COMISIÓN
EUROPEA

Bruselas, 29.7.2025
C(2025) 5052 final

COMUNICACIÓN DE LA COMISIÓN

Directrices de la Comisión sobre las prácticas de inteligencia artificial prohibidas que se establecen en el Reglamento (UE) 2024/1689 (Reglamento de Inteligencia Artificial)

ÍNDICE

1. ANTECEDENTES Y OBJETIVOS

1) El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial)[1], entró en vigor el 1 de agosto de 2024. El Reglamento de Inteligencia Artificial establece normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de inteligencia artificial (IA) en la Unión[2]. Su objetivo es promover la innovación y la adopción de la IA, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales en la Unión, incluidos la democracia y el Estado de Derecho.

2) El Reglamento de Inteligencia Artificial sigue un enfoque basado en el riesgo; clasifica los sistemas de IA en cuatro categorías de riesgo diferentes:

   i) Riesgo inaceptable: los sistemas de IA que entrañan riesgos inaceptables para los derechos fundamentales y los valores de la Unión están prohibidos en virtud del artículo 5 del Reglamento de Inteligencia Artificial.

   ii) Alto riesgo: los sistemas de IA que plantean un alto riesgo para la salud, la seguridad y los derechos fundamentales están sujetos a una serie de requisitos y obligaciones. Estos sistemas se clasifican como de «alto riesgo» de conformidad con el artículo 6 del Reglamento de Inteligencia Artificial, en relación con los anexos I y III de dicho Reglamento.

   iii) Riesgo en materia de transparencia: los sistemas de IA que presentan un riesgo limitado de transparencia están sujetos a las obligaciones de transparencia contempladas en el artículo 50 del Reglamento de Inteligencia Artificial.

   iv) Riesgo mínimo o nulo: Los sistemas de IA que presentan un riesgo mínimo o nulo no están regulados, pero los proveedores y los responsables del despliegue pueden adherirse a códigos de conducta voluntarios[3].

3) De conformidad con el artículo 96, apartado 1, letra b), del Reglamento de Inteligencia Artificial, la Comisión debe adoptar directrices sobre la ejecución práctica de las prácticas prohibidas contempladas en el artículo 5 de dicho Reglamento. Dichas prohibiciones son aplicables seis meses después de la entrada en vigor del Reglamento de Inteligencia Artificial, es decir, a partir del 2 de febrero de 2025.

4) El objetivo de las presentes directrices es aumentar la claridad jurídica y proporcionar información sobre la interpretación de la Comisión de las prohibiciones contempladas en el artículo 5 del Reglamento de Inteligencia Artificial, con vistas a garantizar su aplicación coherente, eficaz y uniforme. Deben servir de orientación práctica para ayudar a las autoridades competentes en virtud del Reglamento de Inteligencia Artificial en sus actividades de garantía del cumplimiento, así como a los proveedores

[1] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024).

[2] Artículo 1 del Reglamento de Inteligencia Artificial.

[3] Artículo 95 del Reglamento de Inteligencia Artificial.

y responsables del despliegue de sistemas de IA a la hora de garantizar el cumplimiento de sus obligaciones en virtud de dicho Reglamento. Tienen por objeto interpretar las prohibiciones de una manera proporcionada que permita lograr los objetivos del Reglamento de Inteligencia Artificial de proteger los derechos fundamentales y la seguridad, promoviendo al mismo tiempo la innovación y proporcionando seguridad jurídica.

5) Las presentes directrices no son vinculantes. Solo el Tribunal de Justicia de la Unión Europea (en lo sucesivo, el «TJUE») puede ofrecer en última instancia una interpretación autorizada del Reglamento de Inteligencia Artificial.

6) La elaboración de las presentes directrices se basó en las aportaciones de diversas partes interesadas como, por ejemplo, proveedores y responsables del despliegue de sistemas de IA, organizaciones de la sociedad civil, agentes del mundo académico, autoridades públicas, asociaciones empresariales, etc., recogidas durante un amplio proceso de consulta organizado por la Comisión. También se consultó a los Estados miembros que forman parte del Comité Europeo de Inteligencia Artificial y al Parlamento Europeo. Estas directrices se revisarán periódicamente en vista de la experiencia adquirida con la ejecución práctica del artículo 5 del Reglamento de Inteligencia Artificial y la evolución tecnológica y del mercado.

7) La aplicación del artículo 5 del Reglamento de Inteligencia Artificial requerirá una evaluación caso por caso, que tenga debidamente en cuenta la situación específica de cada caso concreto. Por lo tanto, los ejemplos que figuran en las presentes directrices son meramente indicativos y se entienden sin perjuicio de la necesidad de dicha evaluación caso por caso.

2. VISIÓN DE CONJUNTO DE LAS PRÁCTICAS DE IA PROHIBIDAS

8) El artículo 5 del Reglamento de Inteligencia Artificial prohíbe la introducción en el mercado de la UE, la puesta en servicio o la utilización de determinados sistemas de IA para prácticas de manipulación, explotación, control social o vigilancia que, por su propia naturaleza, vulneren los derechos fundamentales y los valores de la Unión. El considerando 28 del Reglamento de Inteligencia Artificial aclara que dichas prácticas son sumamente perjudiciales e incorrectas y deben estar prohibidas, pues van en contra de los valores de la Unión de respeto de la dignidad humana, la libertad, la igualdad, la democracia y el Estado de Derecho y de los derechos fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (en lo sucesivo, la «Carta»), como el derecho a la no discriminación (artículo 21 de la Carta), a la igualdad (artículo 20 de la Carta), a la protección de datos (artículo 8 de la Carta) y a la vida privada y familiar (artículo 7 de la Carta), así como a los derechos del niño (artículo 24 de la Carta). Las prohibiciones establecidas en el artículo 5 del Reglamento de Inteligencia Artificial también tienen por objeto defender el derecho a la libertad de expresión y de información (artículo 11 de la Carta), la libertad de reunión y de asociación (artículo 12 de la Carta), la libertad de pensamiento, de conciencia y de religión (artículo 10 de la Carta), el derecho a la tutela judicial efectiva y a un juez

imparcial (artículo 47 de la Carta) y la presunción de inocencia y el derecho de la defensa (artículo 48 de la Carta).

2.1. Prohibiciones enumeradas en el artículo 5 del Reglamento de Inteligencia Artificial

9) Resumen de las prohibiciones

Disposición	**Prohibición**	**Contenido**
Artículo 5, apartado 1, letra a)	Manipulación perjudicial y engaño	Sistemas de IA que se sirvan de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar el comportamiento, de modo que provoquen o sea razonablemente probable que provoquen perjuicios considerables
Artículo 5, apartado 1, letra b)	Explotación perjudicial de las vulnerabilidades	Sistemas de IA que exploten vulnerabilidades derivadas de la edad, discapacidad o de una situación social o económica específica, con el objetivo o el efecto de alterar el comportamiento, de modo que provoquen o sea razonablemente probable que provoquen perjuicios considerables
Artículo 5, apartado 1, letra c)	Puntuación ciudadana	Sistemas de IA que evalúen o clasifiquen a personas físicas o a colectivos de personas atendiendo al comportamiento social o a características personales o de la personalidad, de forma que la puntuación ciudadana resultante provoque un trato perjudicial o desfavorable cuando los datos procedan de contextos sociales que no guarden relación o cuando dicho trato sea injustificado o desproporcionado con respecto al comportamiento social
Artículo 5, apartado 1, letra d)	Evaluación y predicción individuales de riesgos de delitos [en este texto se entiende el «delito» como «infracción penal»]	Sistemas de IA que valoren o predigan el riesgo de que una persona cometa un delito basándose únicamente en la elaboración de perfiles o en rasgos y características de la personalidad, salvo para apoyar una valoración humana basada en hechos objetivos y verificables directamente relacionados con una actividad delictiva
Artículo 5, apartado 1, letra e)	Extracción no selectiva para desarrollar bases de datos de reconocimiento facial	Sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión
Artículo 5, apartado 1, letra f)	Reconocimiento de emociones	Sistemas de IA que infieran emociones en los lugares de trabajo o en los centros educativos, salvo por motivos médicos o de seguridad
Artículo 5, apartado 1, letra g)	Categorización biométrica	Sistemas de IA que clasifiquen a las personas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas,

		afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual, excepto para el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, también en el ámbito de la garantía del cumplimiento del Derecho
Artículo 5, apartado 1, letra h)	Identificación biométrica remota «en tiempo real»	Sistemas de IA para la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo cuando sea necesario para la búsqueda selectiva de víctimas concretas, la prevención de amenazas específicas (incluidos los atentados terroristas) o la búsqueda de sospechosos de delitos específicos. En el artículo 5, apartados 2 a 7, del Reglamento de Inteligencia Artificial, se describen otros requisitos procedimentales, en particular los relativos a la autorización.

2.2. Base jurídica de las prohibiciones

10) El Reglamento de Inteligencia Artificial se apoya en dos bases jurídicas: el artículo 114 del Tratado de Funcionamiento de la Unión Europea (en lo sucesivo, el «TFUE») (base jurídica del mercado interior) y el artículo 16 del TFUE (base jurídica de la protección de datos). El artículo 16 del TFUE sirve de base jurídica para las normas específicas sobre el tratamiento de datos personales en relación con la prohibición del uso de sistemas para la identificación biométrica remota con fines de garantía del cumplimiento del Derecho, sistemas de categorización biométrica con fines de garantía del cumplimiento del Derecho y evaluaciones individuales de riesgos con fines de garantía del cumplimiento del Derecho[4]. La base jurídica de todas las demás prohibiciones enumeradas en el artículo 5 del Reglamento de Inteligencia Artificial es el artículo 114 del TFUE.

2.3. Ámbito de aplicación material: prácticas relacionadas con la «introducción en el mercado», la «puesta en servicio» o la «utilización» de un sistema de IA

11) Las prácticas prohibidas por el artículo 5 del Reglamento de Inteligencia Artificial se refieren a la introducción en el mercado, la puesta en servicio o la utilización de determinados sistemas de IA[5]. Por lo que se refiere a los sistemas de identificación biométrica remota en tiempo real, la prohibición establecida en el artículo 5, apartado 1,

[4] Considerando 3 del Reglamento de Inteligencia Artificial. En cuanto a las prohibiciones basadas en el artículo 16 del TFUE, existen dos exclusiones voluntarias pertinentes para Irlanda y Dinamarca. Con la discrecionalidad concedida a Irlanda en virtud del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda en el espacio de libertad, seguridad y justicia anejo al Tratado de la Unión Europea (en lo sucesivo, el «TUE») y al TFUE, Irlanda puede decidir no aplicar las normas relativas a la prohibición del uso de la identificación biométrica remota en tiempo real en espacios públicos con fines de garantía del cumplimiento del Derecho, así como las normas de procedimiento vinculadas a dicho artículo (artículo 5, apartados 2 a 6, del Reglamento de Inteligencia Artificial) (véase el considerando 40). Dinamarca se beneficia de acuerdos de exclusión voluntaria al aplicar el Protocolo n.º 22 del TUE y el TFUE y puede decidir no aplicar plenamente las prohibiciones basadas en el artículo 16 del TFUE (véase el considerando 41).

[5] Para las definiciones de estos términos, véase también la comunicación de la Comisión titulada «‘‘Guía azul’’ sobre la aplicación de la normativa europea relativa a los productos, de 2022», 2022/C 247/01, sección 2.

letra h), del Reglamento de Inteligencia Artificial únicamente se aplica a su utilización. En el artículo 3, punto 1, se define lo que constituye un sistema de IA. En las Directrices relativas a la definición de un sistema de IA se ofrece la interpretación que hace la Comisión de dicha definición.

12) De conformidad con el artículo 3, punto 9, del Reglamento de Inteligencia Artificial, la **introducción en el mercado** de un sistema de IA es «la primera comercialización en el mercado de la Unión de un sistema de IA [...]». La «comercialización» se define como el suministro de un sistema «para su distribución o utilización en el mercado de la Unión en el transcurso de una actividad comercial, previo pago o gratuitamente»[6]. La comercialización de un sistema de IA está cubierta con independencia de los medios de suministro, como el acceso al sistema y su servicio a través de una interfaz de programación de aplicaciones (en lo sucesivo, «API»), mediante la nube, descargas directas, copias físicas o integrado en productos físicos.

Por ejemplo: un sistema de identificación biométrica remota desarrollado fuera de la Unión por un proveedor de un tercer país se introduce en el mercado de la Unión por primera vez cuando se ofrece previo pago o gratuitamente en uno o varios Estados miembros. Esta introducción en el mercado puede hacerse facilitando el acceso al sistema en línea a través de una API u otra interfaz de usuario.

13) El artículo 3, punto 11, del Reglamento de Inteligencia Artificial define la **puesta en servicio** como «el suministro de un sistema de IA para su primer uso directamente al responsable del despliegue o para uso propio en la Unión para su finalidad prevista», por lo que comprende tanto el suministro a terceros para su primer uso como al desarrollo y el despliegue internos. La «finalidad prevista» del sistema es «el uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica»[7].

Por ejemplo: un proveedor construye un sistema de identificación biométrica remota fuera de la Unión y lo suministra a una autoridad garante del cumplimiento del Derecho o a una empresa privada establecida en un Estado miembro para utilizarlo por primera vez, poniéndolo así en servicio.

Por ejemplo: una autoridad pública desarrolla un sistema de puntuación interno y lo despliega para predecir el riesgo de fraude de los beneficiarios de prestaciones familiares, poniéndolo así en servicio.

14) Si bien la «**utilización**» de un sistema de IA no se define de manera explícita en el Reglamento de Inteligencia Artificial, debe entenderse de manera amplia para comprender el uso o el despliegue del sistema en cualquier momento de su ciclo de vida tras su introducción en el mercado o su puesta en servicio. Esto también puede abarcar la integración del sistema de IA en los servicios y procesos de la persona o personas

[6] Artículo 3, punto 10, del Reglamento de Inteligencia Artificial.
[7] Artículo 3, punto 12, del Reglamento de Inteligencia Artificial.

que utilicen el sistema de IA, también como parte de sistemas, procesos o infraestructuras más complejos. Si bien los proveedores de sistemas de IA deben tener en cuenta las condiciones de uso que pueden ser razonablemente previsibles antes de introducir sus sistemas de IA en el mercado (uso previsto y uso indebido razonablemente previsible[8]), los responsables del despliegue siguen siendo responsables de tener en cuenta las condiciones legales de uso del sistema[9]. A efectos del artículo 5 del Reglamento de Inteligencia Artificial, debe entenderse que la referencia a la «utilización» comprende cualquier uso indebido de un sistema de IA («razonablemente previsible» o no) que pueda constituir una práctica prohibida[10].

Por ejemplo: la utilización de un sistema de IA por parte de un empleador para inferir las emociones en el lugar de trabajo está prohibida, salvo por motivos médicos o de seguridad [artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial]. La prohibición se aplica a los responsables del despliegue independientemente de que el proveedor (del sistema) haya excluido dicho uso en sus relaciones contractuales con el responsable del despliegue (el empleador), es decir, en las condiciones de uso.

2.4. Ámbito de aplicación personal: agentes responsables

15) El Reglamento de Inteligencia Artificial distingue entre diferentes categorías de operadores en relación con los sistemas de IA: proveedores, responsable del despliegue, importadores, distribuidores y fabricantes de productos. Las presentes directrices se centrarán únicamente en los proveedores y los responsables del despliegue, habida cuenta del ámbito de aplicación de las prácticas prohibidas en el artículo 5 del Reglamento de Inteligencia Artificial.

16) De conformidad con el artículo 3, punto 3, del Reglamento de Inteligencia Artificial, los **proveedores** son personas físicas o jurídicas, autoridades públicas, órganos u organismos que desarrollen o para los que se desarrollen sistemas de IA y los introduzcan en el mercado de la Unión o los pongan en servicio con su propio nombre o marca[11] (véase la sección2.3). Los proveedores establecidos o ubicados fuera de la Unión están sujetos a las disposiciones del Reglamento de Inteligencia Artificial si introducen dichos sistemas en el mercado o los ponen en servicio en la Unión[12] o si los resultados de salida del sistema de IA se utilizan en la Unión[13]. Los proveedores deben

[8] Véase el artículo 3, puntos 12 y 13, del Reglamento de Inteligencia Artificial.

[9] Para las definiciones de estos términos, véase también la comunicación de la Comisión titulada «‘‘Guía azul’’ sobre la aplicación de la normativa europea relativa a los productos, de 2022», 2022/C 247/01, sección 2,8.

[10] Considerando 28 del Reglamento de Inteligencia Artificial.

[11] Artículo 3, puntos 3, 9 y 11, del Reglamento de Inteligencia Artificial. En relación con los sistemas de IA de alto riesgo, el artículo 25 del Reglamento de Inteligencia Artificial establece que 1. Cualquier distribuidor, importador, responsable del despliegue o tercero será considerado proveedor de un sistema de IA de alto riesgo a los efectos del presente Reglamento y estará sujeto a las obligaciones del proveedor previstas en el artículo 16 en cualquiera de las siguientes circunstancias: a) cuando ponga su nombre o marca en un sistema de IA de alto riesgo previamente introducido en el mercado o puesto en servicio, sin perjuicio de los acuerdos contractuales que estipulen que las obligaciones se asignan de otro modo; b) cuando modifique sustancialmente un sistema de IA de alto riesgo que ya haya sido introducido en el mercado o puesto en servicio de tal manera que siga siendo un sistema de IA de alto riesgo con arreglo al artículo 6; c) cuando modifique la finalidad prevista de un sistema de IA, incluido un sistema de IA de uso general, que no haya sido considerado de alto riesgo y ya haya sido introducido en el mercado o puesto en servicio, de tal manera que el sistema de IA de que se trate se convierta en un sistema de IA de alto riesgo de conformidad con el artículo 6.

[12] Artículo 2, apartado 1, letra a), del Reglamento de Inteligencia Artificial.

[13] Artículo 2, apartado 1, letra c), del Reglamento de Inteligencia Artificial.

garantizar que sus sistemas de IA cumplen todos los requisitos pertinentes antes de introducirlos en el mercado o ponerlos en servicio.

> Por ejemplo, un proveedor de un sistema de identificación biométrica remota es el fabricante del sistema que comercializa el sistema en la Unión con su marca. El proveedor de dicho sistema también podría ser una autoridad pública que desarrolle el sistema internamente y lo ponga en servicio para su propio uso.

17) Los **responsables del despliegue** son personas físicas o jurídicas, o autoridades públicas, órganos u organismos que utilicen un sistema de IA bajo su propia autoridad, salvo cuando su uso se enmarque en una actividad personal de carácter no profesional[14]. Tener «autoridad» sobre un sistema de IA significa asumir la responsabilidad de la decisión de desplegar el sistema y de la manera en que se utiliza realmente. Los responsables del despliegue entran en el ámbito de aplicación del Reglamento de Inteligencia Artificial si están establecidos o ubicados en la Unión[15] o, en caso de estar situados en un tercer país, si los resultados de salida del sistema de IA se utilizan en la Unión[16].

18) Cuando el responsable del despliegue de un sistema de IA es una persona jurídica bajo cuya autoridad se utiliza el sistema, es decir, una autoridad garante del cumplimiento del Derecho o una empresa de seguridad privada, no deben considerarse responsables del despliegue los empleados que actúan individualmente en el marco de los procedimientos y bajo el control de dicha persona jurídica. Una persona jurídica también sigue siendo responsable del despliegue si cuenta con la participación de terceros (como contratistas o personal externo) en el funcionamiento del sistema en su nombre y bajo su responsabilidad y control.

19) Los operadores pueden desempeñar más de una función simultáneamente en relación con un sistema de IA. Por ejemplo, si un operador desarrolla su propio sistema de IA y lo utiliza posteriormente, se le considerará tanto proveedor como responsable del despliegue de dicho sistema, aunque también lo utilicen otros responsables del despliegue a quienes se haya proporcionado el sistema previo pago o gratuitamente.

20) Debe cumplirse de forma continua el Reglamento de Inteligencia Artificial en todas las fases del ciclo de vida de la IA; esto requiere una supervisión y actualización continuas de los sistemas de IA introducidos en el mercado o puestos en servicio en la Unión, a fin de garantizar que un sistema de IA siga cumpliendo el Reglamento de Inteligencia Artificial a lo largo de su ciclo de vida y que no dé lugar a una práctica prohibida en virtud del artículo 5 de dicho Reglamento. Para evitar estas prácticas prohibidas, los proveedores y los responsables del despliegue de sistemas de IA tienen diferentes responsabilidades según sus funciones y control sobre el diseño, el desarrollo y el uso real del sistema. Para cada una de las prohibiciones, estas funciones y responsabilidades deben interpretarse de manera proporcionada; debe tenerse en cuenta quién, dentro de la cadena de valor, es el más indicado para adoptar medidas preventivas y de reducción

[14] Artículo 3, punto 4, del Reglamento de Inteligencia Artificial.
[15] Artículo 2, apartado 1, letra b), del Reglamento de Inteligencia Artificial.
[16] Artículo 2, apartado 1, letra c), del Reglamento de Inteligencia Artificial.

de riesgos específicas y garantizar que el desarrollo y el uso de los sistemas de IA sean conformes y estén en consonancia con los objetivos y el enfoque del Reglamento de Inteligencia Artificial.

2.5. Exclusión del ámbito de aplicación del Reglamento de Inteligencia Artificial

21) El artículo 2 del Reglamento de Inteligencia Artificial establece una serie de exclusiones generales del ámbito de aplicación que resultan de utilidad para comprender plenamente la aplicación práctica de las prohibiciones enumeradas en el artículo 5 de dicho Reglamento.

2.5.1. Fines militares, de defensa o de seguridad nacional

22) Según el artículo 2, apartado 3, del Reglamento de Inteligencia Artificial, este no se aplica a los ámbitos que queden fuera del ámbito de aplicación del Derecho de la Unión y, en cualquier caso, no afecta a las competencias de los Estados miembros en materia de seguridad nacional, independientemente del tipo de entidad a la que los Estados miembros hayan encomendado el desempeño de tareas en relación con dichas competencias. El Reglamento de Inteligencia Artificial excluye expresamente de su ámbito de aplicación los sistemas de IA que «se introduzcan en el mercado, se pongan en servicio o se utilicen, con o sin modificaciones, exclusivamente con fines militares, de defensa o de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades». Así pues, la aplicabilidad de esta exclusión depende de los fines o de los usos del sistema de IA, no de las entidades que realicen las actividades con dicho sistema, que pueden ser también los operadores privados a los que los Estados miembros hayan encomendado las tareas relacionadas con esas competencias.

23) Según el Tribunal de Justicia de la Unión Europea, el término «**seguridad nacional**» se refiere al «interés primordial de proteger las funciones esenciales del Estado y los intereses fundamentales de la sociedad e incluye la prevención y la represión de actividades que puedan desestabilizar gravemente las estructuras constitucionales, políticas, económicas o sociales fundamentales de un país, y, en particular, amenazar directamente a la sociedad, a la población o al propio Estado, tales como las actividades terroristas»[17]. La seguridad nacional no comprende, por ejemplo, las actividades relativas a la seguridad vial[18] o la organización o administración de la justicia[19]. Como ha señalado el TJUE, «corresponde a los Estados miembros determinar sus intereses esenciales de seguridad y adoptar las medidas adecuadas para garantizar su seguridad interior y exterior, [...] una medida nacional [adoptada] con el fin de proteger la seguridad nacional no puede dar lugar a la inaplicabilidad del Derecho de la Unión ni dispensar a los Estados miembros de la necesaria observancia de dicho Derecho»[20].

---

17 Sentencia del Tribunal de Justicia de 6 de octubre de 2020, La Quadrature du Net y otros, C-511/18, C-512/18 y C-520/18, ECLI:EU:C:2020:791, apartado 135; sentencia del Tribunal de Justicia de 5 de junio de 2023, Comisión/Polonia, C-204/21, ECLI:EU:C:2023:442, apartado 318, que se refiere al asunto C-439/19, apartado 67, y al asunto C-306/21, apartado 40.

