisión/Consejo, C- 338/01, EU:C:2004:253, apartado 60.

## A. OBJETIVO DE LA PROPUESTA DE REGLAMENTO

10. La propuesta de Reglamento armoniza la introducción en el mercado, la puesta en servicio y la utilización de un determinado tipo de *software* (sistemas de IA). El hecho de que las autoridades públicas y los operadores privados puedan ser proveedores o usuarios de estos sistemas de IA no es incompatible *per se* con el uso del artículo 114 del TFUE como base jurídica<sup>8</sup>.
11. Además, el hecho de que entre los proveedores o usuarios de dichos sistemas de IA pudiera haber autoridades encargadas de la aplicación de la ley o quienes actúen en su nombre no basta para justificar la utilización del artículo 87 del TFUE como base jurídica. Para determinar si ello es necesario hay que analizar el objetivo y el contenido de la propuesta de Reglamento.
12. La propuesta de Reglamento tiene por objeto, en general, también con respecto a los sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público, y a los sistemas de IA de alto riesgo, garantizar un nivel elevado y coherente de protección en toda la Unión y evitar que las divergencias obstaculicen la libre circulación en el mercado interior de los sistemas de IA y los productos y servicios conexos. Establece obligaciones uniformes para todos los operadores y garantiza la protección uniforme de los fines imperiosos de interés general y de los derechos de las personas en todo el mercado interior (considerando 2). Más concretamente, la propuesta de Reglamento establece normas que regulan la introducción en el mercado y la puesta en servicio de determinados sistemas de IA, lo que garantizará el buen funcionamiento del mercado interior y permitirá que dichos sistemas se beneficien del principio de la libre circulación de bienes y servicios (considerando 5). En general, la propuesta pretende establecer una IA de confianza desde el diseño, aplicable de forma generalizada, con un conjunto completo de normas aplicables al desarrollo, la comercialización y el uso de productos, servicios y sistemas basados en la IA. Dado que la IA ya se ha introducido en un gran número de servicios y productos y seguirá haciéndolo en el futuro, la propuesta sigue una lógica de mercado interior al establecer un «marco de seguridad de los productos» construido en torno a un conjunto de cuatro categorías de riesgo. Impone requisitos para la entrada en el mercado y la certificación de los sistemas de IA de alto riesgo mediante un procedimiento obligatorio de marcado CE.

---

<sup>8</sup> Véase el dictamen jurídico del Servicio Jurídico del Consejo (ST 11395/14, apartados 39 a 41) y precedentes como la Directiva (UE) 2016/2102, las Directivas 2014/24/UE, 2014/25/UE y 2014/23/UE.

13. Ninguno de los objetivos declarados de la propuesta de Reglamento se refiere a garantizar objetivos de seguridad pública. Aunque los objetivos de seguridad pública deban cumplirse indirectamente a través del proceso de armonización de la introducción en el mercado, la puesta en servicio y el uso de sistemas de IA por parte de las autoridades encargadas de la aplicación de la ley, el Tribunal<sup>9</sup>, interpretando el artículo 87, apartado 2, del TFUE a la luz del artículo 67 del TFUE, resolvió que, para que un acto de la Unión, habida cuenta de su objetivo y su contenido, se base en el primer artículo, debe estar directamente relacionado con los objetivos establecidos en el artículo 67 del TFUE (es decir, en este caso, la prevención de la delincuencia y la cooperación policial). Esta interpretación queda excluida en el contexto de la propuesta de Reglamento, ya que las únicas normas armonizadas sobre el uso de dichos sistemas por parte de las autoridades encargadas de la aplicación de la ley son: 1) normas similares a las normas de seguridad de los productos que se aplican de manera uniforme a todos los proveedores y usuarios en relación con la introducción en el mercado, la puesta en servicio o el uso de sistemas de IA, o 2) normas sobre la protección de datos de carácter personal para las que se añadió el artículo 16 del TFUE como base jurídica (véase la parte III del presente documento).
14. En otro asunto<sup>10</sup>, aunque el objetivo de la modificación de la Directiva sobre armas de fuego consistía en garantizar un nivel más elevado de seguridad pública en relación con la amenaza terrorista y otras formas de delincuencia, el Tribunal consideró que la armonización de los aspectos relativos a la seguridad de las mercancías es uno de los elementos esenciales para garantizar el buen funcionamiento del mercado interior, puesto que normativas dispares en esta materia pueden crear obstáculos a los intercambios comerciales<sup>11</sup>.