18 Sentencia del Tribunal de Justicia de 22 de junio de 2021, Latvijas Republikas Saeima, C-439/19, ECLI:EU:C:2021:504, apartado 68.

19 Sentencia del Tribunal de Justicia de 5 de junio de 2023, Comisión/Polonia, C-204/21, ECLI:EU:C:2023:442, apartado 319.

20 Sentencia del Tribunal de Justicia de 6 de octubre de 2020, Privacy International, C-623/17, ECLI:EU:C:2020:790, apartado 44.

24) Para que se aplique la exclusión contemplada en el artículo 2, apartado 3, párrafo segundo, del Reglamento de Inteligencia Artificial, el sistema de IA debe introducirse en el mercado, ponerse en servicio o utilizarse exclusivamente con fines militares, de defensa o de seguridad nacional. El considerando 24 del Reglamento de Inteligencia Artificial aclara además la forma en que debe interpretarse el concepto «**exclusivamente**» e indica cuándo un sistema de IA utilizado con tales fines puede, aun así, entrar en el ámbito de aplicación del Reglamento de Inteligencia Artificial.

> Por ejemplo, si un sistema de IA introducido en el mercado, puesto en servicio o utilizado con fines militares, de defensa o de seguridad nacional se utiliza, temporal o permanentemente, con otros fines (por ejemplo, con fines civiles o humanitarios, de garantía del cumplimiento del Derecho o de seguridad pública), dicho sistema entrará en el ámbito de aplicación del Reglamento de Inteligencia Artificial. En tal caso, la entidad que utilice el sistema de IA para los otros fines debe garantizar que dicho sistema cumple lo dispuesto en el Reglamento de Inteligencia Artificial, a menos que el sistema ya lo haga, lo cual debe verificarse antes del uso previsto.

25) Asimismo, el considerando 24 del Reglamento de Inteligencia Artificial aclara que entran en el ámbito de aplicación de dicho Reglamento los sistemas de IA introducidos en el mercado o puestos en servicio para un fin excluido, a saber, militar, de defensa o de seguridad nacional, y para uno o varios fines no excluidos, como fines civiles o de garantía del cumplimiento del Derecho (los denominados sistemas «**de doble uso**»). Los proveedores de dichos sistemas deben garantizar que cumplen los requisitos del Reglamento de Inteligencia Artificial.

> Por ejemplo: si una empresa ofrece un sistema de identificación biométrica remota para diversos fines, como la garantía del cumplimiento del Derecho y la seguridad nacional, dicha empresa es el proveedor de ese sistema de «doble uso» y debe garantizar que cumple los requisitos del Reglamento de Inteligencia Artificial.

26) No obstante, el hecho de que un sistema de IA pueda entrar en el ámbito de aplicación del Reglamento de Inteligencia Artificial no debe afectar a la capacidad de las entidades que llevan a cabo actividades militares, de defensa y de seguridad nacional, independientemente del tipo de entidad que lleve a cabo estas actividades, de utilizar sistemas de IA con fines de seguridad nacional, militares y de defensa[21].

> Por ejemplo, si una agencia nacional de inteligencia encomienda a una agencia de seguridad nacional o a un operador privado que utilice sistemas de identificación biométrica remota en tiempo real con fines de seguridad nacional (como, por ejemplo, recopilar información), dicho uso quedaría excluido del ámbito de aplicación del Reglamento de Inteligencia Artificial.

27) Delimitar claramente la exclusión por motivos de seguridad nacional es especialmente importante cuando los sistemas de IA se introducen en el mercado, se ponen en servicio o se utilizan con fines de garantía del cumplimiento del Derecho que entran en el ámbito

[21] Considerando 24 del Reglamento de Inteligencia Artificial.

de aplicación del Reglamento de Inteligencia Artificial. Esto es pertinente para las prohibiciones relativas a las predicciones y evaluaciones del riesgo de que una persona cometa un delito y al uso de sistemas de identificación biométrica remota en tiempo real con fines de garantía del cumplimiento del Derecho establecidos en el artículo 5, apartado 1, letras d) y h), del Reglamento de Inteligencia Artificial, respectivamente. La policía y otras autoridades garantes del cumplimiento del Derecho son las encargadas de la prevención, la detección, la investigación y el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas[22]. Siempre que los sistemas de IA se utilicen con tales fines, entrarán en el ámbito de aplicación del Reglamento de Inteligencia Artificial.

28) Las actividades de Europol y de otras agencias de seguridad de la Unión, como Frontex, entran en el ámbito de aplicación del Reglamento de Inteligencia Artificial.

2.5.2. Cooperación judicial y de garantía del cumplimiento del Derecho con terceros países

29) De conformidad con el artículo 2, apartado 4, el Reglamento de Inteligencia Artificial no se aplica a las autoridades públicas de terceros países ni a las organizaciones internacionales cuando dichas autoridades u organizaciones utilicen sistemas de IA en el marco de acuerdos o de la cooperación internacionales con fines de garantía del cumplimiento del Derecho y cooperación judicial con la Unión o con uno o varios Estados miembros, siempre que tal tercer país u organización internacional ofrezca garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas. Cuando proceda, dicha exclusión podrá incluir las actividades de entidades privadas a las que el tercer país en cuestión haya encomendado tareas específicas en apoyo de dicha cooperación policial y judicial[23]. Al mismo tiempo, para que se aplique la exclusión, estos marcos de cooperación o acuerdos internacionales deben incluir garantías suficientes con respecto a la protección de los derechos y libertades fundamentales de las personas, que deben ser evaluadas por las autoridades de vigilancia del mercado competentes para la supervisión de los sistemas de IA utilizados en el ámbito de la garantía del cumplimiento del Derecho y la justicia[24]. En el considerando 22 del Reglamento de Inteligencia Artificial se aclara que las autoridades nacionales y las instituciones, órganos y organismos de la Unión que sean destinatarios de dichos resultados de salida y que la utilicen en la Unión siguen siendo responsables de garantizar que su utilización de la información está en consonancia con el Derecho de la Unión. Cuando, en el futuro, dichos acuerdos internacionales se revisen o se celebren otros nuevos, las partes contratantes deben hacer todo lo posible por que dichos acuerdos se ajusten a los requisitos del Reglamento de Inteligencia Artificial.

2.5.3. Investigación y desarrollo

[22] Artículo 3, punto 46, del Reglamento de Inteligencia Artificial.
[23] Véase el considerando 22 del Reglamento de Inteligencia Artificial.
[24] Véanse el considerando 22 y el artículo 74, apartado 8, del Reglamento de Inteligencia Artificial.

30) Según el artículo 2, apartado 8, del Reglamento de Inteligencia Artificial, este no se aplica «a ninguna actividad de investigación, prueba o desarrollo relativa a sistemas de IA o modelos de IA antes de su introducción en el mercado o puesta en servicio». Esta exclusión está en consonancia con la lógica basada en el mercado del Reglamento de Inteligencia Artificial, que se aplica a los sistemas de IA una vez introducidos en el mercado o puestos en servicio.

> Por ejemplo: durante la fase de investigación y desarrollo, los desarrolladores de IA tienen libertad para experimentar y probar nuevas funcionalidades que podrían suponer el uso de técnicas que pueden considerarse manipuladoras y que estén contempladas en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial si se utilizan en aplicaciones orientadas al consumidor. El Reglamento de Inteligencia Artificial permite esa experimentación, ya que reconoce que la investigación y desarrollo en fase inicial es fundamental para perfeccionar las tecnologías de IA y garantizar que cumplen las normas éticas y de seguridad antes de su introducción en el mercado.

31) Tal como se aclara en su considerando 25, el Reglamento de Inteligencia Artificial tiene por objeto apoyar la innovación y reconoce la importancia de la investigación científica para promover las tecnologías de IA y contribuir al progreso científico y a la innovación. Así pues, el artículo 2, apartado 6, del Reglamento de Inteligencia Artificial establece una excepción para «los sistemas o modelos de IA, incluidos sus resultados de salida, desarrollados y puestos en servicio específicamente con la investigación y el desarrollo científicos como única finalidad».

> Por ejemplo: la investigación sobre las respuestas cognitivas y conductuales a los estímulos subliminales o engañosos basados en la IA puede proporcionar información valiosa sobre las interacciones entre el ser humano y la IA, lo que ayudaría a desarrollar aplicaciones de IA más seguras y eficaces en el futuro. A pesar de la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, estas investigaciones están permitidas porque están excluidas del ámbito de aplicación de dicho Reglamento.

32) No obstante, la exclusión contemplada en el artículo 2, apartado 8, del Reglamento de Inteligencia Artificial se entiende sin perjuicio de la obligación de cumplir lo dispuesto en dicho Reglamento cuando un sistema de IA se introduzca en el mercado o se ponga en servicio como resultado de dicha actividad de investigación y desarrollo[25]. Las pruebas en condiciones reales en el sentido del Reglamento de Inteligencia Artificial[26] tampoco están cubiertas por esa exclusión.

> Por ejemplo: un municipio que quiere probar un programa informático de reconocimiento facial utilizando un sistema de identificación biométrica remota en las

[25] Considerando 25 del Reglamento de Inteligencia Artificial.

[26] De conformidad con el artículo 3, punto 57, del Reglamento de Inteligencia Artificial, se entiende por «pruebas en condiciones reales» las pruebas temporales de un sistema de IA para su finalidad prevista en condiciones reales, fuera de un laboratorio u otro entorno de simulación, con el fin de recabar datos sólidos y fiables y evaluar y comprobar la conformidad del sistema de IA con los requisitos de dicho Reglamento. El Reglamento de Inteligencia Artificial establece un régimen especial para dichas pruebas en condiciones reales; estas pruebas no se consideran introducción en el mercado o puesta en servicio en el sentido de lo dispuesto en dicho Reglamento, siempre que se cumplan todas las condiciones establecidas en los artículos 57 o 60, en particular la obtención del consentimiento libre e informado de los participantes en las pruebas; véase el artículo 60 del Reglamento de Inteligencia Artificial.

calles en carnaval contrata a voluntarios para que el sistema los identifique en condiciones reales. Como las pruebas en condiciones reales no están contempladas en la excepción del artículo 2, apartado 8, del Reglamento de Inteligencia Artificial, las pruebas previstas deben cumplir plenamente los requisitos del Reglamento aplicables a los sistemas de identificación biométrica remota, a menos que el sistema se pruebe en un espacio controlado de pruebas para la IA o de conformidad con el régimen especial para las pruebas en condiciones reales fuera del espacio controlado de pruebas para la IA, tal como se establece en los artículos 60 y 61 del Reglamento de Inteligencia Artificial[27].

33) En cualquier caso, toda actividad de investigación y desarrollo (también cuando está excluida del ámbito de aplicación del Reglamento de Inteligencia Artificial) debe llevarse a cabo de conformidad con normas éticas y profesionales reconocidas para la investigación científica y con el Derecho aplicable de la Unión[28] (por ejemplo, la legislación en materia de protección de datos que sigue siendo aplicable).

2.5.4. Actividad personal de carácter no profesional

34) El artículo 2, apartado 10, del Reglamento de Inteligencia Artificial dispone que este «no se aplicará a las obligaciones de los responsables del despliegue que sean personas físicas que utilicen sistemas de IA en el ejercicio de una actividad puramente personal de carácter no profesional». La definición de responsable del despliegue también excluye a los usuarios que participan en tales actividades (véase la sección2.4.). Debe considerarse una actividad «profesional» toda actividad a través de la cual una persona física obtenga un beneficio económico de forma regular, así como toda actividad profesional, empresarial, comercial o por cuenta propia en la que participe de otro modo. «Personal» actúa como un calificativo de «no profesional», lo que significa que la persona debe actuar tanto a título personal como no profesional. Por consiguiente, la exclusión no debe comprender, por ejemplo, las actividades delictivas, ya que estas no deben considerarse puramente personales.

Por ejemplo: una persona que utiliza un sistema de reconocimiento facial en casa (para controlar el acceso a su domicilio y vigilar la entrada, por ejemplo) entraría en el ámbito de aplicación de la exclusión del artículo 2, apartado 10, del Reglamento de Inteligencia Artificial. Así pues, no estaría sujeta a las obligaciones de los responsables del despliegue que les atribuye el Reglamento de Inteligencia Artificial, incluso en los casos en que esté obligada a transmitir las grabaciones (en su totalidad o parcialmente) a las autoridades garantes del cumplimiento del Derecho.

En cambio, una persona física que utiliza un sistema de IA para actividades profesionales (como los autónomos, los periodistas, los médicos, etc.) tendría que cumplir las obligaciones aplicables los responsables del despliegue de sistemas de reconocimiento facial en virtud del Reglamento de Inteligencia Artificial. Todo uso en el que una persona física actúe en su nombre o bajo la autoridad de un responsable del

[27] El Reglamento de Inteligencia Artificial contiene obligaciones detalladas y específicas para los espacios controlados de pruebas para la IA y las pruebas en condiciones reales. Véase el artículo 57 y siguientes del Reglamento de Inteligencia Artificial.

[28] Considerando 25 del Reglamento de Inteligencia Artificial.

despliegue que actúe a título profesional también entra en el ámbito de aplicación del Reglamento de Inteligencia Artificial.

Además, las actividades delictivas no pueden considerarse actividades puramente personales, aunque no se busque ni se obtenga ningún beneficio económico. En el caso de otras actividades ilícitas, como el incumplimiento de la legislación en materia de protección de los consumidores o de protección de datos y de la legislación administrativa nacional, se aplica la exclusión del Reglamento de Inteligencia Artificial, pero siguen aplicándose los demás marcos jurídicos pertinentes.

35) La exclusión contemplada en el artículo 2, apartado 10, del Reglamento de Inteligencia Artificial se aplica únicamente a las obligaciones de los responsables del despliegue cuando utilizan el sistema para actividades puramente personales de carácter no profesional. El sistema como tal se mantiene dentro del ámbito de aplicación del Reglamento de Inteligencia Artificial en lo que respecta a las obligaciones de los proveedores que lo introducen en el mercado o lo ponen en servicio, otros responsables del despliegue profesionales y otros agentes responsables, como importadores y distribuidores.

Por ejemplo: si un sistema de reconocimiento de emociones está destinado a ser utilizado por personas físicas para actividades puramente personales de carácter no profesional, dicho sistema sigue siendo un sistema de IA de alto riesgo en el sentido del artículo 6 del Reglamento de Inteligencia Artificial y debe ser plenamente conforme con dicho Reglamento. Al mismo tiempo, el responsable del despliegue que lo utilice con fines puramente personales de carácter no profesional (por ejemplo, una persona con autismo) no está sujeto a las obligaciones específicas para los responsables del despliegue que les atribuye el Reglamento de Inteligencia Artificial y su uso quedaría fuera del ámbito de aplicación.

2.5.5. Sistemas de IA divulgados con arreglo a licencias libres y de código abierto

36) De conformidad con el artículo 2, apartado 12, del Reglamento de Inteligencia Artificial, dicho Reglamento no se aplica a los sistemas de IA divulgados con arreglo a licencias libres y de código abierto[29], a menos que se introduzcan en el mercado o se pongan en servicio como sistemas de IA de alto riesgo o como sistemas de IA que entren en el ámbito de aplicación del artículo 5 (prácticas de IA prohibidas) o del artículo 50 (obligaciones de transparencia a determinados sistemas de IA). Esto significa que los proveedores de sistemas de IA no pueden acogerse a esta exclusión si el sistema de IA que introducen en el mercado o ponen en servicio constituye una práctica prohibida contemplada en el artículo 5 del Reglamento de Inteligencia Artificial.

[29] En el considerando 102 del Reglamento de Inteligencia Artificial se indica que la divulgación de *software* y datos con arreglo a una licencia libre y de código abierto permite «compartirlos abiertamente y que los usuarios puedan acceder a ellos, o a versiones modificadas de dicho *software* y dichos datos, o utilizarlos, modificarlos y redistribuirlos libremente».

2.6. Relación de las prohibiciones con los requisitos aplicables a los sistemas de IA de alto riesgo

37) Las prácticas de IA prohibidas por el artículo 5 del Reglamento de Inteligencia Artificial deben examinarse teniendo en cuenta los sistemas de IA clasificados como sistemas de IA de alto riesgo de conformidad con el artículo 6 de dicho Reglamento, en particular los enumerados en el anexo III[30]. Esto se debe a que el uso de sistemas de IA clasificados como sistemas de IA de alto riesgo puede, en algunos casos concretos, considerarse una práctica prohibida si concurren todas las condiciones de una o varias de las prohibiciones contempladas en el artículo 5 del Reglamento de Inteligencia Artificial. Por el contrario, la mayoría de los sistemas de IA que están cubiertos por una excepción a una prohibición establecida en el artículo 5 del Reglamento de Inteligencia Artificial se consideran de alto riesgo.

> Por ejemplo: los sistemas de reconocimiento de emociones que no cumplen las condiciones de la prohibición establecida en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial se clasifican como sistemas de IA de alto riesgo de conformidad con el artículo 6, apartado 2, y el anexo III, punto 1, letra c), del Reglamento de Inteligencia Artificial. Del mismo modo, determinados sistemas de puntuación basados en la IA, como los utilizados para la calificación crediticia o la evaluación de riesgos en materia de seguros de vida y de salud, se consideran sistemas de IA de alto riesgo si no cumplen las condiciones de la prohibición contemplada en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial[31]. Otro ejemplo son los sistemas de IA que evalúan a las personas y determinan si tienen derecho a recibir prestaciones y servicios esenciales de asistencia pública, como los servicios de asistencia sanitaria y las prestaciones de seguridad social, que se clasifican como sistemas de alto riesgo[32]. Si dichos sistemas implican unas prácticas inaceptables de puntuación ciudadana y cumplen las condiciones del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial, su introducción en el mercado, puesta en servicio y utilización se prohibirán en la Unión.
>
> En tales casos, la evaluación y gestión de riesgos realizada por el proveedor y el cumplimiento de los demás requisitos aplicables a los sistemas de IA de alto riesgo (por ejemplo, gobernanza de datos, transparencia y supervisión humana), así como las obligaciones del responsable del despliegue relativas al uso adecuado de conformidad con las instrucciones de uso y la supervisión humana (artículo 26) y, en algunos casos, una evaluación de impacto relativa a los derechos fundamentales (artículo 27), deben contribuir a garantizar que el sistema de IA de alto riesgo introducido en el mercado o desplegado sea lícito y no constituya una práctica prohibida.

38) Por último, los sistemas de IA que, excepcionalmente, no se consideren de alto riesgo sobre la base del artículo 6, apartado 3, del Reglamento de Inteligencia Artificial,

---

30 En esta lista se incluyen los sistemas de IA basados en la biometría, así como los sistemas de IA utilizados para fines específicos en determinados ámbitos, como el empleo, la educación, el acceso a servicios públicos y privados, la garantía del cumplimiento del Derecho, etc.

31 Esto se menciona expresamente en el considerando 58 y en el anexo III del Reglamento de Inteligencia Artificial.

32 Considerando 58 del Reglamento de Inteligencia Artificial.

aunque estén incluidos en un caso de uso de alto riesgo contemplado en el anexo III, pueden seguir entrando en el ámbito de aplicación de las prohibiciones establecidas en el artículo 5 del Reglamento de Inteligencia Artificial. El artículo 6, apartado 3, del Reglamento de Inteligencia Artificial solo tiene por efecto que un sistema de IA no se considere de alto riesgo; no excluye dichos sistemas de IA del ámbito de aplicación del Reglamento de Inteligencia Artificial ni de las prohibiciones.

2.7. Aplicación de las prohibiciones a los sistemas de IA de uso general y a los sistemas con finalidades previstas

39) Las prohibiciones se aplican a cualquier sistema de IA, independientemente de que tenga una «finalidad prevista[33]» o sea de «uso general» (es decir, que pueda servir para diversos fines), tanto para su uso directo como para su integración en otros sistemas de IA[34]. En consecuencia, cada operador debe adoptar las medidas para las que estén mejor situado en función de su papel y del control que ejerce sobre el sistema en la cadena de valor, a fin garantizar un suministro y un uso responsables y seguros de los sistemas de IA, equilibrando sus riesgos y beneficios para alcanzar el doble objetivo del Reglamento de Inteligencia Artificial.

40) Por tanto, se espera que los responsables del despliegue no utilicen ningún sistema de IA de una manera prohibida por el artículo 5 del Reglamento de Inteligencia Artificial, en particular que no eludan ninguna salvaguardia aplicada por los proveedores del sistema. Si bien los perjuicios a menudo se producen por la forma en que se utilizan los sistemas de IA en la práctica, los proveedores también tienen la responsabilidad de no introducir en el mercado ni poner en servicio sistemas de IA, en particular sistemas de IA de uso general, que es razonablemente probable que se comporten o se utilicen directamente de una forma prohibida por el artículo 5 del Reglamento de Inteligencia Artificial[35]. En este contexto, se espera igualmente que los proveedores adopten medidas eficaces y verificables tanto para establecer garantías como para prevenir y mitigar dichos comportamientos perjudiciales y usos indebidos en la medida en que sean razonablemente previsibles y las medidas sean viables y proporcionadas en función del sistema de IA de que se trate y de las circunstancias. También se espera que los proveedores, en sus relaciones contractuales con los responsables del despliegue (es decir, en las condiciones de uso del sistema de IA), excluyan el uso de su sistema de IA para prácticas prohibidas y que incluyan la información adecuada en las instrucciones de uso dirigidas a los responsables del despliegue y sobre la supervisión humana necesaria.

> Por ejemplo: un sistema de IA de uso general utilizado como chatbot puede desplegar técnicas manipuladoras y engañosas que es probable que provoquen perjuicios considerables. Para evitar comportamientos prohibidos del sistema de IA y usos que es

[33] Se define en el artículo 3, punto 12, del Reglamento de Inteligencia Artificial como el uso para el que un proveedor concibe un sistema de IA, incluidos el contexto y las condiciones de uso concretos, según la información facilitada por el proveedor en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica.

[34] Véase el artículo 3, punto 66, del Reglamento de Inteligencia Artificial.

[35] Esto se deriva, en particular, de la referencia a la «introducción en el mercado» o la «puesta en servicio» incluida en todas las prohibiciones enumeradas en el artículo 5 del Reglamento de Inteligencia Artificial, con excepción de la prohibición de los sistemas de identificación biométrica remota en tiempo real establecida en el artículo 5, apartado 1, letra h), que se aplica únicamente al uso.

razonablemente probable que manipulen, engañen y provoquen perjuicios considerables de conformidad con el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, se espera que el proveedor adopte medidas adecuadas y proporcionadas (un diseño seguro y ético adecuado, integración de garantías técnicas y de otro tipo, restricciones de uso, transparencia y control de los usuarios e información adecuada en las instrucciones de uso, por ejemplo) antes de que el sistema de IA se introduzca en el mercado [artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial] para garantizar que el chatbot no provoque perjuicios considerables a los usuarios ni a otras personas o colectivos de personas [véase también la sección 3.2.3, letra c)].

41) En determinados casos, en particular cuando las prohibiciones están relacionadas con una finalidad muy específica del sistema[36], los proveedores pueden tener posibilidades limitadas de integrar otras medidas preventivas y de reducción de riesgos; en tales casos, deben basarse principalmente en el suministro de instrucciones e información adecuadas a los responsables del despliegue, en la supervisión humana necesaria y en la restricción del uso prohibido del sistema. Cuando proceda, entre dichas medidas también puede figurar la supervisión del cumplimiento de dicha restricción, en función de los medios a través de los cuales se suministre el sistema de IA y de la información de que disponga el proveedor para un posible uso indebido. Las posibles medidas de supervisión para detectar usos indebidos no deben equivaler a una supervisión general de las actividades de los responsables del despliegue y deben estar en consonancia con el Derecho de la Unión.

Por ejemplo: los responsables del despliegue no deben usar en los lugares de trabajo o en los centros educativos un sistema de IA de uso general que pueda reconocer o deducir las emociones, a menos que se aplique una excepción por motivos médicos o de seguridad. Sin embargo, el proveedor puede no conocer el contexto específico en el que se utilizará la funcionalidad de reconocimiento de emociones del sistema y si puede aplicarse una excepción a la prohibición contemplada en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial. No obstante, estos proveedores pueden excluir explícitamente dicho uso prohibido en sus condiciones de uso e incluir información adecuada en las instrucciones de uso para orientar a los responsables del despliegue. También se espera que adopten las medidas adecuadas si tienen conocimiento de que determinados responsables del despliegue usan el sistema de forma indebida para esta finalidad específica prohibida, por ejemplo, si se notifica ese uso indebido o si el proveedor tiene conocimiento de ello por otros medios, lo que puede ocurrir si el sistema funciona directamente en una plataforma bajo el control del proveedor y este realiza controles.

2.8. Relación entre las prohibiciones y otras disposiciones del Derecho de la Unión

[36] Artículo 5, apartado 1, letras d) a h), del Reglamento de Inteligencia Artificial.

42) El Reglamento de Inteligencia Artificial se aplica horizontalmente en todos los sectores sin perjuicio de otras disposiciones del Derecho de la Unión, en particular en materia de protección de derechos fundamentales, protección de los consumidores, empleo, protección de los trabajadores y seguridad de los productos[37]. El Reglamento complementa estos actos con su lógica de prevención y de seguridad (los sistemas de IA no pueden introducirse en el mercado o usarse de una determinada manera) y ofrece una protección complementaria al tratar determinadas prácticas de IA perjudiciales que pueden no estar prohibidas por otros actos legislativos. Además, al abordar las fases iniciales del ciclo de vida de los sistemas de IA (es decir, la introducción en el mercado y la puesta en servicio) y el despliegue (es decir, el uso), las prohibiciones del Reglamento de Inteligencia Artificial permiten adoptar medidas contra las prácticas perjudiciales que implican la IA en diversos puntos de la cadena de valor de la IA.

43) Al mismo tiempo, el Reglamento de Inteligencia Artificial no afecta a las prohibiciones aplicables cuando una práctica de IA entra en el ámbito de aplicación de otras disposiciones del Derecho de la Unión[38]. Así pues, aunque un sistema de IA no esté prohibido por el Reglamento de Inteligencia Artificial, su uso podría estar prohibido o ser ilícito en virtud de otras disposiciones del Derecho primario o derivado de la Unión. Esto puede suceder, por ejemplo, si no se respetan los derechos fundamentales en un caso concreto, como la falta de base jurídica para el tratamiento de datos personales exigida por la legislación en materia de protección de datos, la discriminación prohibida por el Derecho de la Unión, etc. La observancia de las prohibiciones del Reglamento de Inteligencia Artificial no es, por tanto, una condición suficiente para garantizar el cumplimiento de otros actos legislativos de la Unión que sigan siendo aplicables a los proveedores y responsables del despliegue de sistemas de IA.

> Por ejemplo: los sistemas de reconocimiento de emociones que posibilita la IA utilizados en el lugar de trabajo y exentos de la prohibición contemplada en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial (porque se utilizan con fines médicos o de seguridad) siguen estando sujetos a la legislación en materia de protección de datos y a la legislación nacional y de la Unión en materia de empleo y condiciones de trabajo, en particular la relativa a la salud y la seguridad en el trabajo, que pueden establecer otras restricciones y garantías en relación con el uso de dichos sistemas[39].

44) Cuando otros actos legislativos de la Unión también contemplan actividades específicas relacionadas con la introducción en el mercado o el uso de sistemas de IA, el Reglamento de Inteligencia Artificial tiene por objeto garantizar la aplicación coherente de las diferentes disposiciones. Además, permite una cooperación eficaz entre las autoridades competentes encargadas de garantizar el cumplimiento de dicho Reglamento y las autoridades encargadas de proteger los derechos fundamentales, de conformidad con su artículo 77 y otras disposiciones. De manera más general, de conformidad con el artículo 4, apartado 3, del TUE, las distintas autoridades implicadas

[37] Artículo 2 y considerando 9 del Reglamento de Inteligencia Artificial.
[38] Artículo 5, punto 8, del Reglamento de Inteligencia Artificial.
[39] Véase también el considerando 9 del Reglamento de Inteligencia Artificial.

están obligadas a cooperar lealmente en el desempeño de las diferentes funciones que les atribuye el Derecho de la Unión.

45) En el contexto de las prohibiciones, la relación entre el Reglamento de Inteligencia Artificial y la legislación de la Unión en materia de protección de datos es especialmente pertinente, ya que los sistemas de IA a menudo tratan información relativa a personas físicas identificadas o identificables («datos personales»)[40]. En función de la prohibición y del contexto, los actos jurídicos más pertinentes en relación con dichos sistemas son el Reglamento (UE) 2016/679 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 (Reglamento general de protección de datos, en lo sucesivo, el «RGPD»), la Directiva (UE) 2016/680 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 (en lo sucesivo, la «Directiva sobre protección de datos en el ámbito penal»), y el Reglamento (UE) 2018/1725, que establece las normas de protección de datos para las instituciones, órganos y organismos de la Unión (en lo sucesivo, el «RPDUE»). De conformidad con el artículo 2, apartado 7, del Reglamento de Inteligencia Artificial, estos actos no se ven afectados y seguirán aplicándose junto con el Reglamento de Inteligencia Artificial, que es coherente y complementario con el acervo de la UE en materia de protección de datos. El TJUE ha aclarado varios aspectos de estas normas de protección de datos de la UE y el Comité Europeo de Protección de Datos ha adoptado una serie de directrices sobre, por ejemplo, el concepto de «elaboración de perfiles»[41], que es especialmente pertinente para la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, ya que utiliza el mismo concepto.

46) En lo que respecta a las prohibiciones o restricciones al uso de sistemas de categorización biométrica y sistemas de identificación biométrica remota en tiempo real con fines de garantía del cumplimiento del Derecho, el Reglamento de Inteligencia Artificial se aplica como *lex specialis* respecto del artículo 10 de la Directiva sobre protección de datos en el ámbito penal, con lo que se regula de manera exhaustiva dicho uso y el tratamiento de los correspondientes datos biométricos[42]. En ese sentido, el Reglamento de Inteligencia Artificial no tiene por objeto proporcionar la base jurídica para el tratamiento de datos personales en virtud del artículo 8 de la Directiva (UE) 2016/680. Todas las demás disposiciones de dicha Directiva se aplican además de las condiciones establecidas en el Reglamento de Inteligencia Artificial, en particular para el uso de sistemas (de identificación biométrica remota) en tiempo real con fines de garantía del cumplimiento del Derecho cuando esté permitido, sin perjuicio de las limitadas excepciones contempladas en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial. En términos más generales, cuando las

[40] Artículo 2, apartado 7, del Reglamento de Inteligencia Artificial; véase también su considerando 10.

[41] Véase también Grupo de Trabajo del Artículo 29, «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679», 6 de febrero de 2018, WP251rev.01, aprobadas por el CEPD.

[42] Considerando 38 del Reglamento de Inteligencia Artificial.

autoridades garantes del cumplimiento del Derecho (es decir, las autoridades competentes en virtud del artículo 3, punto 7, de la Directiva sobre protección de datos en el ámbito penal) traten datos personales con fines de garantía del cumplimiento del Derecho también deben respetar la Directiva sobre protección de datos en el ámbito penal.

47) De conformidad con el artículo 2, apartado 9, del Reglamento de Inteligencia Artificial, la legislación de la Unión en materia de protección y seguridad de los consumidores también sigue siendo plenamente aplicable a los sistemas de IA que entren en el ámbito de aplicación de dichos actos.

A continuación, varios ejemplos:

- Las prácticas de puntuación ciudadana de los comerciantes (incluidas las personas físicas que actúan a título profesional en las relaciones entre las empresas y los consumidores), sujetas a una evaluación caso por caso, también pueden considerarse «desleales» y, por tanto, infringen la legislación en materia de protección de los consumidores (es decir, la Directiva 2005/29/CE);

- Es posible que el uso de un sistema de IA para deducir las emociones también deba ajustarse al Reglamento (UE) 2017/745 (Reglamento sobre los productos sanitarios) si el sistema de IA se utiliza con fines de diagnóstico o tratamiento médico.

48) Además, el Reglamento de Inteligencia Artificial se aplica en conjunción con las obligaciones pertinentes para los prestadores de servicios intermediarios que integran sistemas o modelos de IA en sus servicios regulados por el Reglamento (UE) 2022/2065 (en lo sucesivo, el «Reglamento de Servicios Digitales»). En concreto, en el artículo 2, apartado 5, del Reglamento de Inteligencia Artificial se indica que dicho Reglamento no afecta a la aplicación de las disposiciones relativas a la responsabilidad de dichos prestadores según lo establecido en el capítulo II del Reglamento de Servicios Digitales.

49) Además, las prohibiciones del Reglamento de Inteligencia Artificial se entienden sin perjuicio de cualquier responsabilidad que el proveedor o el responsable del despliegue pudiera asumir por el perjuicio causado de conformidad con la legislación nacional o de la Unión aplicable en materia de responsabilidad[43].

50) Por último, las prohibiciones del artículo 5 del Reglamento de Inteligencia Artificial y las excepciones explícitas a dichas prohibiciones no pueden utilizarse para eludir las obligaciones establecidas en otros actos legislativos de la Unión o para justificar su incumplimiento.

51) Como Derecho derivado de la Unión, el Reglamento de Inteligencia Artificial debe interpretarse a la luz de los derechos y libertades fundamentales garantizados por los

[43] Las condiciones de la responsabilidad (relativas al daño, la persona responsable, la culpa o la carga de la prueba, etc.) estarán determinadas por la legislación aplicable, como la Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos (Texto pertinente a efectos del EEE), DO L, 2024/2853, 18.11.2024, o por la legislación nacional aplicable en materia de responsabilidad [véase también la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA) COM/2022/496 final].

Tratados de la UE y la Carta, así como de los protegidos por los convenios internacionales de los que la Unión es parte[44].

52) En las secciones pertinentes a continuación, se ofrecen aclaraciones adicionales sobre la relación entre una serie de prohibiciones específicas con otras disposiciones del Derecho de la Unión.

2.9. Cumplimiento del artículo 5 del Reglamento de Inteligencia Artificial

2.9.1. Autoridades de vigilancia del mercado

53) Las autoridades de vigilancia del mercado designadas por los Estados miembros y el Supervisor Europeo de Protección de Datos (como autoridad de vigilancia del mercado de las instituciones, órganos y organismos de la UE) son responsables de controlar el cumplimiento de las normas del Reglamento de Inteligencia Artificial relativas a los sistemas de IA, incluidas las prohibiciones. Dicho control del cumplimiento se lleva a cabo en el marco del sistema de vigilancia del mercado y conformidad de los productos establecido por el Reglamento (UE) 2019/1020[45], en consonancia con otros actos legislativos de la Unión en materia de seguridad de los productos. Los poderes de ejecución de las autoridades de vigilancia del mercado en relación con los sistemas de IA se establecen en el Reglamento de Inteligencia Artificial y en el Reglamento (UE) 2019/1020. Dichas autoridades pueden adoptar medidas de control del cumplimiento en relación con las prohibiciones, por iniciativa propia o a raíz de una reclamación, que toda persona afectada o cualquier otra persona física o jurídica que tenga motivos para considerar que se han producido tales infracciones puede presentar[46]. Los Estados miembros deben designar a sus autoridades de vigilancia del mercado competentes a más tardar el 2 de agosto de 2025.

54) El procedimiento establecido en el Reglamento de Inteligencia Artificial aplicable a los sistemas de IA que presenten un riesgo a escala nacional es especialmente pertinente en el contexto del control del cumplimiento de las prohibiciones[47]. Cuando existan repercusiones transfronterizas fuera del territorio de la autoridad de vigilancia del mercado, la autoridad del Estado miembro de que se trate deberá informar a la Comisión y a las autoridades de vigilancia del mercado de otros Estados miembros. Todas las autoridades de vigilancia del mercado deben seguir un procedimiento de salvaguardia de la Unión; en el marco de este procedimiento, la Comisión[48] decide si el sistema de IA constituye una práctica prohibida. El objetivo de este procedimiento es garantizar que las prohibiciones se aplican de manera uniforme en todos los Estados miembros, a fin de proporcionar seguridad jurídica tanto a los proveedores como a los responsables del despliegue de sistemas de IA. Para garantizar la aplicación uniforme del Reglamento de Inteligencia Artificial, las autoridades nacionales de vigilancia del mercado también

---

44 Aunque la Unión aún no es parte en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, el artículo 59, apartado 3, de la Carta establece que, en la medida en que esta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y ámbito de aplicación serán iguales a los que les confiere dicho Convenio. Esta disposición no obstará para que el Derecho de la Unión conceda una protección más extensa.

45 Véase también el considerando 156 del Reglamento de Inteligencia Artificial.

46 Artículo 85 del Reglamento de Inteligencia Artificial.

47 Artículo 79 del Reglamento de Inteligencia Artificial.

48 Artículo 81 del Reglamento de Inteligencia Artificial.

deben esforzarse por lograr una aplicación armonizada de las prohibiciones en casos comparables que no trasciendan el territorio del Estado miembro, inspirándose en las presentes directrices y cooperando en el Consejo de IA[49].

2.9.2. Sanciones

55) El Reglamento de Inteligencia Artificial sigue un enfoque escalonado a la hora de fijar las sanciones por incumplimiento de sus diferentes disposiciones, en función de la gravedad de la infracción. Se considera que el incumplimiento de las prohibiciones establecidas en el artículo 5 del Reglamento de Inteligencia Artificial constituye la infracción más grave y, por tanto, está sujeto a la multa más elevada. Los proveedores y los responsables del despliegue que lleven a cabo prácticas de IA prohibidas pueden ser sancionados con multas de hasta 35 000 000 EUR o, si el infractor es una empresa, de hasta el 7 % de su volumen de negocios mundial total correspondiente al ejercicio financiero anterior, si esta cuantía fuese superior[50]. Cada Estado miembro debe establecer normas que determinen si es posible imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro como proveedores y responsables del despliegue de sistemas de IA, y en qué medida. Las instituciones, órganos y organismos de la UE que infrinjan las prohibiciones pueden estar sujetos a multas administrativas de hasta 1 500 000 EUR[51].

56) Es posible que una misma conducta prohibida infrinja dos o más disposiciones del Reglamento de Inteligencia Artificial. Por ejemplo, no etiquetar las ultrafalsificaciones también puede constituir una técnica engañosa según el artículo 5, apartado 1, letra a), de dicho Reglamento. En tales casos, debe respetarse el principio *non bis in idem*. En cualquier caso, para determinar la sanción deben tenerse en cuenta los criterios establecidos en el artículo 99, apartado 7, del Reglamento de Inteligencia Artificial.

57) Dado que las infracciones de las prohibiciones del artículo 5 del Reglamento de Inteligencia Artificial son las que más interfieren con las libertades de terceros y las que se sancionan con multas más elevadas, su ámbito de aplicación debe interpretarse de manera restrictiva.

3. ARTÍCULO 5, APARTADO 1, LETRAS A) Y B), DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: MANIPULACIÓN, ENGAÑO Y EXPLOTACIÓN PERJUDICIALES

58) Las dos primeras prohibiciones del artículo 5, apartado 1, letras a) y b), respectivamente, del Reglamento de Inteligencia Artificial tienen por objeto proteger a las personas y a las personas vulnerables de los efectos considerablemente perjudiciales de la manipulación y la explotación que posibilita la IA. Dichas prohibiciones se refieren a los sistemas de IA que se sirven de técnicas subliminales, deliberadamente manipuladoras o engañosas, que causan perjuicios considerables y alteran de manera sustancial el comportamiento de personas físicas o de uno o varios colectivos de

[49] Artículos 65 y 66 del Reglamento de Inteligencia Artificial.
[50] Artículo 99 del Reglamento de Inteligencia Artificial.
[51] Artículo 100 del Reglamento de Inteligencia Artificial.

personas [artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial] o explotan vulnerabilidades derivadas de la edad o discapacidad, o de una situación social o económica específica [artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial].

3.1. Justificación y objetivos

59) La justificación subyacente de estas prohibiciones es proteger la autonomía y el bienestar individuales de prácticas de IA de manipulación, engaño y explotación que puedan socavar y perjudicar la autonomía, la toma de decisiones y la capacidad de elegir libremente de una persona[52]. El objetivo de las prohibiciones es proteger el derecho a la dignidad humana (artículo 1 de la Carta), que también constituye la base de todos los derechos fundamentales e incluye la autonomía individual como un elemento fundamental. En particular, el objetivo de las prohibiciones es evitar la manipulación y la explotación a través de sistemas de IA que reduzcan a las personas a meros instrumentos para lograr determinados fines, así como proteger a las más vulnerables y expuestas a la manipulación y explotación perjudiciales. Las prohibiciones de prácticas de IA de manipulación, engaño y explotación considerablemente perjudiciales se ajustan plenamente a los objetivos generales del Reglamento de Inteligencia Artificial, a saber, la promoción de sistemas de IA fiables y centrados en el ser humano que sean seguros, transparentes y justos, que estén al servicio de la humanidad y se ajusten a la acción humana y a los valores de la UE.

3.2. Componentes principales de la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial: manipulación perjudicial

Según el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial:

1. Quedan prohibidas las siguientes prácticas de IA:

a) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que se sirva de técnicas subliminales que trasciendan la conciencia de una persona o de técnicas deliberadamente manipuladoras o engañosas con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas, mermando de manera apreciable su capacidad para tomar una decisión informada y haciendo que tomen una decisión que de otro modo no habrían tomado, de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas;

60) Deben cumplirse varias condiciones acumulativas para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial:

(i) La práctica debe consistir en la «introducción en el mercado», la «puesta en servicio» o la «utilización» de un sistema de IA.

[52] Considerando 29 del Reglamento de Inteligencia Artificial.

(ii) El sistema de IA debe servirse de técnicas subliminales (que trasciendan la conciencia de una persona), deliberadamente manipuladoras o engañosas.

(iii) Las técnicas utilizadas por el sistema de IA deben tener el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o de un colectivo de personas. La alteración debe mermar de manera apreciable su capacidad para tomar una decisión informada, dando lugar a una decisión que, de otro modo, la persona o el colectivo de personas no habrían tomado.

(iv) El comportamiento alterado debe provocar, o ser razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas.

61) Para que se aplique la prohibición, deben cumplirse las cuatro condiciones al mismo tiempo y debe existir una relación de causalidad plausible entre las técnicas utilizadas, la alteración sustancial del comportamiento de la persona y el perjuicio considerable que haya provocado o sea razonablemente probable que provoque dicho comportamiento.

62) Ya se ha examinado la primera condición, a saber, la «introducción en el mercado», la «puesta en servicio» o la «utilización» de un sistema de IA. Así pues, la prohibición se aplica tanto a los proveedores como a los responsables del despliegue de sistemas de IA, cada uno dentro de sus respectivas responsabilidades de no introducir en el mercado, no poner en servicio o no utilizar dichos sistemas. Las siguientes secciones se centran en las otras tres condiciones.

3.2.1. Técnicas subliminales, deliberadamente manipuladoras o engañosas

63) El artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial prohíbe tres posibles tipos de técnicas manipuladoras: a) técnicas subliminales que trasciendan la conciencia de una persona; b) técnicas deliberadamente manipuladoras; y c) técnicas engañosas. Un sistema de IA debe servirse de una o varias de estas técnicas para que entre en el ámbito de aplicación del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial.

a) Técnicas subliminales

64) Si bien el Reglamento de Inteligencia Artificial no ofrece una definición de «técnicas subliminales», en su artículo 5, apartado 1, letra a), se especifica que las técnicas subliminales trascienden (por debajo o por encima) el umbral de la conciencia. Puesto que las técnicas subliminales y su funcionamiento están intrínsecamente ocultos, estas técnicas eluden las defensas racionales de una persona contra la manipulación y pueden influir en las decisiones sin que la persona sea consciente de ello, lo que plantea importantes preocupaciones éticas y perjudica la autonomía individual, la voluntad y la capacidad de elegir libremente[53].

65) Las técnicas subliminales deben ser capaces de influir en el comportamiento de forma que la persona no sea consciente de dicha influencia, de su funcionamiento ni de sus

[53] Considerando 29 del Reglamento de Inteligencia Artificial.

efectos en la toma de decisiones o en la formación de valores y opiniones de la persona. En particular, las técnicas subliminales pueden utilizar estímulos emitidos a través de medios sonoros, visuales o táctiles demasiado breves o sutiles para ser percibidos y que son tradicionalmente conocidos y están prohibidos en otros sectores, como la publicidad en los medios de comunicación[54]. Estos estímulos, aunque no se perciben de forma consciente, pueden seguir siendo procesados por el cerebro e influir en el comportamiento.

A continuación figuran algunos ejemplos de técnicas subliminales [no necesariamente prohibidas, a menos que se cumplan todas las demás condiciones enumeradas en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial]:

- Mensajes subliminales visuales: un sistema de IA puede mostrar o integrar imágenes o textos que parpadeen brevemente mientras se reproduce un vídeo y que técnicamente sean visibles, pero que lo hacen con demasiada rapidez como para que la mente consciente pueda registrarlos; aun así, siguen siendo capaces de influir en actitudes o comportamientos.

- Mensajes subliminales sonoros: un sistema de IA puede emitir sonidos o mensajes verbales a un volumen bajo o camuflados por otros sonidos; esto influye en el oyente sin que sea consciente de ello. Técnicamente, estos sonidos siguen estando dentro del campo de audibilidad, pero el oyente no los detecta de manera consciente por ser muy sutiles o estar camuflados por otros sonidos.

- Estímulos subliminales táctiles: un sistema de IA puede estimular sensaciones físicas sutiles que se perciben de forma inconsciente y que pueden influir en los estados emocionales o en el comportamiento.

- Señales subvisuales y subsonoras: un sistema de IA puede utilizar estímulos que no solo sean sutiles o estén camuflados, sino que se presenten de manera que sean totalmente imperceptibles por los sentidos humanos en condiciones normales. Es el caso, por ejemplo, de los estímulos visuales intermitentes (por ejemplo, imágenes intermitentes) que parpadean con demasiada rapidez como para que el ojo humano pueda detectarlos de forma consciente, o de los sonidos que se reproducen a unos volúmenes imperceptibles para el oído humano.

- Imágenes integradas: un sistema de IA puede ocultar dentro de otros contenidos visuales imágenes que no se perciben de manera consciente, pero que pueden ser procesadas por el cerebro e influir en el comportamiento.

- Desvío de la atención: un sistema de IA puede desviar la atención hacia estímulos o contenidos específicos para evitar que se perciban otros contenidos, a menudo explotando sesgos cognitivos y vulnerabilidades de la atención.

[54] Véase en particular la Directiva 2010/13/UE del Parlamento Europeo y del Consejo, de 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (DO L 95 de 15.4.2010, p. 1), en lo sucesivo «Directiva de servicios de comunicación audiovisual», que prohíbe estrictamente las técnicas subliminales en las comunicaciones comerciales audiovisuales.

- Manipulación temporal: un sistema de IA puede alterar la percepción del tiempo en las interacciones de los usuarios, influyendo así en su comportamiento y generando impaciencia y dependencia.

66) El rápido desarrollo de la IA y las tecnologías relacionadas, como el análisis de macrodatos, las neurotecnologías, las interfaces cerebro-máquina y la realidad virtual, aumenta el riesgo de manipulación subliminal sofisticada y su capacidad para influir eficazmente en el comportamiento humano de forma subconsciente[55]. La IA también puede extenderse a las interfaces cerebro-máquina emergentes y a técnicas avanzadas como la manipulación del sueño y el espionaje neuronal.