---

<sup>9</sup> Sentencia de 6 de mayo de 2014, Comisión Europea/Parlamento Europeo, Consejo de la Unión Europea, C- 43/12, ECLI:EU:C:2014:298.

<sup>10</sup> Sentencia de 3 de diciembre de 2019, República Checa/Parlamento Europeo, C-482/17, EU:C:2019:1035.

<sup>11</sup> *Ibid.*, apartado 57: «Pues bien, al consistir la particularidad de las armas de fuego, contrariamente a lo que sostiene la República de Polonia, en su peligrosidad no solo para los usuarios, sino también para el gran público, como señaló ya el Tribunal de Justicia en el apartado 54 de la sentencia de 23 de enero de 2018, Buhagiar y otros (C- 267/16, EU:C:2018:26), las consideraciones de seguridad pública resultan, como recuerda el quinto considerando de la Directiva 91/477, indispensables en el marco de una normativa sobre la adquisición y tenencia de estas mercancías». Véase también la sentencia de 23 de enero de 2018, Albert Buhagiar y otros/Minister for Justice, C-267/16, EU:C:2018:26, apartado 54: «A este respecto, es importante observar que, en vista del riesgo para la seguridad de las personas que suponen las armas de fuego, su libre circulación únicamente ha podido alcanzarse mediante una regulación estricta de los requisitos para su transferencia entre Estados miembros, entre los que figura el principio de autorización previa expedida por los Estados miembros afectados por la transferencia de tales mercancías».



15. Los objetivos de la propuesta de Reglamento, en particular el artículo 5, apartado 1, letra d), y apartados 2, 3 y 4, sobre el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, así como las disposiciones relativas a los sistemas de IA de alto riesgo a que hace referencia el punto 6 del anexo III, no están directamente vinculados a un objetivo de seguridad pública. En cambio, la propuesta responde a las principales preocupaciones relacionadas con el modo en que los sistemas de IA afectan a la salud, la seguridad y los derechos fundamentales. Por tanto, las disposiciones pertinentes están directamente relacionadas con el objetivo de garantizar las condiciones de competencia equitativas en la introducción, la puesta en servicio o el uso de sistemas de IA en el mercado interior y de proteger la salud, la seguridad y los derechos fundamentales de los usuarios.
16. En vista de lo anterior, el objetivo principal de la propuesta de Reglamento es mejorar el funcionamiento del mercado interior en el sentido del artículo 114 del TFUE, y los objetivos a que se refiere el artículo 67 del TFUE solo están vinculados de forma indirecta y accesorio a ese objetivo principal.

**B. CONTENIDO DE LA PROPUESTA DE REGLAMENTO**

17. La propuesta de Reglamento contiene básicamente normas sobre lo que se necesita para introducir un producto específico (un *software* de IA) en el mercado (o para ponerlo en servicio) de tal manera que se garantice su seguridad y el respeto de los derechos fundamentales. En ella se establece un conjunto completo de normas para el desarrollo, la comercialización y el uso de productos, servicios y sistemas basados en la IA. La propuesta de Reglamento no obliga a las autoridades encargadas de la aplicación de la ley a usar un sistema de IA introducido legalmente en el mercado, ni regula de manera directa el modo en que las autoridades encargadas de la aplicación de la ley deben usar dicho sistema de IA. En cambio, delimita claramente las situaciones en las que el uso previsto se considera de alto riesgo por el mero hecho de que sean las autoridades encargadas de la aplicación de la ley o las autoridades judiciales las que vayan a usar un sistema de IA.