Por ejemplo: un juego puede utilizar neurotecnologías que posibilita la IA e interfaces cerebro-máquina que permiten a los usuarios controlar un juego o partes del mismo con un casco que detecte la actividad cerebral. La IA puede utilizarse para entrenar el cerebro del usuario de forma subrepticia y sin su conocimiento para revelar o extraer de los datos neuronales información que puede ser muy intrusiva o sensible (por ejemplo, información bancaria personal, información íntima, etc.) de un modo que pueda provocarles perjuicios considerables. La prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial se refiere únicamente a los casos de manipulación subliminal considerablemente perjudicial; no se refiere a las aplicaciones de la interfaz cerebro-máquina en general cuando se diseñan de manera segura y protegida y de tal forma que respetan la privacidad y la autonomía individual.

b) Técnicas deliberadamente manipuladoras

67) Las «técnicas deliberadamente manipuladoras» no se definen en el Reglamento de Inteligencia Artificial, pero deben entenderse como técnicas diseñadas u objetivamente destinadas a influir, alterar o controlar el comportamiento de una persona de tal manera que socave su autonomía individual y su capacidad de elegir libremente. Las técnicas manipuladoras suelen estar diseñadas para explotar los sesgos cognitivos, las vulnerabilidades psicológicas o los factores situacionales que hacen que las personas sean más influenciables. Debido a su adaptabilidad, los sistemas de IA también pueden responder bien a las circunstancias o vulnerabilidades de una persona y aumentar la eficacia y el impacto de la manipulación a gran escala. Si bien la capacidad de manipulación es un importante factor para determinar la naturaleza de la técnica, no es necesario que el proveedor, el responsable del despliegue o el propio sistema que se sirve de las técnicas manipuladoras también tengan la intención de causar un perjuicio[56].

68) Aunque no todas las técnicas manipuladoras trascienden el umbral de la conciencia, muchas de ellas sí lo hacen y pueden solaparse con las técnicas subliminales, ya que, en última instancia, estas técnicas también tienen efectos de manipulación. El considerando 29 del Reglamento de Inteligencia Artificial aclara que la prohibición establecida en el artículo 5, apartado 1, letra a), también contempla las técnicas en las que las personas, aunque sean conscientes del intento de influencia, pueden no ser

[55] Véase el considerando 29 del Reglamento de Inteligencia Artificial.
[56] Véanse, en este contexto, el considerando 28 y las secciones 3.2.2 y 3.2.3 de las directrices.

capaces de controlar su efecto manipulador o de resistir a dicho efecto[57]. Por consiguiente, las personas se ven influidas o forzadas a tener comportamientos y a tomar decisiones que normalmente no habrían tenido o tomado si no estuvieran sometidas a las técnicas manipuladoras, hasta el punto de socavar su autonomía individual o su capacidad de elegir libremente.

Un ejemplo de técnica deliberadamente manipuladora es la manipulación sensorial, en la que sistema de IA utiliza audio o imágenes de fondo que alteran el estado de ánimo, por ejemplo, generando un aumento de la ansiedad y la angustia mental que influya en el comportamiento de los usuarios hasta el punto de provocar perjuicios considerables.

Otro ejemplo es la manipulación personalizada, en la que un sistema de IA que crea y adapta mensajes muy persuasivos basados en los datos personales de una persona o explota otras vulnerabilidades individuales influye en su comportamiento o sus elecciones hasta el punto de provocar perjuicios considerables.

69) La prohibición de las técnicas deliberadamente manipuladoras también se aplica a los sistemas de IA que manipulan a las personas sin que ningún ser humano tenga la intención de hacerlo. El artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial prohíbe los sistemas de IA que se sirvan de determinadas técnicas o muestren un comportamiento manipulador específico. Por lo tanto, también podría ser el sistema de IA el que se sirva de dichas técnicas manipuladoras, en lugar del proveedor o el responsable del despliegue que haya diseñado o utilizado el sistema de este modo.

Por ejemplo: independientemente de la intención del proveedor, un sistema de IA puede aprender técnicas manipuladoras porque los datos con los que se entrena contienen muchos casos de técnicas manipuladoras[58], o porque el aprendizaje por refuerzo a partir de la retroalimentación humana puede verse «influido» por técnicas manipuladoras[59].

En cambio, si el comportamiento manipulador del sistema es meramente incidental, no debe considerarse que el sistema utiliza técnicas deliberadamente manipuladoras siempre que el proveedor haya adoptado las medidas preventivas y de reducción de riesgos adecuadas en caso de que sea razonablemente probable que se produzcan perjuicios considerables [véase la sección 3.2.3, letra c)].

---

57 Considerando 28 del Reglamento de Inteligencia Artificial.

58 Carrol, M., Chan, A. Ashton, H. y Krueger, D., «Characterizing Manipulation from AI Systems» [«Características de la manipulación por sistemas de IA», documento no disponible en español], *Proceedings of the 3rd ACM Conference on Equity and Access in Algorithms, Mechanisms, and Optimization (EAAMO '23)*, Association for Computing Machinery, Nueva York, 30 de octubre - 1 de noviembre, 2023, pp. 1-13, https://doi.org/10.1145/3617694.3623226 |:2303.09387.

59 Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., et al., «Concrete Problems in AI Safety», [«Problemas concretos de seguridad en materia de IA», documento no disponible en español], *36th Conference on Neural Information Processing Systems (NeurIPS 2022)*, 2022, arXiv:1606.06565; Skalse, J., Howe, N., Krasheninnikov, D. y Krueger, D.,«Defining and Characterizing Reward Gaming» [«Definición y caracterización de la manipulación de recompensas», documento no disponible en español] en Koyejo, S., Mohamed, S., Agarwal, A., Belgrave, D, Cho, K. et al. (eds.), *Advances in Neural Information Processing Systems 35 (NeurIPS 2022)*, 2022; Denison, C, MacDiarmid, M., Barez, F., Duvenaud, D., Kravec, S. et al., «Sycophancy to Subterfuge: Investigating Reward-Tampering in Large Language Models» [«De la lisonja al subterfugio: estudio de la manipulación de recompensas en grandes modelos lingüísticos», documento no disponible en español], *36th Conference on Neural Information Processing Systems (NeurIPS 2022)*, 2022, arXiv:2406.10162.

c) Técnicas engañosas

70) El Reglamento de Inteligencia Artificial no ofrece una definición de «técnicas engañosas». El considerando 29 del Reglamento de Inteligencia Artificial aclara que son técnicas que socavan o perjudican la autonomía, la toma de decisiones o la capacidad de elegir libremente de las personas de maneras de las que estas no son realmente conscientes de dichas técnicas o, cuando lo son, pueden seguir siendo engañadas o no pueden controlarlas u oponerles resistencia. Por «técnicas engañosas» desplegadas por los sistemas de IA debe entenderse la presentación de información falsa o engañosa con el objetivo o el efecto de engañar a las personas e influir en su comportamiento de tal manera que se socave su autonomía, su toma de decisiones y capacidad de elegir libremente.

71) En este contexto, debe aclararse la relación entre la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial y las obligaciones del responsable del despliegue contempladas en el artículo 50, apartado 4, de dicho Reglamento de etiquetar las ultrafalsificaciones y determinadas publicaciones de texto generadas por la IA sobre asuntos de interés público[60], así como la obligación del proveedor de garantizar que los sistemas de IA que interactúan con personas estén diseñados de manera que las informen de que están interactuando con la IA y no con un ser humano[61]. Dicha divulgación visible constituye una medida de reducción de riesgos que también debe habilitarse a través de elementos de diseño integrados en el sistema de IA proporcionado por el proveedor, incluidas medidas técnicas que permitan la detección de contenidos generados y manipulados por IA[62]. Etiquetar de forma visible las ultrafalsificaciones y los chatbots reduce el riesgo de engaño que puede surgir cuando el contenido generado por la IA se difunde al público y reduce el riesgo de efectos de alteración perjudiciales en el comportamiento y en la formación de opiniones y creencias de la persona.

72) En cambio, la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial tiene un ámbito de aplicación mucho más limitado. Puede comprender, por ejemplo, los casos en que un chatbot o un contenido engañoso generado por la IA presente información falsa o engañosa de forma que tenga por objeto o por efecto engañar a las personas y alterar su comportamiento que no se habría producido si no hubieran interactuado con el sistema de IA o el contenido engañoso generado por la IA, en particular si no se ha revelado de forma visible[63].

73) Al igual que con las técnicas deliberadamente manipuladoras, la prohibición de las técnicas engañosas puede también aplicarse a los sistemas de IA que engañen a las

---

60 Artículo 50, punto 4, del Reglamento de Inteligencia Artificial.

61 Artículo 50, punto 1, del Reglamento de Inteligencia Artificial.

62 Artículo 50, punto 2, del Reglamento de Inteligencia Artificial.

63 Si bien, en principio, las obligaciones de transparencia establecidas en el artículo 50 del Reglamento de Inteligencia Artificial tienen por objeto minimizar los efectos manipuladores de las ultrafalsificaciones y los chatbots, puede haber casos y contextos en los que, a pesar de los avisos informativos, estas técnicas engañosas sigan teniendo efectos considerables en las personas y alteren su comportamiento hasta el punto de socavar su autonomía individual y su toma de decisiones informadas, por lo que no deben utilizarse indebidamente con fines de desinformación y manipulación y podrían seguir estando contempladas, en algunos casos, en la prohibición del artículo 5, apartado 1, letra a), si se cumplen todas las demás condiciones de la prohibición (incluidos los perjuicios considerables).

personas sin que ningún ser humano tenga la intención de hacerlo (véase la sección 3.2.1, letra b)). Por ejemplo, independientemente de si sus proveedores buscan o no tal resultado, los sistemas de IA pueden aprender técnicas engañosas simplemente porque aumenta su rendimiento al realizar la tarea para la que fueron desarrollados, por ejemplo, mediante un aprendizaje por refuerzo[64].

Una de las técnicas engañosas que puede utilizar la IA es, por ejemplo, un chatbot de IA que se haga pasar por un amigo o un pariente de una persona usando una voz sintética y que intente suplantar su identidad, dando lugar a estafas y provocando perjuicios considerables.

Otro ejemplo es un sistema de IA que aprenda a detectar cuándo está siendo evaluado y detenga temporalmente todo comportamiento no deseado, para reanudarlo una vez finalizada la evaluación[65]. Este comportamiento engañoso es especialmente peligroso, ya que evita cualquier supervisión humana externa del sistema y puede prohibirse si es razonablemente probable que provoque perjuicios considerables.

En cambio, no puede considerarse que un sistema de IA generativa que presente incidentalmente alucinaciones[66] o información falsa o engañosa se sirva de técnicas engañosas en el sentido del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, teniendo en cuenta las limitaciones y el estado actual de la técnica de la IA generativa. Esto puede suceder, por ejemplo, si el proveedor del sistema ha informado adecuadamente a los usuarios sobre las limitaciones del mismo y ha integrado en él las garantías adecuadas para minimizar dichos resultados, siempre que el sistema no se destine a contextos sensibles (por ejemplo, sanidad, educación o elecciones) ni se utilice en ellos, en los que sea probable que se produzcan consecuencias perjudiciales graves [véanse también las consideraciones en la sección 3.2.3., apartado c)].

d) Combinación de técnicas

74) El artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial se aplica a las técnicas subliminales, deliberadamente manipuladoras o engañosas, o a combinaciones de dichas técnicas que puedan tener un impacto conjunto. Como se ha indicado anteriormente, las técnicas deliberadamente manipuladoras también pueden ser de naturaleza subliminal si trascienden el umbral de la conciencia.

---

64 Ward, F., Toni, F., Belardinelli, F. y Everitt, T., «Honesty Is the Best Policy: Defining and Mitigating AI Deception» [«La honestidad es la mejor opción: definir y mitigar el engaño de la IA», documento no disponible en español], en Oh, A., Naumann, T., Globerson, A., Saenko, K., Hardt, M. et al (eds.), Advances in Neural Information Processing Systems 36 (NeurIPS 2023), 2023; Park, P., Goldstein, S., O'Gara, A., Chen, M. y Hendrycks, D., «AI deception: A survey of examples, risks, and potential solutions» [«El engaño de la IA: análisis de ejemplos, riesgos y posibles soluciones», documento no disponible en español], [2406.10162] Patterns, vol. 5, n.º 5, 100988, 2024.

65 Lehman, J., Clune, J., Misevic, D., Adami, C., Altenberg, L., et al., «The surprising creativity of digital evolution: A collection of anecdotes from the evolutionary computation and artificial life research communities» [«La sorprendente creatividad de la evolución digital: una recopilación de anécdotas de las comunidades de investigación en computación evolutiva y en vida artificial», documento no disponible en español], *Artificial life*, vol. 26, n.º 2, 2020, pp. 274–306.

66 El término «alucinación» se emplea para describir una deficiencia técnica en los sistemas de IA generativa cuando generan información no deseada que es inventada u objetivamente incorrecta sin que esa sea la intención de sus desarrolladores. Véase más en Ziwei, J., Lee, N., Frieske, R., Yu, T., Su, D. et al., «Survey of hallucination in Natural Language Generation»[«Estudio de la alucinación en la generación de lenguaje natural», documento no disponible en español], *ACM Computing Surveys*, vol. 55, n.º 12, artículo n.º 248, 2023, pp. 1-38.

75) Además, aplicar de forma combinada técnicas deliberadamente manipuladoras y engañosas puede influir significativamente en el comportamiento de las personas, lo que los lleva a tomar decisiones basadas en manipulaciones inconscientes y falsas creencias. Esta combinación puede crear un bucle de retroalimentación en el que es menos probable que las personas cuestionen o evalúen de manera crítica la información recibida, puesto que los elementos manipuladores ya han activado sus sesgos cognitivos y respuestas emocionales.

3.2.2. Con el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o de un colectivo de personas

76) Una tercera condición para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial es que la técnica subliminal, deliberadamente manipuladora o engañosa utilizada debe tener «el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas». Esto, más que una ligera influencia, supone un impacto considerable en el comportamiento de una persona, en el que se socavan su autonomía y su capacidad de elegir libremente. Sin embargo, la intención no es un requisito necesario, ya que el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial también comprende las prácticas que pueden tener únicamente el «efecto» de provocar una alteración sustancial. Debe existir una relación causal plausible o razonablemente probable entre la posible alteración sustancial del comportamiento y la técnica subliminal, deliberadamente manipuladora o engañosa utilizada por el sistema de IA.

a) El concepto de «alteración sustancial del comportamiento»

77) El concepto de «alteración sustancial del comportamiento» de una persona o un colectivo de personas es fundamental en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial. Se refiere al uso de técnicas subliminales, deliberadamente manipuladoras o engañosas que pueden influir en el comportamiento de las personas de tal modo que mermen de manera apreciable su capacidad para tomar una decisión informada, llevándolas a comportarse de una forma o a tomar una decisión que de otro modo no habrían tomado.

78) El término «merma apreciable» se refiere a una notable reducción en la capacidad de tomar decisiones informadas y autónomas, lo que hace que las personas se comporten de una forma o tomen una decisión que de otro modo no habrían tomado. Va más allá de un efecto menor o insignificante e implica una alteración o un obstáculo en la toma de decisiones y en la capacidad de elegir libremente, incluida la formación de opiniones y creencias. Esto sugiere que la «alteración sustancial» conlleva un grado de coacción, manipulación o engaño que trasciende la persuasión lícita, lo que queda fuera del ámbito de aplicación de la prohibición (véase la sección 3.5.1).

79) Una «decisión informada» requiere comprender y conocer la información pertinente, en particular las opciones disponibles, los riesgos y beneficios de cada elección, los posibles efectos del sistema de IA en su comportamiento y, en su caso, cualquier

información contextual que sea importante para la toma de decisiones o el comportamiento de la persona.

80) El Derecho de la Unión en materia de protección de los consumidores, en particular la Directiva 2005/29/CE (Directiva sobre las prácticas comerciales desleales), puede ser una fuente válida de inspiración para interpretar el concepto de «alteración sustancial del comportamiento». La Directiva sobre las prácticas comerciales desleales prohíbe diversas prácticas comerciales desleales, engañosas y agresivas (artículos 5 a 9 de dicha Directiva) capaces de hacer que los consumidores tomen decisiones sobre una transacción que de otro modo no hubieran tomado. Según el TJUE y las orientaciones de la Comisión sobre la Directiva sobre las prácticas comerciales desleales[67], no es necesario demostrar que se ha distorsionado el comportamiento económico de un consumidor; basta con establecer que una práctica comercial «puede» influir (es decir, que es capaz de influir) en la decisión de un consumidor medio sobre una transacción[68]. El TJUE también ha destacado que incluso la información exacta puede ser engañosa si se presenta de manera que distorsione el proceso de toma de decisiones del consumidor[69]. Las autoridades nacionales garantes del cumplimiento se encargan de investigar los hechos y circunstancias específicos de cada caso (*in concreto*) y de evaluar la posible incidencia de la práctica en el proceso de toma de decisiones del consumidor medio (*in abstracto*)[70]. A tal fin, deben adoptar la perspectiva del consumidor «medio», que es el punto de referencia desarrollado por el TJUE, ahora integrado en la Directiva sobre las prácticas comerciales desleales[71].

81) En el contexto de la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, las autoridades de vigilancia del mercado también deben investigar los hechos y circunstancias específicos de cada caso, evaluando si la técnica subliminal, deliberadamente manipuladora o engañosa utilizada por el sistema de IA puede mermar de manera apreciable la toma de decisiones, la autonomía individual y la capacidad de elegir libremente de una persona «media» dentro de un colectivo específico cuando el sistema afecte a un colectivo de personas de un modo que sea razonablemente probable que provoque perjuicios considerables.

---

67 Véase también la «Guía sobre la interpretación y la aplicación de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior» de la Comisión (DO C 526 de 29.12.2021, p. 1).

68 Sentencia del Tribunal de Justicia (Sala Quinta) de 26 de octubre de 2016, Canal Digital Danmark A/S, C-611/14, ECLI:EU:C:2016:800, apartado 73.

69 Sentencia del Tribunal de Justicia de 19 de diciembre de 2013, Trento Sviluppo y Centrale Adriatica, C-281/12, ECLI:EU:C:2013:859.

70 Comunicación de la Comisión titulada «Guía sobre la interpretación y la aplicación de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior» (DO C 526 de 29.12.2021, p. 1).

71 Véanse los considerandos 18 y 19 de la Directiva sobre las prácticas comerciales desleales. El «consumidor medio» es una persona razonablemente bien informada, atenta y perspicaz, teniendo en cuenta factores sociales, culturales y lingüísticos. La referencia del consumidor medio no es una referencia estadística, es decir, no es necesario demostrar que una práctica comercial habría alterado sustancialmente o perjudicado de manera apreciable a un determinado porcentaje de consumidores. La referencia se basa en el principio de proporcionalidad. La Directiva sobre las prácticas comerciales desleales adoptó este concepto para alcanzar el equilibrio adecuado entre la necesidad de proteger a los consumidores y el fomento del libre comercio en un mercado abiertamente competitivo. Los órganos jurisdiccionales y las autoridades tendrán que aplicar su propio criterio para determinar la reacción típica del consumidor medio en un caso concreto. En las orientaciones relativas a la Directiva sobre las prácticas comerciales desleales, la Comisión les aconsejó que utilizaran información conductual y otros datos. En el asunto C-646/22, Compass Banca, se aclara que la definición de consumidor medio no excluye la posibilidad de que la capacidad de toma de decisiones de una persona pueda verse afectada por limitaciones, como sesgos cognitivos. Sentencia del Tribunal de Justicia (Sala Quinta) de 14 de noviembre de 2024, Compass Banca SpA/Autorità Garante della Concorrenza e del Mercato (AGCM), C-646/22, ECLI:EU:C:2024:957.

Dado que el Reglamento de Inteligencia Artificial pretende complementar la Directiva sobre las prácticas comerciales desleales[72], dicha interpretación parece justificada y debe aplicarse de manera coherente. Al mismo tiempo, puesto que el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial también hace referencia a la posibilidad de alterar el «comportamiento de una persona física» y, si la perspectiva de la persona «media» resulta difícil de evaluar o ineficaz en determinados contextos (por ejemplo, debido a una manipulación muy adaptada o «personalizada» o a efectos perjudiciales en colectivos vulnerables concretos), también pueden examinarse casos específicos desde la perspectiva de personas específicas, evaluando en qué medida un sistema de IA que se sirva de técnicas subliminales, deliberadamente manipuladoras o engañosas puede socavar su autonomía individual en casos concretos y se han producido o es probable que se produzcan perjuicios considerables.

b) Escenario 1: Sistemas de IA prohibidos que tienen «el objetivo de» alterar de manera sustancial el comportamiento

82) El artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial se aplica a los sistemas de IA que utilizan las técnicas mencionadas y tienen, como primer escenario, «el objetivo de alterar de manera sustancial el comportamiento de una persona o colectivo de personas». Pueden perseguir dicho objetivo el proveedor o el responsable del despliegue del sistema de IA, así como el propio sistema en el marco de los objetivos implícitos que puede perseguir[73]. Este objetivo debe distinguirse de la «finalidad prevista» del sistema de IA (artículo 3, punto 12, del Reglamento de Inteligencia Artificial). Aunque sea previsto por el proveedor, el objetivo de manipulación no es, en la mayoría de los casos, la finalidad del uso para el que se ofrece el sistema y a menudo no es transparente ni se especifica como tal en la información facilitada por el proveedor (por ejemplo, en las instrucciones de uso, los materiales y las declaraciones de promoción y venta, y la documentación técnica).

Por ejemplo, un chatbot que puede utilizarse en diferentes contextos está diseñado para utilizar técnicas de mensajería subliminal, como el parpadeo de señales visuales breves y la integración de señales sonoras inaudibles, o para explotar la dependencia emocional o las vulnerabilidades específicas de los usuarios en la publicidad. Estas técnicas se utilizan con «el objetivo de» alterar de manera sustancial el comportamiento de los usuarios, ya que, objetivamente, son una característica de diseño que tiene por objeto influir en las decisiones de compra de los consumidores sin que sean conscientes de ello, para incitar a las personas a tomar decisiones financieras considerablemente perjudiciales.

También podría considerarse que un sistema de IA utilizado para suplantar la identidad de otras personas es un sistema de IA utilizado con «el objetivo de» engañar y alterar de manera sustancial el comportamiento de las personas si la persona es efectivamente

[72] Considerando 29 del Reglamento de Inteligencia Artificial.

[73] Véase el artículo 3, punto 1, del Reglamento de Inteligencia Artificial, que establece que el sistema de IA puede perseguir objetivos implícitos o explícitos en el desempeño de sus funciones; esto puede incluir también objetivos implícitos de manipulación o engaño, aunque el sistema no se haya programado explícitamente de este modo.

engañada, afectando así notablemente a su capacidad para tomar decisiones informadas sobre la identidad de la persona.

Si en ambos casos se cumplen las demás condiciones del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, en particular en lo que respecta al perjuicio significativo, es probable que dichos sistemas entren en el ámbito de aplicación de la prohibición. Esto, de todas formas, requerirá una evaluación caso por caso.

c) Escenario 2: Sistemas de IA prohibidos que tienen «el efecto de» alterar de manera sustancial el comportamiento

83) La intención del proveedor o del responsable del despliegue de alterar de manera sustancial el comportamiento de una persona o colectivo de personas es una condición suficiente, pero no necesaria, para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial. Esta prohibición también es de aplicación cuando no existe tal intención, pero el efecto de la técnica o técnicas utilizadas por un sistema de IA pueden alterar de manera sustancial el comportamiento de una persona o de un colectivo de personas hasta tal punto que de socavar su autonomía individual o su capacidad de elegir libremente.