18. Por otro lado, el artículo 29 de la propuesta de Reglamento contiene normas sobre las condiciones de uso de los sistemas de IA de alto riesgo, pero dicha disposición no es específica del sector, tiene un alcance limitado (referido principalmente a las instrucciones de uso del producto) y está vinculada de manera intrínseca a las obligaciones impuestas a los desarrolladores de sistemas de IA en virtud de la propuesta de Reglamento. También proporciona a los Estados miembros cierto margen de maniobra para establecer otras normas sobre el uso de tales sistemas de IA de alto riesgo. Por lo que respecta a los sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público utilizados con fines de aplicación de la ley (artículo 5), la propuesta de Reglamento regula parcialmente el uso de dichos sistemas desde la perspectiva de la protección de datos con arreglo al artículo 16 del TFUE (véase la parte III del presente documento).
19. Además, solo los Estados miembros pueden optar por autorizar total o parcialmente el uso de dichos sistemas de identificación biométrica remota «en tiempo real». Las condiciones específicas para tal uso deben establecerse en el Derecho interno, pero deben respetar los criterios generales y las salvaguardias establecidos en el Reglamento: autorización judicial o administrativa previa, solicitud, concesión y ejercicio de la autorización previa, así como la indicación de los delitos en relación con los cuales pueden utilizarse dichos sistemas.

20. Los sistemas de IA son un tipo particular de *software*. Por tanto, las normas armonizadas que se aplican a la introducción en el mercado o la puesta en servicio y el uso de sistemas de IA son normas armonizadas similares a las normas de seguridad de los productos. Se aplican de manera uniforme sin distinguir entre usuarios públicos y privados. De acuerdo con los considerandos pertinentes de la propuesta de Reglamento, debe garantizarse un nivel elevado y coherente de protección en toda la Unión. Al mismo tiempo, deben evitarse las divergencias que obstaculizan la libre circulación en el mercado interior de los sistemas de IA y los productos y servicios conexos. Esto se lograría estableciendo obligaciones uniformes para todos los operadores y garantizando la protección uniforme de los fines imperiosos de interés general y de los derechos de las personas en todo el mercado interior con arreglo al artículo 114 del TFUE<sup>12</sup>.
21. La propuesta de Reglamento contiene varias referencias a la aplicación de la ley, la gestión del control fronterizo y la administración de justicia en el anexo III, relativo a los sistemas de IA de alto riesgo (puntos 6, 7 y 8, respectivamente). Dichas referencias incluyen una enumeración detallada y exhaustiva correspondiente al artículo 6, apartado 2, además de otros sistemas de alto riesgo en relación con los riesgos para la seguridad de los productos a que se refiere el artículo 6, apartado 1. En efecto, según el artículo 6, apartado 1, algunos sistemas de IA deben considerarse de alto riesgo por definición, debido a la gravedad prevista y a los elevados riesgos que plantean para los derechos fundamentales, la salud y la seguridad. Otros sistemas considerados de alto riesgo y enumerados en el anexo III son la educación, la gestión de infraestructuras esenciales (críticas), el empleo, la identificación y categorización biométricas, así como el acceso a servicios públicos y privados esenciales.

---

<sup>12</sup> Por este motivo, se necesita un marco jurídico de la Unión que defina unas normas armonizadas en materia de inteligencia artificial orientadas a impulsar el desarrollo, la utilización y la adopción en el mercado interior de la inteligencia artificial y que, al mismo tiempo, ofrezca un nivel elevado de protección de los intereses públicos, como la salud y la seguridad, y de los derechos fundamentales reconocidos y protegidos por el Derecho de la Unión. Para alcanzar dicho objetivo, conviene establecer normas que regulen la introducción en el mercado y la puesta en servicio de determinados sistemas de IA, lo que garantizará el buen funcionamiento del mercado interior y permitirá que dichos sistemas se beneficien del principio de la libre circulación de bienes y servicios (véanse los considerandos 2 y 5 de la propuesta).