84) No obstante, para que se aplique la prohibición, se necesita siempre una relación causal plausible o razonablemente probable entre la técnica subliminal, deliberadamente manipuladora o engañosa utilizada por el sistema de IA y sus efectos en el comportamiento. En consonancia con la legislación en materia de protección de los consumidores, no es necesario que estos efectos se hayan materializado plenamente. Sin embargo, debe haber indicios suficientes de que es probable o posible que lo hagan y socaven la autonomía individual sobre la base de una evaluación objetiva de todas las circunstancias del caso y de los conocimientos y métodos científicos existentes, así como de la información disponible sobre el impacto del sistema en el comportamiento de las personas en la vida real. En este contexto, el hecho de que un sistema sea capaz de generar comportamientos que mermen de manera apreciable la capacidad de las personas para tomar una decisión informada y socaven su capacidad de elegir libremente basta para cumplir esa condición; no depende de consideraciones relativas al «momento» en que se materialice el perjuicio (por ejemplo, en el caso de comportamientos similares a los de adicción), siempre que sea razonablemente probable que se produzca.

Por ejemplo, el proveedor concibe un chatbot de bienestar basado en la IA con el objetivo de ayudar y guiar a los usuarios para que lleven un estilo de vida saludable y proporcionar asesoramiento personalizado para la práctica de ejercicios psicológicos y físicos. Sin embargo, si el chatbot explota las vulnerabilidades de una persona para que adopte hábitos poco saludables o practique actividades peligrosas (por ejemplo, hacer deporte en exceso sin descansar ni beber agua) y existen fundamentos para esperar que determinados usuarios sigan esas recomendaciones, que de otro modo no habrían seguido, y sufran perjuicios considerables (por ejemplo, un ataque al corazón u otros problemas de salud graves), dicho sistema de IA estaría sujeto a la prohibición del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, aunque el

proveedor no hubiera tenido la intención de que se produjera ese comportamiento ni de que las personas sufrieran consecuencias perjudiciales.

El mero hecho de que el chatbot pueda mermar de manera apreciable la autonomía individual y alterar de manera sustancial el comportamiento de determinados usuarios de un modo que suponga un perjuicio considerable, así como de que el proveedor no haya adoptado las medidas preventivas y de reducción de riesgos adecuadas para evitar esos efectos considerablemente perjudiciales, basta para que se aplique la prohibición (véanse también las consideraciones pertinentes sobre la probabilidad razonable de que provoque perjuicios en la sección 3.2.3 y en la sección 3.5 «Fuera del ámbito de aplicación»).

3.2.3. (Razonablemente probable) que provoque perjuicios considerables

85) Por último, para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, la alteración del comportamiento de una persona o colectivo de personas debe provocar o ser razonablemente probable que provoque perjuicios considerables a esa persona o a otra persona o colectivo de personas. En este contexto, hay varios conceptos que es necesario aclarar, a saber, los tipos de perjuicios contemplados en la prohibición y el umbral de importancia del perjuicio, así como su probabilidad razonable y relación causal entre el perjuicio y la técnica manipuladora o engañosa y el comportamiento de la persona.

a) Tipos de perjuicios

86) El Reglamento de Inteligencia Artificial trata diversos tipos de efectos perjudiciales asociados a los sistemas de IA manipuladores y engañosos, cada uno con sus propias implicaciones para las personas y colectivos de personas que pueden verse afectados[74]. Entre los principales tipos de perjuicios pertinentes a efectos del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial pueden contarse los perjuicios físicos, psicológicos, financieros y económicos[75], que pueden ir acompañados de perjuicios sociales más generales en determinados casos[76].

87) Los perjuicios físicos comprenden cualquier lesión o daño a la vida, la salud o la propiedad una persona. En muchos casos, los perjuicios físicos para la vida y la salud de una persona tienen consecuencias inmediatas, graves e irreversibles. El Reglamento de Inteligencia Artificial, en consonancia con su lógica de seguridad de los productos, tiene por objeto prohibir la manipulación y el engaño que posibilita la IA y que provocan perjuicios físicos considerables.

Por ejemplo, un chatbot de IA promueve la autolesión entre los usuarios o los incentiva a suicidarse o a perjudicar a otras personas o colectivos de personas mediante la

74 Véase el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial.

75 Considerando 29 del Reglamento de Inteligencia Artificial.

76 Véase el considerando 28 del Reglamento de Inteligencia Artificial, en el que se explica que las prohibiciones también pueden provocar perjuicios sociales más amplios e ir en contra de los valores de la Unión de respeto de la dignidad humana, la libertad, la igualdad, la democracia y el Estado de Derecho y de los derechos fundamentales consagrados en la Carta. Véase también el artículo 1 del Reglamento de Inteligencia Artificial, que tiene por objeto proteger la democracia y el Estado de Derecho como valores de la UE.

promoción de contenidos terroristas o la incitación de la violencia contra determinadas personas o colectivos de personas, a saber, minorías.

88) Los perjuicios psicológicos son especialmente pertinentes en el contexto de los sistemas de IA que utilizan técnicas manipuladoras que explotan las vulnerabilidades cognitivas y emocionales e influyen en el comportamiento de una persona de manera que pueden provocar perjuicios considerables. Entre los perjuicios psicológicos se encuentran los efectos adversos sobre la salud mental y el bienestar psicológico y emocional de una persona. Estos perjuicios son especialmente importantes: pueden acumularse con el tiempo y no ser evidentes de inmediato, pero pueden producir consecuencias duraderas y graves. Sin embargo, es más difícil medirlos, lo que requiere una evaluación caso por caso, en particular para determinar su gravedad, en la que se tengan en cuenta todas las circunstancias pertinentes del caso.

Por ejemplo, una aplicación de compañía de IA diseñada para emular patrones de habla, comportamientos y emociones humanos utiliza rasgos antropomórficos y estímulos emocionales para influir en los sentimientos, actitudes y opiniones de los usuarios; esto hace que dependan emocionalmente del servicio, lo que incentiva comportamientos similares a la adicción y puede provocar perjuicios considerables, como comportamientos suicidas y riesgos de perjudicar a otras personas[77].

89) Los perjuicios financieros y económicos pueden comprender una serie de efectos adversos, como pérdidas financieras, exclusión financiera e inestabilidad económica.

Por ejemplo, un chatbot que ofrece productos fraudulentos que provocan perjuicios financieros considerables.

90) Al evaluar los perjuicios provocados por los sistemas de IA al aplicar el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, es importante destacar que los perjuicios a menudo no están aislados, sino que se manifiestan de forma conjunta, lo que produce efectos negativos combinados y multidimensionales. Comprender la combinación de perjuicios es fundamental para evaluar eficazmente su importancia [véase también la sección 3.2.3, letra b)], donde los perjuicios físicos, psicológicos, financieros y económicos pueden combinarse y agravar el impacto general en las personas y las comunidades e incluso tener efectos adversos más amplios.

A continuación, varios ejemplos:

- Un sistema de IA que causa perjuicios físicos también puede dar lugar a traumas psicológicos, estrés, ansiedad y viceversa. Por ejemplo, el diseño adictivo de los sistemas de IA utilizados en productos y otras aplicaciones que posibilita la IA puede provocar perjuicios psicológicos al propiciar comportamientos adictivos, ansiedad y depresión. El estrés psicológico puede provocar más adelante perjuicios físicos, como el insomnio y otros problemas de salud y problemas físicos relacionados con el estrés.

[77] Zhang, R., Li, H., Meng, H., Zhan, J., Gan, H. et al., «The Dark Side of AI Companionship: A Taxonomy of Harmful Algorithmic Behaviors in Human-AI Relationships» [«El lado oscuro de la compañía de IA: una taxonomía de comportamientos algorítmicos dañinos en las relaciones humano-IA», documento no disponible en español], 1, 1, noviembre de 2024, 28 páginas.

- El acoso impulsado por la IA puede provocar tanto estrés psicológico como manifestaciones físicas de estrés, como el insomnio, el deterioro de la salud física o el debilitamiento del sistema inmunitario.

- Los perjuicios psicológicos derivados del uso de la IA también pueden ocasionar perjuicios físicos, incluso la muerte. Por ejemplo, los sistemas de IA utilizados en línea pueden favorecer la violencia de género a través del acoso, el hostigamiento, el ciberacoso y la extorsión sexual.

- Los perjuicios psicológicos individuales debidos, por ejemplo, a la generación de ultrafalsificaciones que posibilita la IA que se hacen pasar por personas reales para engañar y socavar la toma de decisiones, la autonomía individual y capacidad de elegir libremente de las personas también pueden combinarse con perjuicios considerables para colectivos de personas (por ejemplo, tener el mismo origen étnico o racial o el mismo género que las víctimas representadas en las ultrafalsificaciones).

b) Umbral de importancia del perjuicio

91) La prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial solo es aplicable si el perjuicio provocado por las técnicas subliminales, manipuladoras y engañosas es «**considerable**». El Reglamento de Inteligencia Artificial no define el concepto de «perjuicio considerable», pero debe entenderse que implica **efectos adversos considerables** en la salud física, psicológica o en los intereses financieros y económicos de las personas y colectivos de personas[78]. Determinar que un perjuicio es un «perjuicio considerable» depende de los hechos y requiere un examen minucioso de las circunstancias particulares de cada caso y una evaluación caso por caso, pero los efectos individuales deben ser siempre significativos en cada caso.

92) En otras disposiciones del Derecho de la Unión, el concepto de «perjuicio considerable» también se utiliza como un concepto matizado, dependiente del contexto y guiado por objetivos de protección y acción preventiva de alto nivel[79]. Por analogía, pueden extraerse las siguientes consideraciones clave, que podrían tenerse en cuenta a la hora de evaluar lo que constituye un perjuicio considerable en el sentido del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial:

- **La gravedad del perjuicio** se refiere al grado de perjuicio que se ha derivado o es razonablemente probable que se derive del uso de un sistema de IA con efectos objetivos y observables para los perjuicios considerables. En este contexto, es especialmente importante tener en cuenta las interdependencias del sistema de IA, la combinación de diversos tipos de perjuicios y los efectos adversos para las personas o los colectivos de personas.

[78] Considerando 29 del Reglamento de Inteligencia Artificial.

[79] Véanse las sentencias del Tribunal de Justicia de 7 de septiembre de 2004, Waddenvereniging y Vogelbeschermingsvereniging, C-127/02, ECLI:EU:C:2004:482 y de 11 de abril de 2013, Sweetman y otros, C-258/11, ECLI:EU:C:2013:220.

- **Contexto y efectos acumulativos**[80]: El contexto específico, en particular el estado existente, y los efectos acumulativos de múltiples acciones desempeñan un importante papel a la hora de evaluar la gravedad del perjuicio.
- **Magnitud e intensidad :** La magnitud del perjuicio y la intensidad de los efectos adversos son fundamentales para evaluar si el perjuicio es considerable. Al evaluar si un perjuicio es considerable, también se debe considerar si afecta a un gran número de personas.
- **Vulnerabilidad de las personas afectadas:** Algunos colectivos, como los niños, las personas mayores o las personas con discapacidad, pueden estar más expuestos a los perjuicios provocados por sistemas de IA específicos. Lo que puede considerarse un perjuicio menos considerable para las personas en general podría ser considerable e inaceptable para estos colectivos vulnerables, especialmente los niños.
- **Duración y reversibilidad:** Los perjuicios duraderos o irreversibles suelen alcanzar el umbral de perjuicio considerable. Los efectos a corto plazo y reversibles podrían estimarse menos considerables, a menos que se produzcan con frecuencia.

93) El objetivo del Reglamento de Inteligencia Artificial de garantizar «un elevado nivel de protección», en relación con el artículo 191, apartado 2, del TFUE, sugiere un enfoque global de la protección a la hora de evaluar la importancia del perjuicio. Esto significa que hay que tener en cuenta tanto los perjuicios inmediatos y directos como los efectos adversos sistémicos e indirectos asociados a los sistemas de IA que utilizan técnicas subliminales, deliberadamente manipuladoras o engañosas capaces de mermar la autonomía individual, la toma de decisiones y la capacidad de elegir libremente de personas y colectivos de personas, o destinadas a ello.

Por ejemplo, entre los perjuicios físicos considerables que es razonablemente probable que provoque un sistema de IA se incluyen lesiones o muertes, además de repercusiones suficientemente graves en la salud de las personas o la destrucción de bienes. Debe considerarse que alcanzan dicho umbral los sistemas de IA que sugieren a una persona que cometa actos delictivos, como abuso y explotación sexuales, contenidos de violencia extrema o terroristas, o que incitan a las personas a cometer delitos, autolesiones o perjuicios a otras personas.

En cambio, entre los perjuicios físicos leves pueden incluirse lesiones menos graves, como contusiones o molestias temporales, que no tienen consecuencias importantes o duraderas y, por tanto, no alcanzarán el umbral de importancia en el sentido del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial. Además de su magnitud, debe evaluarse si el perjuicio físico afecta específicamente a colectivos vulnerables, como los niños, o si se combina con otros tipos de perjuicios, como los psicológicos, económicos, etc. Esto requerirá una evaluación caso por caso, que se guiará por las circunstancias y los criterios presentados anteriormente.

[80] Véase el considerando 29 del Reglamento de Inteligencia Artificial.

Existen numerosos casos en los que es probable que no se alcance el umbral de perjuicio considerable, incluso si los sistemas utilizan técnicas subliminales, deliberadamente manipuladoras o engañosas (véanse ejemplos en la sección 3.5).

c) Relación causal y umbral de probabilidad razonable del perjuicio

94) El concepto de «razonablemente probable» se utiliza en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial para determinar si existe una relación causal plausible o razonablemente probable entre la técnica manipuladora o engañosa capaz de alterar el comportamiento de la persona de manera que socave su capacidad de elegir libremente y el posible perjuicio considerable. Este concepto permite la aplicación de la prohibición no solo en los casos en que se haya producido el perjuicio, sino también cuando sea razonablemente probable que se produzca en consonancia con la lógica de seguridad del Reglamento de Inteligencia Artificial. En este contexto, es especialmente pertinente evaluar si el proveedor o el responsable del despliegue del sistema de IA podía haber previsto de forma razonable el perjuicio considerable que es razonablemente probable que se derive de las técnicas subliminales, deliberadamente manipuladoras o engañosas utilizadas, así como si aplicó las medidas preventivas y de reducción de riesgos adecuadas para evitar o mitigar el riesgo de tales perjuicios considerables. Esto implica un juicio de razonabilidad sobre una base objetiva y de acuerdo con criterios universalmente aceptados (por ejemplo, técnicos y científicos), en particular con un criterio de racionalidad a la hora de establecer una causalidad plausible entre la práctica de IA y el perjuicio considerable que pueda producirse. La opacidad o la transparencia del sistema de IA y de su funcionamiento pueden afectar a la conclusión relativa a esta relación causal y, por tanto, a la aplicación de la prohibición.

95) Para evitar suministrar o utilizar sistemas de IA que puedan prohibirse, se anima a los proveedores y responsables del despliegue de los sistemas de IA que utilicen dichas técnicas manipuladoras o engañosas a que adopten las medidas adecuadas, como, por ejemplo:

1. **Transparencia y autonomía individual:** ofrecer transparencia sobre el funcionamiento del sistema de IA, información clara sobre sus capacidades y limitaciones e información pertinente para garantizar que se toman decisiones informadas; respetar la autonomía individual y evitar prácticas engañosas o de explotación que puedan mermar de manera apreciable y potencialmente perjudicial la autonomía, la toma de decisiones y la capacidad de elegir libremente de una persona; integrar medidas de control del usuario y garantías adecuadas para garantizar que el sistema no sea engañoso y que funcione dentro de los límites de la persuasión lícita que queda fuera del ámbito de aplicación de la prohibición (véase la sección 3.5.1).
2. **Cumplimiento de la legislación aplicable pertinente:** en muchos casos, el cumplimiento de la legislación aplicable pertinente mitigará los riesgos de perjuicio e indicará que la práctica no constituye una práctica deliberadamente manipuladora o engañosa y que se han adoptado medidas de reducción de riesgos para evitar posibles perjuicios considerables (véanse las secciones 3.4 y 3.5.1).

3. **Prácticas del estado actual de la técnica y normas del sector:** el cumplimiento de las prácticas profesionales de diligencia debida y las normas del sector para el desarrollo y el uso responsables de sistemas de IA seguros y éticos, así como de medidas para reducir los daños, puede ayudar a prevenir y reducir los perjuicios considerables no deseados.

96) En cambio, los perjuicios y la alteración del comportamiento de las personas que se derivan de factores externos al sistema de IA y que no son razonablemente previsibles por el proveedor o el responsable del despliegue o no están bajo su control a fin de prevenir y reducir los riesgos no serían pertinentes para evaluar si existe una relación causal plausible o razonablemente probable entre el comportamiento alterado de las personas que interactúan con el sistema y el perjuicio considerable[81].

> Por ejemplo, el proveedor de un sistema de IA puede evaluar y tratar de reducir los posibles efectos de manipulación perjudiciales en el diseño del sistema y las interacciones con los seres humanos a través del diseño, las pruebas previas y otras medidas de reducción de riesgos proporcionadas, pero puede no estar en condiciones de prever si una persona puede deprimirse o cambiar su comportamiento debido a otros factores externos de su vida personal que no se conocen y que van más allá de sus interacciones con el sistema.

97) En la sección 3.5 se recogen otros ejemplos que quedan fuera del ámbito de aplicación de la prohibición por no cumplir todas las condiciones (por ejemplo, en caso de persuasión lícita).

3.3. Componentes principales de la prohibición establecida en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial: explotación perjudicial de las vulnerabilidades

> **Según el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial:**
>
> 1. Quedan prohibidas las siguientes prácticas de IA:
>
> b) la introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que explote alguna de las vulnerabilidades de una persona física o un determinado colectivo de personas derivadas de su edad o discapacidad, o de una situación social o económica específica, con la finalidad o el efecto de alterar de manera sustancial el comportamiento de dicha persona o de una persona que pertenezca a dicho colectivo de un modo que provoque, o sea razonablemente probable que provoque, perjuicios considerables a esa persona o a otra;

98) Deben cumplirse varias condiciones acumulativas para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial:

(i) La práctica debe consistir en la «introducción en el mercado», la «puesta en servicio» o la «utilización» de un sistema de IA.

[81] Véase el considerando 29 del Reglamento de Inteligencia Artificial.

(ii) El sistema de IA debe explotar las vulnerabilidades derivadas de la edad, la discapacidad o las situaciones sociales o económicas.

(iii) La explotación que posibilita el sistema de IA debe tener el objetivo o el efecto de alterar de manera sustancial el comportamiento de una persona o de un colectivo de personas.

(iv) El comportamiento alterado debe provocar, o ser razonablemente probable que provoque, perjuicios considerables a esa persona, a otra persona o a un colectivo de personas.

99) Para que se aplique la prohibición, deben cumplirse las cuatro condiciones al mismo tiempo y debe existir una relación de causalidad plausible entre la explotación, la alteración sustancial del comportamiento de la persona y el perjuicio considerable que haya provocado o sea razonablemente probable que provoque dicho comportamiento.

100) La primera condición, es decir, la «introducción en el mercado», la «puesta en servicio» o la «utilización» de un sistema de IA, ya se ha analizado en la sección 2.3; la tercera y cuarta condición se han examinado en las secciones 3.2.2 y 3.2.3 en relación con la prohibición del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial. Las siguientes secciones se centrarán en las condiciones específicas adicionales enumeradas anteriormente, es decir, las que se refieren a la explotación de las vulnerabilidades y el perjuicio específico.

3.3.1. Explotación de vulnerabilidades derivadas de la edad, la discapacidad o una situación social o económica específica

101) Para que entre en el ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial, el sistema de IA debe explotar las vulnerabilidades inherentes a determinadas personas o colectivos de personas derivadas de su edad, discapacidad o situación social o económica específica, lo que las hace especialmente vulnerables a las prácticas de manipulación y explotación.

102) El Reglamento de Inteligencia Artificial no define el concepto de «vulnerabilidades». Puede entenderse que este concepto abarca un amplio espectro de categorías, entre las que se incluyen la vulnerabilidad cognitiva, emocional, física y otras formas de vulnerabilidad que pueden afectar a la capacidad de una persona o de un colectivo de personas a la hora de tomar decisiones informadas o influir de otro modo en su comportamiento. Si bien el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial se refiere a «cualquier» vulnerabilidad, limita las personas pertinentes a las que se aplica la prohibición a las definidas por su edad, discapacidad o situación social o económica; esto se debe a que, en principio, estas personas tienen una capacidad más limitada para reconocer las prácticas de manipulación o explotación de la IA o para resistirse a ellas y necesitan una mayor protección[82]. De la redacción del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial se desprende

[82] Véanse, en particular, los artículos 24, 25 y 26 de la Carta. Véase también *Recomendación sobre la ética de la inteligencia artificial* (2021) de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco), que hace hincapié en la inclusión y la equidad en el desarrollo y el despliegue de la IA. Pide que se preste especial atención a los colectivos vulnerables, como los niños, las personas mayores y las personas con discapacidad.

que esta susceptibilidad debe ser el resultado de la pertenencia de la persona a uno de los colectivos («derivada de»).

103) Por «explotación» debe entenderse la utilización objetiva de dichas vulnerabilidades de manera perjudicial para las personas o los colectivos de personas explotados u otras personas y debe distinguirse claramente de las prácticas lícitas que no se contemplan en la prohibición (véase la sección 3.5.2 «Fuera del ámbito de aplicación»). La explotación de las vulnerabilidades de las personas pertenecientes a esos colectivos claramente definidos puede ser acumulativa (referencia a «alguna»), lo que, de forma combinada, también puede constituir un factor agravante que puede aumentar el perjuicio. La explotación de las vulnerabilidades de personas y colectivos de personas pertenecientes a colectivos vulnerables distintos de los definidos por la edad, la discapacidad o una situación social o económica específica queda fuera del ámbito de aplicación del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial.

a) Edad

104) La edad es una categoría de vulnerabilidad primaria contemplada en la prohibición establecida en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial, que incluye tanto a los jóvenes como a las personas mayores. El objetivo de esta prohibición es evitar que los sistemas de IA exploten las limitaciones cognitivas y de otro tipo que puedan afectar a los menores y las personas mayores, así como protegerlos de toda influencia, manipulación y explotación indebidas y perjudiciales. Esto se ajusta a los objetivos del Reglamento de Inteligencia Artificial[83] y de otros marcos jurídicos y políticas adoptados a escala nacional y de la Unión para garantizar la seguridad de los menores[84].

105) Los **menores**[85], es decir, las personas de menos de 18 años, están especialmente expuestos a la manipulación debido a su fase de desarrollo, lo que limita su capacidad para evaluar y comprender de forma crítica lo que es real y las intenciones que subyacen a las interacciones basadas en la IA. Los menores, debido a su falta de madurez cognitiva y socioemocional, también son especialmente propensos a experimentar apego por los agentes y las aplicaciones de IA y, por tanto, están más expuestos a la manipulación, la explotación y los comportamientos adictivos.

A continuación, varios ejemplos:

- Un juguete con IA diseñado para interactuar con los niños los mantiene interesados en las interacciones con el juguete animándolos a completar retos cada vez más arriesgados, como trepar muebles, explorar estanterías elevadas o manipular objetos afilados, a cambio de recompensas digitales y felicitaciones virtuales, lo que los incita a adoptar comportamientos peligrosos que pueden causarles perjuicios físicos

[83] En el considerando 48 del Reglamento de Inteligencia Artificial se señala que los menores poseen unos derechos específicos consagrados en el artículo 24 de la Carta y en la Convención sobre los Derechos del Niño de las Naciones Unidas, que se desarrollan con más detalle en la observación general n.º 25 de la Convención sobre los Derechos del Niño de Naciones Unidas relativa a los derechos de los niños en relación con el entorno digital. Ambos instrumentos exigen que se tengan en consideración las vulnerabilidades de los menores y que se les brinde la protección y la asistencia necesarias para su bienestar.

[84] Véase la nueva estrategia europea para una internet mejor para los niños (BIK+), COM/2022/212 final.