22. Sin embargo, estas normas sobre sistemas de IA de alto riesgo no establecen si las autoridades encargadas de la aplicación de la ley y las autoridades judiciales (o las de los otros ámbitos señalados) deben o no utilizar esos sistemas. La propuesta de Reglamento producirá sus efectos solo de manera indirecta en el desarrollo efectivo de los sistemas de IA que pueden utilizar las autoridades encargadas de la aplicación de la ley y las autoridades judiciales, y en los sistemas de IA que se utilicen actualmente y en el futuro. Así, las normas se refieren a los sistemas de IA que estén «*destinados a ser utilizados*» por dichas autoridades (véanse, por ejemplo, el artículo 3, apartado 12, el artículo 8, apartado 2, y el anexo III). La consecuencia de clasificar un determinado sistema de IA como de alto riesgo es la aplicación de un conjunto específico de normas sobre gestión de riesgos, gobernanza de datos y especificaciones técnicas. Los usuarios de estos sistemas de IA de alto riesgo deben respetar las instrucciones de uso, llevar registros y efectuar evaluaciones de impacto sobre la protección de datos.
23. Además, en el Derecho de la Unión o nacional pueden establecerse obligaciones de los usuarios distintas de las relativas a las instrucciones de uso, sin perjuicio de la discrecionalidad de los usuarios para organizar sus recursos y actividades con el fin de aplicar las medidas de vigilancia humana que indique el proveedor (artículo 29, apartado 2, de la propuesta de Reglamento). Estas normas prevén otras garantías de derechos fundamentales para los sistemas de IA de alto riesgo.

24. En vista de lo anterior, cabe destacar que la propuesta de Reglamento no contiene normas que tengan por objeto permitir o impedir que las autoridades encargadas de la aplicación de la ley usen un sistema de IA de alto riesgo introducido en el mercado. Por efecto de las normas propuestas, se aplicará una etiqueta distinta (alto riesgo) a un sistema de IA desarrollado o utilizado por las autoridades encargadas de la aplicación de la ley debido a su uso previsto. Este uso se regirá por el Derecho interno y, en cierta medida, lo decidirán las propias autoridades encargadas de la aplicación de la ley. De hecho, la propuesta de Reglamento establece unas condiciones mínimas de uso en el artículo 29 (que se limita a las instrucciones de uso) para los sistemas de IA de alto riesgo, incluidos los enumerados en los puntos 6, 7 y 8 del anexo III, que se complementarán con el Derecho interno. Así pues, en consonancia con la jurisprudencia del Tribunal, debe distinguirse entre, por un lado, el objetivo previsto de la propuesta de Reglamento, el cual no consiste en regular el uso de sistemas de IA por parte de las autoridades encargadas de la aplicación de la ley, y, por otro lado, los efectos que la propuesta puede producir de manera indirecta<sup>13</sup>, los cuales son irrelevantes a efectos de analizar la adecuación de la base jurídica.
25. Los puntos 6, 7 y 8 (relativos a la aplicación de la ley, a la migración y a la administración de justicia, respectivamente) no son preponderantes entre los sistemas de IA de alto riesgo. De hecho, con arreglo a la propuesta de Reglamento, un sistema de IA de alto riesgo no tiene por qué figurar necesariamente en el anexo III. Es más, la mayoría de los sistemas de alto riesgo son los enumerados de forma genérica en el artículo 6, apartado 1, letras a) y b), de la propuesta de Reglamento (en relación con la seguridad de los productos). Otros sistemas de IA de alto riesgo se enumeran en el anexo III, en el cual figuran los puntos 1 (identificación biométrica), 2 (infraestructuras esenciales), 3 (educación y formación profesional) y 4 (empleo, gestión de los trabajadores y acceso al autoempleo), que se refieren a ámbitos distintos de Justicia y Asuntos de Interior («JAI»). Todos los usuarios de estos sistemas de IA de alto riesgo están sujetos a un régimen uniforme establecido no en función de su condición específica (por ejemplo, si el usuario es un operador económico o una autoridad pública), sino desde la perspectiva de la protección de la salud, la seguridad y los derechos fundamentales.

---

<sup>13</sup> Véanse la sentencia del Tribunal de Justicia de 21 de junio de 2018, República de Polonia/Parlamento Europeo, Consejo de la Unión Europea, C-5/16, EU:C:2018:483, apartados 63 a 68, y la sentencia del Tribunal de Justicia de 22 de junio de 2022, Leistritz AG/LH, C-534/20, EU:C:2022:495, apartado 28.

26. Así pues, la propuesta de Reglamento contiene normas armonizadas sobre la introducción en el mercado, la puesta en servicio y el uso de sistemas de IA, tanto si son utilizados por operadores privados como por autoridades públicas, que abarcan, de manera accesoria<sup>14</sup>, las autoridades encargadas de la aplicación de la ley y las autoridades judiciales.
27. Dejando de lado el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, que está sujeto a normas específicas sobre el tratamiento de datos personales (véase la parte III del presente documento), la propuesta de Reglamento no contiene normas armonizadas sobre el uso de sistemas de IA de alto riesgo. Como se explica en los apartados 18 y 19, la referencia al uso de sistemas de IA de alto riesgo está relacionada fundamentalmente con las instrucciones de uso del producto (artículo 29) y vinculada a las obligaciones impuestas a los desarrolladores. Como se señala en el apartado 22, la decisión de si las autoridades encargadas de la aplicación de la ley o las autoridades judiciales pueden o no utilizar un sistema de IA de alto riesgo que se introduce en el mercado de conformidad con la propuesta de Reglamento corresponde al Derecho interno y a las autoridades nacionales.
28. De lo anterior se infiere que el artículo 87, apartado 2, del TFUE, en particular su letra a), no es una base jurídica adecuada para la propuesta de Reglamento. Las normas de la propuesta no promueven ni obstaculizan la recogida, el almacenamiento, el tratamiento, el análisis y el intercambio de información pertinente. Simplemente, cuando tales actividades sean realizadas por las autoridades encargadas de la aplicación de la ley, será necesario respetar una serie de condiciones no específicas y armonizadas para salvaguardar los derechos de los usuarios. Asimismo, los objetivos declarados de la propuesta de Reglamento no abarcan el desarrollo de técnicas de investigación comunes. Los requisitos propuestos relativos al uso de sistemas de IA de alto riesgo no son específicos del ámbito de Justicia y Asuntos de Interior y no se refieren a la cooperación policial *stricto sensu* tal como se define en el TFUE.

---

<sup>14</sup> Véase el dictamen del Tribunal de Justicia sobre el Convenio de Estambul, A-1/19, EU:C:2021:198, en particular los apartados 298 y 301.

29. Con respecto a lo dispuesto en el artículo 5, apartado 4, de la propuesta de Reglamento, los Estados miembros aún pueden optar por autorizar el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley. Cuando así lo decidan, los Estados miembros tendrán la obligación de establecer las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de la autorización previa, así como los delitos correspondientes para cuya investigación o enjuiciamiento se autoriza el uso<sup>15</sup>. Con arreglo a las conclusiones de los debates celebrados en el Consejo, estas normas propuestas no supondrían la concesión de nuevas competencias a las respectivas autoridades nacionales. Por el contrario, se delimita el uso de los mecanismos existentes o posibles en el futuro con el fin de garantizar la protección del derecho a la privacidad y a la protección de los datos personales.
30. En vista de lo anterior, el artículo 114 del TFUE constituye la única base jurídica adecuada para las normas armonizadas sobre los sistemas de IA de alto riesgo, entre ellos los utilizados por las autoridades encargadas de la aplicación de la ley y las autoridades judiciales, y ninguna base jurídica del ámbito de Justicia y Asuntos de Interior prevista en el título V de la tercera parte del TFUE, como el artículo 87 del TFUE con respecto a dichas normas armonizadas, está justificada ni resulta adecuada.