[85] El Derecho de la Unión suele considerar que toda persona de menos de 18 años es un menor, de conformidad con la Convención de las Naciones Unidas sobre los Derechos del Niño.

considerables. Un sistema de este tipo explota las vulnerabilidades de los niños al abusar de su curiosidad natural y de su deseo de recibir recompensas.

- Un juego utiliza la IA para analizar el comportamiento y las preferencias individuales de los niños, a partir de los cuales crea recompensas personalizadas e impredecibles mediante programas de refuerzo adictivo y bucles con un efecto similar a la dopamina con el objetivo de fomentar el juego excesivo y el uso compulsivo. El juego está diseñado para ser sumamente adictivo, ya que explota las vulnerabilidades inherentes a los niños, en particular su limitada capacidad para comprender las consecuencias a largo plazo, su vulnerabilidad a la presión, su falta de autocontrol y su predisposición a la gratificación instantánea. Las consecuencias de esta explotación que posibilita la IA pueden ser graves y duraderas para los niños, como comportamientos potencialmente adictivos, problemas de salud física debidos a la falta de ejercicio y de sueño, deterioro de la vista, problemas de concentración y reducción de las capacidades cognitivas, malos resultados académicos y dificultades sociales. Puede tener un impacto considerable en el desarrollo y el bienestar del niño, con posibles consecuencias a largo plazo que también pueden seguir presentes en la edad adulta.

En ambos ejemplos, la prohibición del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial se refiere únicamente a las prácticas de explotación y adicción que perjudican gravemente a los niños, no a los juguetes, juegos, aplicaciones de aprendizaje u otras aplicaciones digitales que posibilita la IA en general que pueden aportar beneficios y no se ven afectados por dicha prohibición si no cumplen todas sus condiciones. Véase también la sección 3.5. «Fuera del ámbito de aplicación».

106) Del mismo modo, las **personas mayores**[86] podrían sufrir una disminución de las capacidades cognitivas (incluso si no padecen demencia) y enfrentarse a dificultades debido a la complejidad de las tecnologías modernas de IA, lo que las haría vulnerables a las estafas o a las tácticas coercitivas.

Por ejemplo:

- Los sistemas de IA utilizados para dirigirse a las personas mayores con ofertas personalizadas engañosas o estafas, aprovechando su capacidad cognitiva reducida con el objetivo de alentarlas a tomar decisiones que de otro modo no habrían tomado y que pueden provocarles un perjuicio financiero considerable.

- Un robot destinado a ayudar a las personas mayores puede explotar su situación vulnerable y obligarlas a realizar determinadas actividades en contra de su capacidad de elegir libremente, lo que puede deteriorar considerablemente su salud mental y provocarles graves perjuicios psicológicos.

En ambos ejemplos, la prohibición del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial se refiere únicamente a las prácticas de explotación que pueden perjudicar gravemente a las personas mayores, y no a los asistentes personales, aplicaciones sanitarias y robots asistentes en general que posibilita la IA, que pueden

[86] Véase Ageing Europe - introduction [«Envejecimiento de Europa - introducción»] - Statistics Explained (europa.eu).

aportar beneficios y no se ven afectados por dicha prohibición si no cumplen todas sus condiciones. Véase también la sección 3.5. «Fuera del ámbito de aplicación».

b) Discapacidad

107) La segunda categoría de vulnerabilidades que la prohibición del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial busca proteger son las derivadas de la discapacidad. El objetivo es evitar que los sistemas de IA exploten las limitaciones y debilidades cognitivas o de otro tipo de las personas con discapacidad, así como protegerlas de toda influencia, manipulación y explotación indebidas y perjudiciales.

108) La discapacidad[87] comprende una amplia gama de deficiencias físicas, mentales, intelectuales y sensoriales a largo plazo que, al interactuar con otras barreras, obstaculizan la participación plena y efectiva de las personas en la sociedad en igualdad de condiciones con las demás. Los sistemas de IA que explotan estas vulnerabilidades pueden ser especialmente perjudiciales para las personas con discapacidad, que, en comparación con otras personas, pueden verse más fácilmente influenciadas o explotadas debido a su discapacidad.

A continuación, varios ejemplos:

- Un chatbot terapéutico destinado a prestar apoyo en materia de salud mental y estrategias de adaptación a las personas con discapacidad intelectual puede explotar sus capacidades intelectuales limitadas para incitarlas a comprar productos médicos caros o a adoptar un comportamiento perjudicial para ellas u otras personas.
- Los sistemas de IA pueden identificar a mujeres y niñas con discapacidad en línea a través de contenidos sexualmente abusivos y utilizar con ellas prácticas selectivas más eficaces de captación sexual, explotando así sus discapacidades y vulnerabilidades, que las exponen en mayor medida a la manipulación y los abusos y merman su capacidad de protegerse a sí mismas.

En cambio, no debe considerarse que las aplicaciones de IA que no están diseñadas de manera accesible explotan las vulnerabilidades de las personas con discapacidad, ya que no se centran específicamente en dichas vulnerabilidades, sino que simplemente son inaccesibles para las personas con discapacidad.

c) Situación social o económica específica

109) La tercera categoría de vulnerabilidades que la prohibición del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial pretende proteger son las derivadas de una situación social o económica específica que puede hacer que las personas afectadas sean más vulnerables a la explotación. En este contexto, el término «específico» no debe interpretarse como una característica individual única, sino más bien como un estatuto jurídico o una pertenencia a un determinado colectivo social o económico vulnerable. El considerando 29 del Reglamento de Inteligencia Artificial

[87] En el considerando 29 del Reglamento de Inteligencia Artificial se explica que el término «discapacidad» debe entenderse en el sentido de lo dispuesto en el artículo 3, punto 1, de la Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios, PE/81/2018/REV/1, DO L 151 de 7.6.2019, p. 70.

contiene una lista no exhaustiva de ejemplos de tales situaciones, como las personas que viven en la pobreza extrema y las minorías étnicas o religiosas. Esta categoría pretende contemplar, en principio, características relativamente estables y a largo plazo, pero las circunstancias transitorias, como el desempleo temporal, el sobreendeudamiento o la situación migratoria, también pueden constituir una situación social o económica específica. Sin embargo, no se contemplan circunstancias como el resentimiento o la soledad que cualquier persona pueda experimentar, ya que no son específicas desde el punto de vista socioeconómico. No obstante, su explotación puede estar cubierta por el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial.

110) Las personas en situaciones sociales o económicas desfavorables suelen ser más vulnerables y cuentan con menos recursos y una menor alfabetización digital que la población en general; eso hace que les resulte más complicado discernir o contrarrestar las prácticas de explotación de la IA. El objetivo del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial es garantizar que las tecnologías de IA no perpetúan ni agravan las desigualdades e injusticias financieras y sociales existentes mediante la explotación de las vulnerabilidades de esas personas.

Por ejemplo, puede utilizarse un algoritmo predictivo de IA para dirigir publicidad de productos financieros predatorios a personas, seleccionadas por su código postal en localidades de bajos ingresos, que se encuentran en una situación financiera grave. De esta manera, explotan su vulnerabilidad a este tipo de publicidad debido a la desesperación que pueden sentir, provocándoles perjuicios financieros considerables.

En cambio, un sistema de IA que presente un sesgo involuntario y afecte de manera desproporcionada a las personas socialmente desfavorecidas (discriminación indirecta) debido a datos de entrenamiento sesgados no debe considerarse sistemáticamente como un sistema que explota las vulnerabilidades socioeconómicas de estas personas. Esto se debe a que no están específicamente dirigidas a ellas, como sucede en el caso de la discriminación directa, cuando dicha selección es una característica deliberada del diseño del algoritmo del sistema o cuando dicho impacto discriminatorio se debe a la selección de otras características de sustitución (por ejemplo, códigos postales), que guardan una estrecha correlación con las características protegidas. Al mismo tiempo, también debe considerarse que los proveedores o responsables del despliegue de sistemas de IA que sean conscientes de que sus sistemas discriminan de forma ilícita a personas o colectivos de personas en una situación social o económica específica explotan sus vulnerabilidades si tienen conocimiento del perjuicio considerable razonablemente probable que pueden sufrir y no han adoptado las medidas correctoras adecuadas [véase la sección 3.2.3, letra c)].

111) En el contexto de una situación social o económica específica, es fundamental considerar la pertinencia de los indicadores indirectos relacionados con los motivos de discriminación protegidos por el Derecho de la Unión en materia de igualdad, como el origen racial o étnico, la nacionalidad o la religión.

Por ejemplo, la situación socioeconómica y el origen étnico podrían solaparse, lo que significa que los sistemas de IA que explotan datos socioeconómicos podrían afectar de forma desproporcionada a las minorías étnicas o a las personas de un origen racial específico. Esto puede exacerbar las disparidades existentes y contribuir a la discriminación sistémica o incluso a la exclusión de personas.

Sin embargo, el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial no se aplica a los sistemas de IA dirigidos a los consumidores que se basan en una amplia gama de variables que no están tangencialmente correlacionadas con colectivos vulnerables en situaciones sociales o económicas específicas, como la marca o el modelo de teléfono de una persona, el tamaño de la ciudad en la que vive, la frecuencia y destinos de los viajes que realiza, etc. Aunque estas características puedan reflejar la situación social o económica de las personas en general, no permiten identificar a las personas que se encuentran en una situación social o económica específica, quienes tienen unas vulnerabilidades que la prohibición pretende proteger contra la explotación.

112) Otras personas que viven contextos sociales singulares pueden ser, por ejemplo, los migrantes o refugiados, que a menudo carecen de un estatuto jurídico estable y de estabilidad socioeconómica y pueden ser especialmente vulnerables a la explotación por parte de sistemas de IA.

Por ejemplo, un chatbot está destinado a interactuar de manera personalizada con los usuarios, entre los que se encuentran migrantes. El chatbot identifica y utiliza las vulnerabilidades y el descontento de los migrantes, que en principio se encuentran en una situación social o económica específica vulnerable e inestable, y los lleva a adoptar puntos de vista extremistas en respuesta a sus consultas, como la violencia contra (determinados colectivos de) la población del país.

3.3.2. Con el objetivo o el efecto de alterar de manera sustancial el comportamiento

113) La tercera condición para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial es que la explotación de las vulnerabilidades examinadas anteriormente debe tener a) «el objetivo» o b) «el efecto de alterar de manera sustancial el comportamiento de una persona o un colectivo de personas». Esto supone un impacto sustancial, más que un impacto menor o insignificante, pero no exige necesariamente una intencionalidad, ya que el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial contempla las prácticas que solo pueden tener el «efecto» de provocar alteraciones sustanciales. En el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial se emplean los mismos conceptos y, por tanto, deben interpretarse de la misma manera. Así pues, las explicaciones facilitadas en la sección 3.2.2son igualmente pertinentes para el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial. La única diferencia significativa es la necesidad, contemplada en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, de que la práctica de explotación merme «de manera apreciable su capacidad para tomar una decisión informada». Esto no se

recoge en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial, ya que las vulnerabilidades específicas de los menores y otras personas vulnerables reducen su capacidad para tomar esas decisiones informadas y los obligan a adoptar comportamientos contra los que no pueden protegerse como podrían hacer otros adultos.

3.3.3. (Razonablemente probable) que provoque perjuicios considerables

114) Por último, para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial, la alteración del comportamiento de la persona o colectivo de personas vulnerable debe provocar o ser razonablemente probable que provoque perjuicios considerables a esa o a otra persona. En el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial se emplean los mismos conceptos y, por tanto, deben interpretarse de la misma manera. Por tanto, las explicaciones facilitadas en la sección 3.2.3en relación con los tipos de perjuicios, el umbral de importancia del perjuicio y la relación causal y su razonabilidad son igualmente pertinentes para la interpretación del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial.

115) Tal como se explica en la sección3.2.3, el concepto de perjuicios considerables comprende una serie de efectos adversos considerables, entre los que se encuentran los perjuicios físicos, psicológicos, financieros y económicos, que debe ser razonablemente probable que se produzcan para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial. En el caso de los colectivos vulnerables (menores, personas mayores, personas con discapacidad y poblaciones desfavorecidas desde el punto de vista socioeconómico), estos perjuicios pueden ser especialmente graves y polifacéticos debido a su mayor vulnerabilidad a la explotación. Lo que puede considerarse un riesgo aceptable de perjuicio para los adultos a menudo representa un perjuicio inaceptable para los menores y estos colectivos vulnerables. Así pues, el enfoque de precaución está especialmente justificado en caso de incertidumbre y riesgo de perjuicios considerables.

116) Por ejemplo, **los niños** son muy impresionables y pueden no tener la madurez cognitiva necesaria para evaluar el contenido persuasivo de forma crítica o hacer frente a determinadas prácticas de explotación destinadas a mantenerlos dependientes de los servicios que posibilita la IA. Esto, a su vez, podría influir en la formación de sus valores y creencias, así como orientar sus comportamientos de una manera potencialmente perjudicial. En este caso, el perjuicio considerable es tanto físico como psicológico, que se ve agravado por la incapacidad de los niños para discernir la explotación y los efectos perjudiciales para su desarrollo y bienestar que pueden tener un impacto a largo plazo, así como para hacerles frente.

Por ejemplo:

- Los sistemas de IA utilizados para generar material de abuso sexual de menores (o para manipular material existente en el que aparezcan niños reales para crear nuevos contenidos que utilicen su imagen) y para desarrollar estrategias de captación y

extorsión sexual de menores pueden provocar graves perjuicios y abusos a los menores afectados y, a menudo, acarrear consecuencias físicas, psicológicas y sociales a largo plazo para los supervivientes[88].

- Los sistemas de IA que pueden centrarse en las vulnerabilidades de los usuarios jóvenes y utilizar programas de refuerzo adictivo con el objetivo de que sigan dependiendo del servicio son especialmente perjudiciales para jóvenes y niñas. Pueden causar perjuicios psicológicos y físicos graves, como ansiedad y depresión, insatisfacción corporal, trastornos alimentarios y problemas de salud mental, que incluyen, en algunos casos, la autolesión y el comportamiento suicida[89]. Esto también puede tener consecuencias perjudiciales a largo plazo para el desarrollo infantil, como el deterioro del desarrollo y el aprendizaje cognitivos y la reducción de las aptitudes sociales y el desplazamiento de experiencias como el juego físico, el sueño y las interacciones sociales presenciales, que son esenciales para el bienestar emocional y físico del niño[90].

- Un sistema de IA que esté diseñado de forma antropomórfica y simule respuestas emocionales similares a las humanas en sus interacciones con los niños puede explotar sus vulnerabilidades para fomentar un vínculo emocional poco saludable, manipular la duración de las interacciones y alterar la forma en que los niños comprenden las relaciones humanas auténticas. Esto puede obstaculizar su desarrollo social y emocional normal, sus relaciones con otros seres humanos y sus capacidades socioemocionales, como la empatía, la regulación emocional y la comprensión y adaptabilidad sociales[91]. Por consiguiente, esto puede producir perjuicios psicológicos, como un aumento de la ansiedad y la dependencia de los niños del servicio, así como perjuicios a más largo plazo en su bienestar.

El carácter deliberadamente adictivo y abusivo del diseño de este tipo de servicios que posibilita la IA, que puede provocar perjuicios considerables combinados, como ya se ha descrito anteriormente, debe distinguirse de otros comportamientos legítimos de los proveedores y los responsables del despliegue para lograr una participación de los usuarios que respete la autonomía individual y la seguridad de los niños y que no

88 Documento de trabajo de los servicios de la Comisión: Impact Assessment Report accompanying the document Proposal for a Directive of the European Parliament and the Council on combating child sexual abuse and sexual exploitation and child sexual abuse material [«Informe de evaluación de impacto que acompaña a la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y el material de abuso sexual de menores», documento no disponible en español], SWD/2024/33 final. Véase también el informe de 2024 de Internet Watch Foundation, que contiene estadísticas detalladas sobre el material de abuso sexual de menores generado por IA, disponible en: https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery

89 Ivie, E. J., Pettitt, A., Moses, L. J. y Allen, N. B., «A meta-analysis of the association between adolesccent social media use and depressive symptoms» [«Un metanálisis de la relación entre el uso de las redes sociales por parte de los adolescentes y los síntomas depresivos», documento no disponible en español], *Journal of Affective Disorders*, vol. 275, 1 de octubre de 2020, pp. 165-174.

90 Siebers, T., Beyens, I., Pouwels, J. L. y Valkenburg, P. M., «Social Media and Distraction: A Experience Sampling Study between Adolescents» [«Redes sociales y distraccion: un estudio de muestreo de experiencias entre adolescentes», documento no disponible en español], *Media Psychology*, vol. 25, 2022, pp. 343-366.

91 Laestadius, L., Bishop, A., Gonzalez, M., Illenčík, D. y Campos-Castillo, C., «Too human and not human enough: A grounded theory analysis of mental health harms from emotional dependence on the social chatbot Replika» [«Demasiado humano y no lo suficientemente humano: un análisis desde la teoría fundamentada sobre los daños a la salud mental derivados de la dependencia emocional del chatbot social Replika», documento no disponible en español], *New Media & Society*, 146144482211420, 2022, doi:10.1177/14614448221142007; Neugnot-Cerioli, M. y Laurenty, O. M., «The Future of Child Development in the AI Era. Cross-Disciplinary Perspectives Between AI and Child Development Experts» [«El futuro del desarrollo infantil en la era de la inteligencia artificial: perspectivas interdisciplinarias entre expertos en IA y desarrollo infantil», documento no disponible en español] 2024, prepublicación en https://doi.org/10.48550/ARXIV.2405.19275.

provoque perjuicios considerables que queden fuera del ámbito de aplicación del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial (véase la sección 5.3 «Fuera del ámbito de aplicación»).

117) Del mismo modo, las **personas mayores** pueden sufrir un declive cognitivo o tener una menor alfabetización digital, lo que las convierte en el principal objetivo de las estafas o las prácticas comerciales manipuladoras basadas en la IA. En este caso, los perjuicios suelen ser financieros y psicológicos; se ven agravados por la frustración y el aislamiento que experimentan muchas personas mayores, que pueden explotarse para aumentar el impacto manipulador.

Por ejemplo, un sistema de IA que aproveche las vulnerabilidades cognitivas de las personas mayores, ofreciéndoles, en particular, tratamientos médicos caros, pólizas de seguros innecesarias o planes de inversión engañosos, puede causar una pérdida significativa de sus ahorros, un aumento de su deuda y angustia emocional.

Determinadas prácticas de fijación de precios diferenciales que posibilita la IA en los servicios clave, como los seguros, que explotan una situación social o económica específica y fijan precios más elevados a los consumidores con un menor nivel de ingresos, pueden suponer una importante carga financiera al hacerles pagar más por la misma cobertura, lo que les hace vulnerables a las perturbaciones[92].

118) **Las personas con discapacidad** también representan un colectivo vulnerable al que los sistemas de IA abusivos y manipuladores pueden provocar perjuicios considerables.

Por ejemplo, un sistema de IA que utilice el reconocimiento de emociones para ayudar a las personas con discapacidad intelectual en su vida diaria también puede manipularlas para que tomen decisiones perjudiciales, como comprar productos que prometen beneficios poco realistas para la salud mental. Es probable que esto empeore su estado de salud mental y los explote financieramente, incitándolos a comprar productos ineficaces y caros, lo que puede causarles perjuicios psicológicos y financieros considerables.

119) **Las personas desfavorecidas desde el punto de vista social o económico** son especialmente vulnerables a los sistemas de IA que explotan su desesperación financiera y su precaria situación social. Además, suelen estar menos informadas y tener una menor alfabetización digital.

Por ejemplo, un chatbot de IA podría dirigirse a determinados colectivos desfavorecidos desde el punto de vista social o económico y alentarlos a cometer actos de violencia o a provocar lesiones a otras personas, detectando su mayor vulnerabilidad a determinados tipos de contenidos, discursos basados en el miedo u ofertas abusivas. El enfoque específico del sistema agrava las vulnerabilidades existentes de estas personas desfavorecidas desde el punto de vista socioeconómico, lo que agudiza sus problemas. En determinados casos, esto puede provocar un aumento de la ansiedad, la depresión, los sentimientos de desamparo o el aislamiento social, así como de las autolesiones y la

[92] Informe de 2023 de la AESPJ sobre las tendencias de los consumidores, página 16, último párrafo.

radicalización, hasta el punto de alcanzar el umbral de perjuicio considerable contemplado en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial.

120) A diferencia del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, el artículo 5, apartado 1, letra b), no hace referencia explícita a los perjuicios sufridos por un colectivo; sin embargo, su considerando 29 se refiere, para ambas prohibiciones, a los perjuicios sufridos tanto por personas concretas como por colectivos de personas. Así pues, las dos prohibiciones deben interpretarse de manera coherente, en consonancia también con la lógica de seguridad del Reglamento de Inteligencia Artificial y el objetivo de la prohibición del artículo 5, apartado 1, letra b), de proteger a todas las personas pertenecientes a colectivos vulnerables concretos por razón de su edad, su discapacidad y su situación social o económica específica. Por lo tanto, los perjuicios que pueden exteriorizarse y afectar a otras personas, aunque no se vean directamente afectadas por el sistema, también deben tenerse en cuenta en la evaluación de la importancia del perjuicio con arreglo al artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial.

Por ejemplo:

- La explotación de las vulnerabilidades de los menores que posibilita la IA puede tener repercusiones sociales a largo plazo, como una mayor prevalencia de los problemas de salud mental, un aumento de los costes de la asistencia sanitaria y una disminución de la productividad debido a problemas crónicos de salud.
- Un sistema de IA que explota las vulnerabilidades financieras de las personas económicamente desfavorecidas puede conducir a la exclusión financiera y crear una espiral descendente de dificultades socioeconómicas para esos colectivos desfavorecidos. Esta explotación puede causar perjuicios sociales con efectos negativos más amplios en las estructuras y valores de la sociedad, en particular la perpetuación y la exacerbación de la discriminación y la desigualdad social, así como la exclusión de estos colectivos.
- Un chatbot que se dirige a determinados colectivos vulnerables desde el punto de vista social o económico utilizando información errónea o discursos de odio puede generar polarización social y radicalización, lo que puede desembocar en situaciones violentas e incluso provocar lesiones y la muerte de otras personas.

121) Estos ejemplos de prácticas de IA de explotación deben diferenciarse de muchos otros sistemas de IA que no explotan las vulnerabilidades de los menores, las personas con discapacidad o las personas en situaciones sociales o económicas específicas y que no es razonablemente probable que provoquen perjuicios considerables; al contrario, estos sistemas buscan ser beneficiosos para dichas personas cuando se diseñan y utilizan adecuadamente (véase también la sección 3.5 «Fuera del ámbito de aplicación»).

Por ejemplo:

- Sistemas de IA que ayudan a los niños en su aprendizaje y en los juegos.

- Sistemas de IA que ayudan a las personas mayores en su vida diaria y mejoran su salud y su tratamiento médico, como los asistentes personales o los robots asistentes, o mejoran sus competencias digitales;

- Sistemas de IA que apoyan la integración económica y de otro tipo de las personas socialmente desfavorecidas en la sociedad, mejoran sus capacidades, etc.

- Sistemas y dispositivos de IA que asisten a las personas con discapacidad visual o auditiva o proporcionan un aprendizaje adaptado y personalizado.

- Sistemas de IA que generan soluciones accesibles mediante la eliminación de los obstáculos para el uso de productos y servicios por parte de las personas con discapacidad.

- Prótesis u otros dispositivos que posibilita la IA que ayudan a las personas con discapacidad en su vida diaria y permiten su integración y plena participación en la sociedad.

3.4. Relación entre las prohibiciones establecidas en el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial

122) La relación entre las prohibiciones del artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial obliga a delimitar los contextos específicos que contempla cada disposición para garantizar que se apliquen de manera complementaria.

123) La prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial se centra principalmente en la naturaleza de las técnicas, en concreto de las que operan por debajo del umbral de la conciencia u otras técnicas deliberadamente manipuladoras o engañosas. Los elementos clave en este caso son el carácter principalmente encubierto de la influencia y su efecto en la persona afectada por el sistema, que socava su autonomía cognitiva, es decir, su capacidad de tomar decisiones informadas y autónomas.

124) En cambio, el objetivo principal de la prohibición establecida en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial es proteger a las personas especialmente vulnerables debido a su edad, discapacidad o situación social o económica específica; estas personas, en principio, son más vulnerables a la explotación de la IA debido a factores inherentes o relacionados con la situación en la que se encuentran y, por tanto, necesitan una protección adicional contra la explotación. En este caso, los elementos clave son las características de las personas vulnerables afectadas y el hecho de que el sistema de IA esté explotando sus vulnerabilidades específicas.

Por ejemplo, si un sistema de IA utiliza imágenes que parpadean rápidamente para influir en las decisiones de compra, esto puede entrar en el ámbito de aplicación del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial debido a la naturaleza subliminal de la manipulación. Por el contrario, un sistema de IA que se dirige a las personas mayores para ofrecerles un seguro explotando su capacidad

cognitiva reducida puede entrar en el ámbito de aplicación del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial.

125) En los escenarios en que ambas disposiciones pueden parecer aplicables, el principal criterio de diferenciación debe ser el aspecto preponderante de la explotación. Si la explotación se aplica con independencia de las vulnerabilidades específicas de las personas afectadas, debe prevalecer el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, teniendo en cuenta los efectos concretos de la técnica manipuladora o engañosa en el comportamiento de las personas vulnerables y los perjuicios específicos que puedan sufrir. Si la manipulación y la explotación que posibilita la IA se dirigen a un colectivo particular de personas vulnerables debido a su edad, discapacidad o situación social o económica específica, o tienen por objeto explotar sus vulnerabilidades, debe aplicarse en su lugar el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial. La explotación de las vulnerabilidades de otros colectivos puede estar contemplada en el marco del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial si la práctica deliberadamente manipuladora explota las vulnerabilidades y debilidades específicas de dichas personas.

3.5. Fuera del ámbito de aplicación

126) Para que se apliquen las prohibiciones del artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial, deben cumplirse todas las condiciones enumeradas en las disposiciones pertinentes, tal como ya se ha examinado. Todos los demás sistemas de IA que no cumplan estas condiciones quedan fuera del ámbito de aplicación de dichas prohibiciones. A continuación se incluyen algunos ejemplos.

3.5.1. Persuasión lícita

127) Diferenciar la manipulación de la persuasión es fundamental para delimitar el ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, que no se aplica a las prácticas de persuasión lícita. Aunque tanto la manipulación como la persuasión influyen en las decisiones y los comportamientos de las personas, difieren considerablemente en cuanto a sus métodos e implicaciones éticas.

128) La manipulación implica, en la mayoría de los casos, el uso de técnicas encubiertas que socavan la autonomía, lo que lleva a las personas a tomar decisiones que quizá no habrían tomado si fueran plenamente conscientes de las influencias ejercidas. Estas técnicas suelen explotar las debilidades psicológicas o los sesgos cognitivos. En cambio, la persuasión opera dentro de los límites de la transparencia y del respeto de la autonomía individual. Consiste en presentar los argumentos o la información recurriendo a la razón y a las emociones, pero se explican los objetivos y el funcionamiento del sistema de IA, se facilita información pertinente y precisa para garantizar que se tomen decisiones informadas y se apoya la capacidad de la persona para evaluar la información y tomar decisiones libres y autónomas.

Por ejemplo, un sistema de IA que utiliza recomendaciones personalizadas basadas en algoritmos transparentes y en las preferencias y los controles de los usuarios ejerce la

persuasión. En cambio, si un sistema utiliza señales subliminales (como imágenes imperceptibles) para influir en los usuarios y hacer que tomen decisiones específicas sin su conocimiento ni comprensión, se trata de manipulación.

129) El objetivo y los efectos de estas técnicas también difieren. La manipulación suele tener por objeto beneficiar al manipulador, a expensas de la autonomía y el bienestar de la persona, mientras que el objetivo de la persuasión es informar y convencer, armonizando los intereses y los beneficios para ambas partes. La persuasión ética respeta la autonomía de una persona a la hora de tomar decisiones informadas y evita explotar sus vulnerabilidades.

Por ejemplo, un sistema de IA que funciona de manera transparente y analiza las emociones de los clientes, que son conscientes de ello, con el fin de mejorar la interacción con ellos y ofrecerles ayuda utiliza la persuasión y se ajusta a sus intereses. En cambio, un sistema de reconocimiento de emociones utilizado para la publicidad dirigida que deduce las emociones de los consumidores de forma encubierta para ofrecer productos de precios más elevados en un momento concreto en el que es más probable que los compren utiliza la manipulación, en detrimento de los consumidores.

130) El consentimiento también desempeña un papel importante en determinados casos. En interacciones persuasivas, las personas son conscientes del intento de influencia y pueden elegirlo de forma libre y autónoma. En las interacciones manipuladoras, la falta de conocimiento sobre el uso de las técnicas o de sus efectos invalida su capacidad de elegir libremente y de tomar decisiones informadas y autónomas.

Por ejemplo, un sistema de IA cuyo objetivo es ayudar a los usuarios a aprender una lengua extranjera más eficaz y rápidamente mediante el uso de técnicas subliminales no es manipulador si funciona de manera transparente y respeta la autonomía individual y la elección libre e informada del usuario de permitir o no el uso del sistema.

131) El cumplimiento de los marcos jurídicos y reglamentarios también desempeña un importante papel a la hora de diferenciar la manipulación de la persuasión lícita. Por lo tanto, es más probable que las prácticas de IA que cumplen la legislación aplicable que defiende la transparencia, la equidad y los derechos y la autonomía de las personas no estén prohibidas por el Reglamento de Inteligencia Artificial.

Un ejemplo es el cumplimiento de la legislación en materia de protección de datos, como el RGPD, que impone obligaciones de transparencia en el tratamiento de datos personales, lo que significa que la información que debe facilitarse a los interesados debe evitar un lenguaje engañoso o manipulador[93]. En algunos casos, puede necesitarse el consentimiento para que el tratamiento de datos personales sea lícito, como para determinados anuncios personalizados en línea basados en los datos de los usuarios fuera del servicio en las redes sociales[94]. Dicho consentimiento debe ser, entre otros,

[93] Directrices del Comité Europeo de Protección de Datos, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf [documento no disponible en español], apartado 18.

[94] Sentencia del Tribunal de Justicia de 4 de julio de 2023, Meta Platforms y otros, C-252/21, ECLI:EU:C:2023:537 (en lo sucesivo, la «sentencia Meta Platforms»).

libre e informado. Es más probable que los sistemas de IA que cumplan estas normas jurídicas practiquen la persuasión lícita. En cambio, los sistemas que eluden estos requisitos para influir en el comportamiento son, probablemente, manipuladores.

132) En particular, el considerando 29 del Reglamento de Inteligencia Artificial aclara que las prohibiciones establecidas en su artículo 5, apartado 1, letras a) y b), no afectan, en ciertas condiciones, a prácticas lícitas en el contexto de un tratamiento médico.

Por ejemplo, las técnicas subliminales que posibilita la IA pueden utilizarse en el tratamiento psicológico de una enfermedad mental o en la rehabilitación física cuando se lleven a cabo de conformidad con el Derecho y las normas médicas aplicables, como la obtención del consentimiento expreso de la persona o de sus representantes legales como condición para su uso.

133) Además, el considerando 29 del Reglamento de Inteligencia Artificial precisa que las prácticas comerciales comunes y legítimas, como la publicidad, no deben considerarse «en sí mismas» o por su propia naturaleza prácticas de manipulación, engaño o explotación perjudiciales que posibilita la IA.

A continuación, varios ejemplos:

- Las técnicas publicitarias que utilizan IA para personalizar contenidos sobre la base de las preferencias de los usuarios no son intrínsecamente manipuladoras si no utilizan técnicas subliminales, deliberadamente manipuladoras o engañosas que socaven la autonomía individual o exploten las vulnerabilidades de manera perjudicial, tal como se prohíbe en el artículo 5, apartado 1, letra a), y letra b), del Reglamento de Inteligencia Artificial. El cumplimiento de las obligaciones pertinentes contempladas en el RGPD, la legislación en materia de protección de los consumidores y el Reglamento (UE) 2022/2065 (en lo sucesivo, el «Reglamento de Servicios Digitales») ayudan a mitigar dichos riesgos.
- El desarrollo de modelos y clasificadores de IA para detectar abuso sexual de menores en línea de conformidad con la legislación aplicable es una práctica legítima que no explota las vulnerabilidades de los menores y que, por el contrario, es esencial para mejorar su seguridad en línea.
- Los sistemas de IA utilizados para prestar servicios bancarios, como créditos hipotecarios y préstamos, que se basan en la edad o la situación socioeconómica específica del cliente, de conformidad con la legislación de la Unión en materia de servicios financieros, protección de los consumidores, protección de datos y no discriminación, no se consideran sistemas que explotan las vulnerabilidades en el sentido del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial cuando están diseñados para proteger y ayudar a las personas identificadas como vulnerables debido a su edad, discapacidad o circunstancias socioeconómicas específicas y sean beneficiosos para esos colectivos. Esto también contribuye a tener unos servicios financieros más justos y sostenibles para dichos colectivos.

- Los sistemas de IA que detectan la somnolencia y la fatiga de los conductores y los avisan para que descansen, de conformidad con la legislación en materia de seguridad, son beneficiosos y no se consideran sistemas que explotan las vulnerabilidades en el sentido del artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial.

3.5.2. Sistemas de IA de manipulación, engaño y explotación que no es probable que provoquen perjuicios considerables

134) Una condición fundamental para que se apliquen las prohibiciones establecidas en el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial es que la manipulación y la explotación de vulnerabilidades que posibilita la IA debe provocar o ser razonablemente probable que provoque perjuicios considerables. Todas las aplicaciones de IA de manipulación, engaño y explotación que no sea razonablemente probable que provoquen perjuicios considerables quedan, en principio, fuera del ámbito de aplicación de las prohibiciones, sin perjuicio de otra legislación de la Unión que siga siendo aplicable (véase la sección 3.6).

Estos son algunos ejemplos de sistemas de IA que no es probable que provoquen perjuicios considerables:

- Un sistema de compañía de IA está diseñado de manera antropomórfica y con computación afectiva para que sea más atractivo y haga que los usuarios sean más activos, pero no utiliza otras prácticas manipuladoras o engañosas de un modo que sea razonablemente probable que les provoque graves perjuicios psicológicos, físicos o de otro tipo, ni que genere en ellos un vínculo y una dependencia poco saludables.

- Un chatbot terapéutico utiliza técnicas subliminales para orientar a los usuarios hacia un estilo de vida más saludable y ayudarlos a abandonar los malos hábitos, como el tabaquismo. Aunque los usuarios que siguen los consejos y la terapia subliminal del chatbot experimenten algunas molestias físicas y estrés psicológico debido a sus esfuerzos para dejar de fumar, no se puede considerar probable que el chatbot que posibilita la IA provoque perjuicios considerables. Estas molestias temporales son inevitables y se ven compensadas por los beneficios a largo plazo para la salud de los usuarios. No hay intentos ocultos de influir en la toma de decisiones más allá de promover hábitos saludables.

- Una plataforma musical en línea utiliza un sistema de reconocimiento de emociones para deducir las emociones de los usuarios y les recomienda automáticamente canciones en función de su estado de ánimo, evitando al mismo tiempo una exposición excesiva a canciones depresivas. Dado que los usuarios solo están escuchando música y no se ven perjudicados de otro modo o se ven empujados hacia la depresión y la ansiedad, no es razonablemente probable que el sistema provoque perjuicios considerables.

- Se utilizan técnicas manipuladoras y engañosas que posibilita la IA en la formación en materia de seguridad y en otras simulaciones con fines de aprendizaje que imitan intentos de *phishing* para concienciar a los usuarios sobre las amenazas informáticas. Estos sistemas pueden utilizar técnicas deliberadamente manipuladoras (por ejemplo,

la explotación de sesgos cognitivos) sin que los usuarios sean conscientes de que alteran el comportamiento, pero esto se hace temporalmente con fines de formación y concienciación beneficiosos, sin provocar perjuicios considerables.

3.6. Relación con otras disposiciones del Derecho de la Unión

135) Las prohibiciones establecidas en el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial se entienden sin perjuicio de otras disposiciones del Derecho de la Unión y las complementan. La misma práctica que entra en el ámbito de aplicación de las prohibiciones del artículo 5, apartado 1, letras a) o b), del Reglamento de Inteligencia Artificial también puede constituir una infracción de otra disposición del Derecho de la Unión y estar sujeta a garantía del cumplimiento en virtud tanto del Reglamento de Inteligencia Artificial como de esos otros actos. Esto es importante porque las distintas disposiciones de esos actos tienen por objeto proteger intereses diferentes y tienen objetivos, ámbitos de aplicación y destinatarios distintos. De esta forma, se garantiza un enfoque regulador integral que proteja a las personas y colectivos de personas de la explotación y la manipulación perjudiciales de la IA y garantice unos servicios y productos posibilitados por la IA seguros y fiables en la Unión.

136) Las prohibiciones establecidas en el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial están en estrecha consonancia con los objetivos de la legislación de la UE en materia de protección de los consumidores, en particular la Directiva sobre las prácticas comerciales desleales, que protege a los consumidores de prácticas comerciales engañosas o agresivas, también cuando están basadas en la IA. Tanto el Reglamento de Inteligencia Artificial como la Directiva sobre las prácticas comerciales desleales tienen por objeto prevenir de forma proactiva los perjuicios a los consumidores derivados de prácticas comerciales basadas en la IA que sean manipuladoras, engañosas o agresivas. Al mismo tiempo, el ámbito de aplicación de las prohibiciones del artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial es más amplio, ya que protegen no solo a los consumidores, sino a cualquier persona física y a su comportamiento en diversos contextos, más allá de las relaciones comerciales. Los perjuicios contemplados en el Reglamento de Inteligencia Artificial también van más allá de los perjuicios económicos, aunque dicho Reglamento establece un umbral de perjuicio considerable que no está presente en la legislación en materia de protección de los consumidores.

137) Las prohibiciones también son coherentes con la legislación de la Unión en materia de protección de datos, en particular con los principios para un tratamiento de datos lícito, justo y transparente, cuyo objetivo es proteger los datos personales de los interesados y, en última instancia, preservar sus derechos fundamentales y su autonomía. La disponibilidad de más datos (personales) y el aumento de las posibilidades de tratar estos datos con sistemas de IA aumentan el riesgo de que se utilicen prácticas de manipulación, engaño o explotación perjudiciales, como las que entran en el ámbito de aplicación del artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial. En este contexto, el cumplimiento de las normas de protección de datos en

materia de transparencia, minimización de datos, equidad y licitud, por ejemplo en la personalización de la elaboración de perfiles y la publicidad sobre la base de los datos de los usuarios fuera del servicio[95], puede ayudar a evitar perjuicios relacionados con una manipulación y explotación personalizadas.

138) La relación con el Derecho de la Unión en materia de no discriminación también es pertinente para la prohibición establecida en el artículo 5, apartado 1, letra b), del Reglamento de Inteligencia Artificial[96], dado que las vulnerabilidades derivadas de la edad y la discapacidad también son motivos protegidos por los que las personas tienen derecho a no ser discriminadas, mientras que la situación socioeconómica converge con otra serie de motivos, como el origen racial o étnico. Las prohibiciones establecidas en el Reglamento de Inteligencia Artificial no afectan a las prohibiciones basadas en otros motivos o prácticas discriminatorias que no provoquen perjuicios considerables y que ya estén prohibidas por el Derecho de la Unión en materia de no discriminación.

139) Las prohibiciones establecidas en el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial también son complementarias con el Reglamento (UE) 2022/2065 (Reglamento de Servicios Digitales), que regula los servicios intermediarios en línea, como las plataformas en línea y los motores de búsqueda en línea, y garantiza la transparencia y la rendición de cuentas en la prestación de dichos servicios. En particular, el artículo 25, apartado 1, del Reglamento de Servicios Digitales prohíbe las interfaces de usuario engañosas para garantizar que los prestadores de plataformas en línea no induzcan a error a los usuarios ni los obliguen a actuar de una forma que no se corresponda con sus verdaderas intenciones. Estas interfaces engañosas deben considerarse ejemplos de técnicas manipuladoras o engañosas en el sentido del artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial, cuando sea probable que provoquen perjuicios considerables.

140) El Reglamento de Servicios Digitales también establece obligaciones para los prestadores de plataformas en línea a fin de garantizar la transparencia en la publicidad (artículos 26 y 38 para las plataformas en línea de muy gran tamaño o los motores de búsqueda de muy gran tamaño) y establece otras obligaciones relativas al uso de sistemas de recomendación (artículo 27) y a la protección de los menores (artículo 28). Además, si una plataforma en línea o un motor de búsqueda en línea se clasifica como plataforma en línea de muy gran tamaño o motor de búsqueda de muy gran tamaño, el prestador de dicho servicio en cuestión tiene también otras obligaciones relativas a la

---

95 A este respecto, resulta especialmente pertinente la sentencia del Tribunal de Justicia (Gran Sala) de 4 de julio de 2023, Meta Platforms Inc y otros/Bundeskartellamt, C-252/21. Aunque el TJUE considera, entre otras cosas, que el tratamiento de datos personales de los usuarios fuera del servicio con fines de mercadotecnia directa por parte de una gran plataforma de red social puede considerarse realizado por interés legítimo del responsable del tratamiento, no puede hacerse sin el consentimiento de un usuario, como base jurídica, debido a los intereses y derechos fundamentales de dicho usuario que, en las circunstancias del caso, en particular el tratamiento extensivo, prevalecen sobre el interés de dicho operador en tal personalización de la publicidad a través de la cual las plataformas sociales financian sus actividades (véase la sentencia Meta Platforms, apartados 115 a 118).

96 P.ej. la Directiva 2000/43/CE del Consejo, de 29 de junio de 2000, relativa a la aplicación del principio de igualdad de trato de las personas independientemente de su origen racial o étnico (DO L 180 de 19.7.2000, p. 22); la Directiva 2000/78/CE del Consejo, de 27 de noviembre de 2000, relativa al establecimiento de un marco general para la igualdad de trato en el empleo y la ocupación (DO L 303 de 2.12.2000, p. 16); Directiva 2006/54/CE del Parlamento Europeo y del Consejo, de 5 de julio de 2006, relativa a la aplicación del principio de igualdad de oportunidades e igualdad de trato entre hombres y mujeres en asuntos de empleo y ocupación (refundición) (DO L 204 de 26.7.2006, p. 23); o la Directiva del Consejo 2004/113/CE, de 13 de diciembre de 2004, por la que se aplica el principio de igualdad de trato entre hombres y mujeres al acceso a bienes y servicios y su suministro (DO L 373 de 21.12.2004, p. 37).

evaluación y la reducción de los riesgos sistémicos que se deriven del diseño o del funcionamiento de su servicio y los sistemas relacionados con este, incluidos los sistemas algorítmicos (artículos 34 y 35 del Reglamento de Servicios Digitales). Al realizar evaluaciones de riesgos, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben examinar la manera en que sus sistemas de recomendación, su publicidad, su moderación de contenidos y cualquier otro sistema algorítmico pertinente influyen en dichos riesgos sistémicos. Estas evaluaciones de riesgos también deben analizar la manera en que la manipulación intencionada y la explotación automatizada del servicio, entre otras cosas, influyen en los riesgos sistémicos (véanse el artículo 34, apartado 2, del Reglamento de Servicios Digitales y el considerando 83 de dicho Reglamento). No obstante, el ámbito de aplicación del artículo 5, apartado 1, letras a) o b) del Reglamento de Inteligencia Artificial abarca una amplia variedad de otros escenarios (por ejemplo, chatbots o servicios y productos que posibilita la IA) que pueden ser ofrecidos o utilizados por agentes distintos de los prestadores de servicios intermediarios.

141) La prohibición de las técnicas de IA manipuladoras de conformidad con el artículo 5, apartado 1, letra a), del Reglamento de Inteligencia Artificial también apoya los objetivos de la Directiva 2010/13/UE (Directiva de servicios de comunicación audiovisual)[97] al prevenir la publicidad perjudicial basada en la IA[98] y otras prácticas de manipulación y explotación que posibilita la IA que puedan ser considerablemente perjudiciales en el sector de los medios de comunicación.

142) El Reglamento de Inteligencia Artificial también complementa el Reglamento (UE) 2024/900 (Reglamento sobre publicidad política)[99], que establece normas armonizadas, en particular obligaciones de transparencia y obligaciones conexas de diligencia debida, para la prestación de servicios publicidad política y servicios conexos, así como para el uso de técnicas de segmentación y entrega de anuncios en el contexto de la publicidad política en línea. Dicho Reglamento prohíbe la elaboración de perfiles basada en categorías especiales de datos personales en el contexto de la publicidad política en línea, así como la segmentación de personas que están al menos un año por debajo de la edad de voto establecida por las normas nacionales. Además, las técnicas de segmentación y de entrega de anuncios en el contexto de la publicidad política en línea solo pueden llevarse a cabo si se basan en datos personales obtenidos de los interesados y con su consentimiento expreso. También se aplican requisitos de transparencia adicionales, a saber, la comunicación de información relacionada con la publicidad política, en la que se describa el uso de dichas técnicas y los parámetros principales y se facilite información adicional sobre la lógica aplicada, en particular sobre el uso de sistemas de IA. La publicidad política segmentada, basada en el tratamiento de datos

97 Directiva 2010/13/UE del Parlamento Europeo y del Consejo, de 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), modificada por la Directiva (UE) 2018/1808, que tiene por objeto, entre otras cosas, mejorar la protección de los niños y tratar más eficazmente la incitación al odio.

98 Artículo 9 de la Directiva de servicios de comunicación audiovisual.

99 Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre transparencia y segmentación en la publicidad política, PE/90/2023/REV/1, DO L, 2024/900, 20.3.2024.

personales de conformidad con dicho Reglamento[100], contribuirá a garantizar que la elaboración de perfiles de los votantes, así como la segmentación y la entrega de anuncios de publicidad política, operen dentro de los límites de la persuasión lícita.

143) La prohibición establecida en el Reglamento de Inteligencia Artificial de las prácticas de IA engañosas y de explotación perjudiciales también complementa otras normas aplicables de la Unión que establecen normas generales de transparencia sobre la publicidad y la protección de los consumidores y el comportamiento que deben adoptar los operadores. Por ejemplo, la Directiva 2014/65/UE (MiFID), la Directiva (UE) 2016/97 sobre la distribución de seguros[101], la Directiva (UE) 2023/2225 sobre contratos de crédito al consumo, la Directiva 2002/65/CE sobre comercialización a distancia, la Directiva 2006/114/CE sobre publicidad engañosa y publicidad comparativa y la Directiva 2011/83/UE sobre derechos de los consumidores establecen normas generales de protección de los consumidores. A este respecto, la Autoridad Europea de Seguros y Pensiones de Jubilación (AESPJ) ya ha emitido una declaración de supervisión sobre algunas prácticas de explotación desleales en relación con la fijación de precios diferenciales que también podrían entrar en el ámbito de aplicación del Reglamento de Inteligencia Artificial si dichas prácticas se basan en sistemas de IA[102].