---

<sup>15</sup> Cabe destacar que el artículo 5, apartado 4, de la propuesta presenta algunas características similares al artículo 15, apartado 1, de la Directiva 2002/58 sobre la privacidad y las comunicaciones electrónicas. En particular, prevé la posibilidad de que los Estados miembros establezcan excepciones a determinadas prohibiciones establecidas en el Derecho de la Unión. Según jurisprudencia reiterada, las disposiciones nacionales que pretendan establecer excepciones a dichas prohibiciones entrarán necesariamente en el ámbito de aplicación del Derecho de la Unión, lo que, a su vez, hará que la Carta les sea aplicable.

### III. ADECUACIÓN DEL ARTÍCULO 16 DEL TFUE COMO BASE JURÍDICA ADICIONAL

31. La propuesta de Reglamento incluye el artículo 16 del TFUE como base jurídica, en relación con el tratamiento de datos personales en el ámbito de la aplicación de la ley; sus considerandos 25 y 26 contienen una referencia al artículo 6 *bis* del Protocolo n.º 21 y al artículo 2 *bis* del Protocolo n.º 22 sobre el tratamiento de datos personales en el ámbito de la prevención de la delincuencia. En opinión de la Comisión, el artículo 16 del TFUE está destinado a servir exclusivamente de base jurídica para las disposiciones que restringen el tratamiento de datos personales biométricos de forma complementaria a la Directiva 2016/680 (Directiva sobre protección de datos en el ámbito penal). El artículo 5, apartado 1, letra d), se formula como una prohibición de principio, a la que se aplica un conjunto de tres excepciones. En concreto, se prohíbe el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, salvo que dicho uso sea estrictamente necesario para: a) realizar búsquedas selectivas de posibles víctimas de un delito, b) prevenir un atentado terrorista o un ataque a la seguridad física o la vida de una persona que se vayan a producir con carácter inminente, c) localizar o identificar o enjuiciar a la persona que ha cometido o se sospecha que ha cometido un delito grave (con una referencia a la orden de detención europea). En el artículo 5, apartados 2, 3 y 4, se imponen otros requisitos a este uso específico de los sistemas de IA por parte de las autoridades encargadas de la aplicación de la ley, en particular una evaluación de la necesidad y la proporcionalidad, una autorización previa (excepto en situaciones de emergencia) y una decisión de los Estados miembros de autorizar o no a nivel nacional el uso específico de las herramientas de IA en dichas situaciones.
32. El artículo 5 es una disposición detallada que regula un uso específico de las herramientas de IA que no solo pretende complementar el marco legislativo de la Unión vigente (la Directiva sobre protección de datos en el ámbito penal, basada a su vez en el artículo 16 del TFUE), sino que también exige un marco de aplicación nacional.



33. En esencia, a pesar de estar redactada en forma de prohibición, la norma específica del artículo 5 puede describirse como una disposición que establece un marco estricto y excepcional para la vigilancia generalizada y «en tiempo real» de personas en espacios abiertos por medio de instrumentos de IA con el fin de identificarlas. La prohibición también va más allá del simple uso de cámaras para grabar, y se refiere al empleo de herramientas de IA para el reconocimiento automático de rasgos humanos en espacios de acceso público (rasgos como el rostro, pero también la marcha, las impresiones dactilares, el ADN, la voz, las pulsaciones de teclas y otras señales biométricas o de comportamiento). También implica la consiguiente captura e identificación de las personas mediante el análisis comparativo o la comprobación de los datos. Además, la norma debe evaluarse teniendo en cuenta que también puede permitirse la identificación «en tiempo real» por usuarios privados en espacios públicos (para actos como, por ejemplo, partidos de fútbol).
34. Otras aclaraciones ofrecidas por la Comisión parecen indicar que, en la actualidad, ningún Estado miembro, o tal vez un número muy limitado de ellos, ha regulado esta cuestión específica, con vistas a permitir que las autoridades encargadas de la aplicación de la ley utilicen herramientas de IA para la detección «en tiempo real» de personas en espacios públicos. Sin embargo, desde un punto de vista práctico, aunque no se han aportado pruebas fehacientes que demuestren la necesidad de modificar las prácticas y las herramientas existentes, parece claro que las futuras técnicas de investigación, los métodos forenses y las normas sobre la obtención de pruebas tendrán que integrar este planteamiento de prohibición o excepciones.
35. Por lo que respecta a la base jurídica, parece que las disposiciones que restringen el tratamiento de datos personales biométricos de forma complementaria (en comparación con la Directiva sobre protección de datos en el ámbito penal) persiguen el objetivo de proteger los datos personales mediante el establecimiento de salvaguardias adecuadas. Dicho objetivo está indisolublemente vinculado al objetivo de las disposiciones que entran en el ámbito del artículo 114 del TFUE, sin que uno sea secundario e indirecto en relación con el otro. La propuesta de Reglamento tiene por objeto establecer un marco general sobre los sistemas de IA adoptando un planteamiento basado en el riesgo. En este contexto, la regulación horizontal de los sistemas de IA puede incluir salvaguardias estrictas aplicables a este sistema específico de IA de detección en «tiempo real». Así pues, este sistema específico de IA que contiene salvaguardias adecuadas de protección de datos personales está indisolublemente vinculado al objetivo general de mejorar el funcionamiento del mercado interior y no es secundario ni indirecto en relación con este último. Por tanto, de conformidad con la jurisprudencia pertinente, la propuesta de Reglamento debe regirse por una doble base (véase el apartado 9 del presente documento).

36. Sin embargo, queda por resolver la cuestión de determinar la base jurídica que debe utilizarse para regular el tratamiento de datos personales para el uso de los sistemas a que se refiere el artículo 5, apartado 1, letra c), a apartado 4, de la propuesta de Reglamento. En efecto, el artículo 87, apartado 2, letra a), del TFUE constituye una base jurídica para las medidas adoptadas por los servicios de aplicación de la ley en relación con la prevención, la detección y la investigación de delitos, en lo que respecta a la recogida, el almacenamiento, el tratamiento, el análisis y el intercambio de información pertinente.
37. Como explicó el abogado general en las conclusiones sobre el acuerdo entre Canadá y la Unión Europea sobre el registro de nombres de los pasajeros (dictamen 1/15), el artículo 16 del TFUE, por una parte, y el artículo 87, apartado 2, letra a), y el artículo 82, apartado 1, letra d), por otra, no pueden mantener relaciones de tipo jerárquico «*lex generalis-lex specialis*»<sup>16</sup>. El artículo 16, apartado 2, del TFUE es la única disposición que se aplica a las normas relativas a la protección de las personas en lo que respecta al tratamiento de datos personales por parte de las autoridades de los Estados miembros encargadas de la aplicación de la ley cuando llevan a cabo actividades de prevención de la delincuencia. El mero hecho de que el artículo 5 se refiera a la lista de delitos graves de la Decisión Marco relativa a la orden de detención europea no modifica esta evaluación: esta remisión no significa que dicha Decisión Marco se aplique como tal<sup>17</sup>. Se trata simplemente de una técnica legislativa para enumerar los delitos graves sin necesidad de crear un anexo Independiente.
38. El caso es que la norma del artículo 5 se establece, no con el fin de delimitar aún más las condiciones de aplicación de esas medidas relacionadas con el ámbito de Justicia y Asuntos de Interior, sino con vistas a garantizar que, en el futuro, cualquier uso de la identificación biométrica «en tiempo real» por parte de los sistemas de IA responda de forma adecuada a los problemas relacionados con los derechos fundamentales, y principalmente a la necesidad de que los datos biométricos se recojan y se traten respetando el derecho a la privacidad y a la protección de los datos personales.

A este respecto, el Reglamento no pretende establecer un nuevo procedimiento obligatorio específico en materia de Justicia y Asuntos de Interior, sino que recurre a medios procesales probados para garantizar el respeto de los derechos fundamentales.

---

<sup>16</sup> Véanse las conclusiones del abogado general P. Mengozzi de 8 de septiembre de 2016, Proyecto de acuerdo entre Canadá y la Unión Europea, dictamen 1/15, EU:C:2016:656, apartados 112 a 120.

<sup>17</sup> Sobre la aplicación de esta lista de delitos graves por parte de los Estados miembros, véase la sentencia del Tribunal de Justicia de 21 de junio de 2022, Ligue des droits humains ASBL/Conseil des ministres, C-817/19, EU:C:2022:65, apartados 150 a 152.

39. Si el artículo 16 del TFUE constituye una base jurídica adicional adecuada, se plantean preguntas en cuanto a la aplicación de los artículos 6 *bis* y 2 *bis* de los Protocolos n.º 21 y n.º 22, respectivamente. Como se explica en los considerandos 25 y 26 de la propuesta, esto significa que, cuando las autoridades encargadas de la aplicación de la ley de Irlanda o de Dinamarca utilicen sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de prevención de la delincuencia, y cuando Irlanda o Dinamarca no estén vinculadas por las normas correspondientes sobre cooperación policial o judicial en materia penal, estos dos Estados miembros no estarán vinculados por el artículo 5, apartado 1, letra d), y apartados 2 y 3, de la propuesta de Reglamento. Este hecho no implica que el artículo 5, apartado 1, letra d), y apartados 2 y 3, contenga normas sobre cooperación policial, como, por ejemplo, normas relativas al intercambio de información entre las autoridades encargadas de la aplicación de la ley. Significa, sencillamente, que las disposiciones del artículo 5, apartado 1, letra d), y apartados 2 y 3, de la propuesta de Reglamento, de forma similar a la Directiva 2016/680 (Directiva sobre protección de datos en el ámbito penal), que es *lex generalis* adoptada con arreglo al artículo 16 del TFUE, regulan el tratamiento de datos personales biométricos en el contexto particular de los sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público para la prevención de la delincuencia, y nada más. La propuesta de la Comisión a este respecto sigue el planteamiento que mantiene el legislador de la Unión para la Directiva sobre protección de datos en el ámbito penal y, en ese sentido, confirma que la invocación del artículo 87, apartado 2, del TFUE en este contexto no está justificada.
40. La adición del artículo 16 del TFUE al artículo 114 del TFUE en este caso está justificada por el hecho de que el artículo 5, apartado 1, letra d), y apartados 2 y 3, prevé los únicos casos de regulación del uso de un sistema de IA ya autorizado que interfiera en el derecho a la protección de datos de carácter personal, que es *lex specialis* con respecto al marco general de protección de datos. Estas normas de protección de datos que constituyen *lex specialis* y que afectan al uso de esos sistemas de IA sensibles no pueden considerarse secundarias o indirectas en relación con la base jurídica vinculada al mercado interior. Por tanto, la adición del artículo 16 del TFUE como base jurídica está suficientemente justificada en la propuesta de Reglamento, y la invocación del artículo 87, apartado 2, letra a), del TFUE no resulta adecuada.

#### IV. CONCLUSIÓN

41. Habida cuenta de lo anterior, el Servicio Jurídico del Consejo opina que:

- a) la invocación de los artículos 16 y 114 del TFUE como bases jurídicas de la propuesta de Reglamento está justificada y resulta adecuada;
- b) la invocación del artículo 87, apartado 2, del TFUE o cualquier otra base jurídica relacionada con el ámbito de Justicia y Asuntos de Interior no está justificada ni resulta adecuada en relación con las normas armonizadas aplicables a los sistemas de IA que pueden facilitar o usar las autoridades encargadas de la aplicación de la ley o las autoridades judiciales.

---