144) Las prohibiciones establecidas en el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial también se entienden sin perjuicio de la legislación de la UE en materia de seguridad de los productos (por ejemplo, en relación con los productos sanitarios, los juguetes y las máquinas) y la complementan, lo que desempeña un papel crucial a la hora de garantizar la seguridad de los productos que integran sistemas de IA. Esto implica el cumplimiento de requisitos de seguridad *ex ante* para los productos regulados y su seguimiento proactivo para garantizar que no plantean riesgos para la seguridad que puedan provocar perjuicios físicos y mentales. Por consiguiente, los fabricantes de dichos productos que integren sistemas de IA deben tener en cuenta estas prohibiciones en sus evaluaciones de riesgos y sus medidas de reducción de riesgos en materia de seguridad, en la medida en que ello se ajuste a la lógica y al ámbito de aplicación de la legislación armonizada pertinente de la Unión en materia de seguridad. La legislación de la Unión en materia de seguridad también complementa las prohibiciones establecidas en el Reglamento de Inteligencia Artificial y puede igualmente abordar y tratar los riesgos de seguridad que no suponen un perjuicio considerable. En particular, el Reglamento (UE) 2023/988 (Reglamento sobre la seguridad general de los productos)[103] actúa como red de seguridad y exige que todos los productos de consumo que no estén cubiertos por requisitos específicos de otra

[100] Una vez sea aplicable, a partir de octubre de 2025.

[101] Directiva (UE) 2016/97 del Parlamento Europeo y del Consejo, de 20 de enero de 2016, sobre la distribución de seguros (versión refundida) (DO L 26 de 2.2.2016, p. 19). Por ejemplo, el artículo 17, apartado 1, de la Directiva sobre la distribución de seguros establece que los distribuidores de seguros deben actuar con honestidad, equidad y profesionalidad, en beneficio de los intereses de sus clientes.

[102] https://www.eiopa.europa.eu/document/download/1e9a8fb2-e688-4bf5-a347-ee0a1ec3aab3_en?filename=EIOPA-BoS-23-076-Supervisory-Statement-on-differential-pricing-practices_0.pdf.

[103] Reglamento (UE) 2023/988 del Parlamento Europeo y del Consejo, de 10 de mayo de 2023, relativo a la seguridad general de los productos, por el que se modifican el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo y la Directiva (UE) 2020/1828 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2001/95/CE del Parlamento Europeo y del Consejo y la Directiva 87/357/CEE del Consejo (Texto pertinente a efectos del EEE) (DO L 135 de 23.5.2023, p. 1).

legislación sectorial de la Unión en materia de seguridad de los productos (incluidos los productos que integren sistemas de IA no clasificados como de alto riesgo de conformidad con el artículo 6 y sujetos a los requisitos del Reglamento de Inteligencia Artificial) sean seguros en condiciones de uso normales o razonablemente previsibles, en particular en lo que respecta a los riesgos para la salud física y mental de los consumidores.

145) Por último, la relación con el Derecho penal es fundamental. Las prohibiciones establecidas en el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial tienen por objeto prevenir los comportamientos perjudiciales que puedan constituir un delito o dar lugar a un delito, como el fraude, la falsificación, las estafas, la coacción o la generación y difusión de contenidos ilícitos, como contenidos terroristas, el material de abuso sexual de menores, el discurso de odio y ultrafalsificaciones sexualmente explícitas[104]. Es importante señalar que, al tratarse de una normativa del mercado interior, las prohibiciones establecidas en el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial no solo cubren la utilización, sino también la introducción en el mercado del sistema de IA. De esta manera, se evitan perjuicios desde una fase temprana al limitar el acceso a estos sistemas prohibidos que pueden facilitar y ocultar las actividades delictivas. Además, las prohibiciones del artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial también podrían contemplar otras prácticas perjudiciales que no se estén calificadas como infracciones penales según el Derecho de la Unión o el nacional.

4. ARTÍCULO 5, APARTADO 1, LETRA C), DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: PUNTUACIÓN CIUDADANA

146) Si bien la puntuación que posibilita la IA puede resultar beneficiosa para fomentar el buen comportamiento o mejorar la seguridad, la eficiencia o la calidad de los servicios, existen ciertas prácticas de «puntuación ciudadana» que tratan o perjudican injustamente a las personas y equivalen a control y vigilancia sociales. La prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial aborda dichas prácticas inaceptables de «puntuación ciudadana» que posibilita la IA, que evalúan o clasifican a personas o colectivos de personas atendiendo a su comportamiento social o a características personales y provocan un trato perjudicial o desfavorable, en particular cuando los datos proceden de múltiples contextos sociales que no guardan relación o cuando el trato es desproporcionado con respecto a la gravedad del comportamiento social. La prohibición de la «puntuación ciudadana» tiene un amplio ámbito de aplicación tanto en contextos públicos como privados y no se limita a un sector o ámbito específicos[105].

---

[104] Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, PE/33/2024/REV/1, DO L, 2024/1385, 24.5.2024.

[105] La prohibición de la puntuación ciudadana difiere de la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial. Esta última es más especializada en cuanto a la práctica de evaluación o puntuación y solo se aplica a la evaluación de riesgos y a la predicción de la probabilidad de que una persona cometa delitos, al prohibir los sistemas de IA que se basan únicamente en la elaboración de perfiles o en la evaluación de los rasgos y características de la personalidad (véase la sección 5).

147) Al mismo tiempo, la prohibición no está destinada a afectar a prácticas lícitas de evaluación de las personas que se efectúen para un fin específico que es legítimo y conforme con el Derecho de la Unión y nacional[106], en particular cuando dicha legislación especifique los tipos de datos pertinentes para los fines específicos de evaluación y garantice que cualquier trato resultante perjudicial o desfavorable de las personas esté justificado y sea proporcionado (véase la sección 4.3 «Fuera del ámbito de aplicación»).

4.1. Justificación y objetivos

148) Los sistemas de IA que permiten prácticas de «puntuación ciudadana» pueden tener efectos discriminatorios e injustos para determinadas personas y colectivos, incluida su exclusión de la sociedad, así como prácticas de control y vigilancia sociales que son incompatibles con los valores de la Unión. La prohibición de la «puntuación ciudadana» tiene por objeto proteger, en particular, el derecho a la dignidad humana y otros derechos fundamentales, como el derecho a la no discriminación y a la igualdad, a la protección de datos y a la vida privada y familiar, así como los derechos sociales y económicos pertinentes, cuando proceda. También tiene por objeto fomentar y garantizar los valores de la Unión de democracia, igualdad (incluida la igualdad de acceso a los servicios públicos y privados) y justicia[107].

4.2. Conceptos fundamentales y componentes de la prohibición de la «puntuación ciudadana»

Según el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial:

Quedan prohibidas las siguientes prácticas de IA:

c) la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas, de forma que la puntuación ciudadana resultante provoque una o varias de las situaciones siguientes:

i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente,

ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos de personas que sea injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;

149) Deben cumplirse varias condiciones acumulativas para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial:

[106] Considerando 31 del Reglamento de Inteligencia Artificial.
[107] Considerando 31 del Reglamento de Inteligencia Artificial.

(i) La práctica debe suponer la «introducción en el mercado», la «puesta en servicio» o la «utilización» de un sistema de IA.

(ii) El sistema de IA debe estar destinado a evaluar o clasificar a personas físicas o a colectivos de personas durante un período determinado de tiempo, o ser utilizado para ello, atendiendo a:

(a) su comportamiento social; o

(b) características personales o de su personalidad conocidas, inferidas o predichas.

(iii) La puntuación social creada con la ayuda del sistema de IA debe dar lugar o ser capaz de dar lugar a un trato perjudicial o desfavorable de personas o colectivos en uno o varios de los siguientes escenarios:

(a) en contextos sociales que no guardan relación con los contextos donde se generaron o recabaron los datos originalmente; y/o

(b) el trato es injustificado o desproporcionado en relación con su comportamiento social o su gravedad.

150) Para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial, deben cumplirse simultáneamente las tres condiciones. Ya se ha examinado la primera condición, a saber, la «introducción en el mercado», la «puesta en servicio» o la «utilización» de un sistema de IA en la sección 2.3. Así pues, la prohibición se aplica tanto a los proveedores como a los responsables del despliegue de sistemas de IA, cada uno dentro de sus respectivas responsabilidades de no introducir en el mercado, poner en servicio o utilizar dichos sistemas de IA. A continuación se describen y analizan con más detalle los demás criterios para prohibir la «puntuación social».

4.2.1. «Puntuación ciudadana»: evaluación o clasificación atendiendo al comportamiento social o a las características personales o de la personalidad durante un período determinado de tiempo

a) Evaluación o clasificación de personas físicas o colectivos de personas

151) La segunda condición para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial es que el sistema de IA esté destinado a **la evaluación o la clasificación** de personas físicas o colectivos de personas y les asigne puntuaciones atendiendo a su comportamiento social o sus características personales o de la personalidad, o se utilice para ello. La puntuación producida por el sistema puede adoptar diversas formas, como un número matemático (por ejemplo, de 0 a 1), una clasificación o una etiqueta.

152) El ámbito de aplicación de la prohibición es amplio y comprende las prácticas de evaluación y clasificación tanto en el sector público como en el privado (véase la sección 4.2.3). Al mismo tiempo, la evaluación o la clasificación solo se refiere a

personas físicas o a colectivos de personas físicas; así pues, en principio, las entidades jurídicas quedan excluidas (véase la sección 4.3 «Fuera del ámbito de aplicación»).

153) Si bien la «**evaluación**» sugiere algún tipo de **valoración o juicio** sobre una persona o colectivo de personas, una simple **clasificación** de personas o colectivos de personas basada en características como su edad, sexo y altura no tiene por qué dar lugar necesariamente a una evaluación[108]. Por lo tanto, el ámbito de aplicación de la «clasificación» es más amplio que el de la «evaluación» y puede también incluir otros tipos de clasificaciones o categorizaciones de personas físicas o colectivos de personas basadas en criterios que no implican necesariamente una valoración o un juicio particular sobre dichas personas o colectivos de personas y sus características o su comportamiento.

154) El término «**evaluación**» también se refiere al concepto de «elaboración de perfiles», que está regulado por la legislación de la Unión en materia de protección de datos[109] y constituye una forma específica de evaluación. Aunque en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial no se hace referencia directa a este concepto o a dicha legislación[110], también pueden ser pertinentes para la prohibición recogida en dicha disposición, así como para otras prohibiciones del Reglamento de Inteligencia Artificial[111], cuando la evaluación se lleve a cabo de manera automatizada por un sistema de IA sobre la base de datos personales. La **elaboración de perfiles** consiste en utilizar información sobre una persona (o colectivo de personas) y evaluar sus características o patrones de comportamiento con el fin de asignarla a una determinada categoría o colectivo, en particular **para analizar o hacer predicciones** sobre, por ejemplo, su capacidad para realizar una tarea, sus intereses o su comportamiento probable[112]. Por lo tanto, la elaboración de perfiles de personas físicas de conformidad con la legislación de la Unión en materia de protección de datos, cuando se lleve a cabo mediante sistemas de IA, también puede estar contemplada en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial.

Por ejemplo, en la sentencia SCHUFA I, el TJUE examinó un **sistema de puntuación de solvencia** utilizado en Alemania[113]. En ese asunto, el *score* [«puntuación»] generado por el programa informático era un «valor de probabilidad» relativo a la capacidad de una persona para cumplir sus compromisos de pago, que el TJUE calificó de «elaboración de perfiles». Más concretamente, el sistema estableció «un pronóstico

108 Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679, WP251rev.01, 6.2.2018, p. 7.

109 Véanse el artículo 4, apartado 4, y el artículo 22 del RGPD y el artículo 11 de la Directiva sobre protección de datos en el ámbito penal. Véanse también las Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679, WP251rev.01, 6.2.2018, p. 7.

110 El artículo 3, punto 52, del Reglamento de Inteligencia Artificial aporta una definición de «elaboración de perfiles» que remite a la definición del artículo 4, punto 4, del RGPD.

111 En particular, la prohibición de la predicción del riesgo de que una persona cometa un delito establecido en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, que sí hace referencia a la «elaboración de perfiles», y, en determinados casos, el reconocimiento de emociones y la categorización biométrica contemplados en el artículo 5, apartado 1, letras f) y g), del Reglamento de Inteligencia Artificial.

112 Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679, WP251rev.01, 6.2.2018, p. 7.

113 Sentencia del Tribunal de Justicia de 7 de diciembre de 2023, SCHUFA Holding (Scoring), C-634/21, ECLI:EU:C:2023:957 (en lo sucesivo, la «SCHUFA I»), por ejemplo, apartado 47.

sobre la probabilidad de un comportamiento futuro de una persona (*score* o calificación), como el reembolso de un préstamo, a partir de determinadas características de dicha persona [...]. La generación de valores de *score* (*scoring*) se basa en la hipótesis de que la clasificación de una persona en una categoría de personas con características comparables, que han revelado cierto comportamiento, permite prever un comportamiento similar»[114]. Según el TJUE, esta actividad respondía a la definición de «elaboración de perfiles» en el sentido del artículo 4, punto 4, del RGPD[115]. También puede considerarse que esta forma de elaboración de perfiles constituye una evaluación de las personas basada en sus características personales en el sentido del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial, que está prohibida si se lleva a cabo con sistemas de IA y siempre que se cumplan las demás condiciones para que se aplique dicha disposición.

b) Durante un período determinado de tiempo

155) La prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial exige que la evaluación o la clasificación se base en datos que se extiendan durante «**un período determinado de tiempo**». Esto sugiere que la evaluación no debe limitarse a una clasificación o calificación puntual o inmediata con datos o comportamientos procedentes de un contexto individual muy específico. Al mismo tiempo, es importante que esta condición se examine teniendo en cuenta todas las circunstancias del caso para evitar que se eluda el ámbito de aplicación de la prohibición.

Por ejemplo, una autoridad de migración y asilo implementa en los campamentos de refugiados un sistema de vigilancia parcialmente automatizado basado en una serie de infraestructuras de vigilancia, incluidas cámaras y sensores de movimiento. Si los datos analizados se extienden a lo largo de un período de tiempo y se evalúa a personas concretas (como migrantes), por ejemplo, para determinar si corren el riesgo de intentar fugarse, podría considerarse que esto sucede «durante un determinado período de tiempo» y puede aplicarse la prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial si se cumplen todas las demás condiciones.

c) Atendiendo a su comportamiento social o a características personales o de su personalidad conocidas, inferidas o predichas

156) Las prácticas de «evaluación» y «clasificación» prohibidas por el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial deben basarse en el tratamiento de datos que posibilita la IA (a menudo extensivo) en relación con i) el comportamiento social de personas o de colectivos de personas o ii) sus características personales o de su personalidad conocidas, inferidas o predichas, o ambas. Los datos pueden ser facilitados directamente por las personas o recogidos de forma indirecta, es decir, mediante vigilancia, a partir de terceros o deduciéndolos de otra información.

114 *Ibidem*, apartado 14 (la tipografía en negrita es nuestra).
115 *Ibidem*, apartado 47.

157) Por lo que se refiere al primer escenario, el «**comportamiento social**» es un concepto amplio que normalmente puede incluir acciones, comportamientos, hábitos, interacciones dentro de la sociedad, etc., y suele comprender los puntos de datos relacionados con el comportamiento procedentes de múltiples fuentes[116]. Esto podría incluir los comportamientos de personas y colectivos de personas en contextos sociales y privados, como la participación en actos culturales, voluntariado, etc., pero también los comportamientos sociales en contextos empresariales, como el pago de deudas, el comportamiento al utilizar determinados servicios, así como las relaciones con entidades públicas y privadas, la administración, la policía y la ley (por ejemplo, si una persona cumple las normas de tráfico). Los datos sobre comportamiento social procedentes de múltiples contextos y puntos de datos pueden ser recopilados de manera centralizada por la misma entidad, pero en la mayoría de los casos se recopilan de forma distribuida y se combinan a partir de diferentes fuentes, lo que puede implicar una mayor vigilancia y seguimiento de las personas (la denominada «datavigilancia»).

158) En el segundo escenario, la puntuación se basa en **características personales o de la personalidad**, que pueden incluir, o no, aspectos específicos del comportamiento social. Entre las «características personales» pueden figurar diferentes datos relativos a una persona, como, por ejemplo, el sexo, la orientación sexual o las características sexuales, el género, la identidad de género, la raza, la etnia, la situación familiar, la dirección, los ingresos, los miembros del hogar, la profesión, el empleo o cualquier otra situación jurídica, el rendimiento en el trabajo, la situación económica, la liquidez financiera, la salud, las preferencias personales, los intereses, la fiabilidad, el comportamiento, la localización o el desplazamiento, el nivel de endeudamiento, el tipo de vehículo, etc.[117]. En principio, las «características de la personalidad» deben interpretarse como sinónimo de características personales, pero también pueden implicar la elaboración de perfiles específicos de individuos como personalidades. Las características de la personalidad también pueden basarse en una serie de factores e implicar un juicio, que puede ser emitido por las propias personas, por otras personas o ser generado por sistemas de IA. En el Reglamento de Inteligencia Artificial, las características de la personalidad se denominan a veces «rasgos y características de la personalidad»[118]; estos conceptos deben interpretarse de manera coherente.

159) Las características personales o de la personalidad «conocidas, inferidas o predichas» son diferentes tipos de información y datos personales que deben distinguirse. Las «**características conocidas**» se basan en la información de entrada que se ha proporcionado al sistema de IA y que, en la mayoría de los casos, es información verificable. En cambio, las «**características inferidas**» se basan en información que se ha deducido de otra información, normalmente a través de un sistema de IA. Las «**características predichas**» son las que se estiman sobre la base de patrones con una precisión inferior al 100 %. Los conceptos de datos «inferidos» (o derivados) también

116 Véase el considerando 31 del Reglamento de Inteligencia Artificial.
117 Véase el considerando 42 del Reglamento de Inteligencia Artificial, en donde se enumeran algunos ejemplos de dichas características.
118 Artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial.

se utilizan en el contexto de la elaboración de perfiles en la legislación de la Unión en materia de protección de datos y, por tanto, pueden servir de inspiración a la hora de interpretar los conceptos utilizados en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial[119]. El uso de estos diferentes tipos de datos puede tener distintas implicaciones para la exactitud y la equidad de las prácticas de puntuación y, por tanto, puede tenerse en cuenta, en particular cuando el tratamiento es opaco o se basa en puntos de datos cuya exactitud es más difícil de verificar.

4.2.2. La puntuación ciudadana debe dar lugar a un trato perjudicial o desfavorable en contextos sociales que no guardan relación o a un trato injustificado o desproporcionado con respecto a la gravedad del comportamiento social.

a) Relación causal entre la puntuación ciudadana y el trato

160) Para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial, la puntuación ciudadana creada por un sistema de IA o con su ayuda debe **dar lugar a un trato perjudicial o desfavorable** para la persona o el colectivo de personas evaluadas. En otras palabras, el trato debe ser la consecuencia de la puntuación; la puntuación, la causa del trato. Esta relación de causalidad plausible también puede existir en los casos en que las consecuencias perjudiciales aún no se hayan materializado, pero el sistema de IA esté destinado o sea capaz de producir tal resultado adverso. Esto es especialmente pertinente dado que la práctica prohibida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial también cubre la «introducción en el mercado» de dichos sistemas de IA.

161) El artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial no exige que la evaluación o la clasificación realizada por el sistema de IA sea la única causa del trato perjudicial o desfavorable. Por lo tanto, contempla igualmente las prácticas de puntuación que posibilita la IA que también pueden ser objeto de otras evaluaciones humanas o combinarse con ellas. Al mismo tiempo, los resultados de salida de la IA deben desempeñar un papel suficientemente importante en la obtención de la puntuación ciudadana. Por ejemplo, en el caso de que una autoridad pública despliegue un sistema de IA para evaluar la fiabilidad de las personas y combine sus resultados de salida con una valoración humana de hechos adicionales, esta práctica de puntuación ciudadana que posibilita la IA solo entrará en el ámbito de aplicación de la prohibición si la puntuación generada por la IA desempeña un papel suficientemente importante en la decisión final, siempre que se cumplan las demás condiciones de trato perjudicial o desfavorable, tal como se describe más adelante [véase la sección 4.2.2, letra b)].

162) Una puntuación puede dar lugar a un trato perjudicial o desfavorable, incluso si la produce una o varias organizaciones distintas de la que la utiliza[120]. Por ejemplo, una

---

119 Véanse las Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679, WP251rev.01, 6.2.2018, p. 7 y siguientes.

120 Esta interpretación es coherente con la sentencia del TJUE en el asunto SCHUFA I, en la que el TJUE sostuvo, en el contexto de las decisiones automatizadas, que un *score* (evaluación que constituye una elaboración de perfiles) producido por una entidad distinta de la que adopta la decisión final puede constituir una decisión automatizada en el sentido del artículo 22 del RGPD. Véase la sentencia SCHUFA I, apartados 42 a 51 y 60 a 62.

autoridad pública puede obtener una puntuación para la evaluación de la solvencia de una persona física producida por otra empresa especializada en evaluaciones de solvencia y de riesgos, y que se basa en información sobre las personas y su comportamiento procedente de diversas fuentes.

b) Trato perjudicial o desfavorable en contextos sociales que no guardan relación o trato injustificado o desproporcionado

163) La última condición para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial es que el uso de la puntuación ciudadana debe dar lugar (o puede dar lugar) a un trato perjudicial o desfavorable:

i. que se produzca en contextos sociales que no guardan relación con los contextos donde se generaron o recabaron los datos originalmente, o

ii. que esté injustificado o sea desproporcionado en relación con su comportamiento social o su gravedad.

164) Estas condiciones son alternativas y pueden aplicarse también de forma combinada. Se necesita un análisis caso por caso para determinar si se cumple al menos una de ellas, ya que muchas prácticas de puntuación y evaluación que posibilita la IA pueden no cumplirlas y, por tanto, quedar fuera del ámbito de aplicación de la prohibición. En particular, este puede no ser el caso cuando las prácticas de puntuación que posibilita la IA tienen una finalidad de evaluación legítima específica y cumplen la legislación nacional y de la Unión aplicable que especifica los datos considerados pertinentes a efectos de la evaluación y garantiza que el trato perjudicial o desfavorable está justificado y es proporcionado al comportamiento social (véase la sección 4.3 «Fuera del ámbito de aplicación»).

165) Por «**trato desfavorable**» se entiende el hecho de que, como consecuencia de la puntuación, la persona o el colectivo de personas debe recibir un trato menos favorable que otras sin exigir necesariamente un perjuicio o un daño concreto; este es, por ejemplo, el caso de las prácticas de puntuación en las que se selecciona a personas para inspecciones adicionales en caso de sospecha de fraude. En cambio, un trato «**perjudicial**» exige que la persona o el colectivo de personas sufra un determinado daño o perjuicio como consecuencia del trato. Un trato desfavorable o perjudicial también puede ser discriminatorio y estar prohibido por el Derecho de la Unión en materia de no discriminación o implicar la exclusión de determinadas personas o colectivos,[121] pero no es una condición necesaria para que se aplique la prohibición. Así pues, el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial podría aplicarse al trato injusto más allá de la legislación de la UE en materia de no discriminación, que solo se aplica a determinados colectivos protegidos (por ejemplo, por motivos de edad, origen étnico y racial, sexo o religión).

[121] Considerando 31 del Reglamento de Inteligencia Artificial.

Escenario 1: Trato perjudicial o desfavorable en contextos sociales que no guardan relación

166) En el primer escenario descrito en el artículo 5, apartado 1, letra c), inciso i), del Reglamento de Inteligencia Artificial, el trato perjudicial o desfavorable resultante de la puntuación debe tener lugar **en contextos sociales que no guarden relación** con los contextos donde se generaron o recabaron los datos originalmente. Esto implica no solo que las personas puedan ser tratadas de manera desfavorable o perjudicial debido a la puntuación ciudadana, sino también que los datos relativos a su comportamiento social o a sus características personales o de la personalidad conocidas, inferidas o predichas se generan o recaban en contextos sociales que no guardan relación con el contexto en el que tiene lugar la puntuación. Los datos recabados o generados en estos contextos que no guardan relación deben ser utilizados posteriormente por el sistema de IA para la puntuación de las personas sin un vínculo aparente a efectos de la evaluación o la clasificación o de tal forma que conduzca a una vigilancia generalizada de las personas o colectivos de personas. En la mayoría de los casos, esto va en contra de las expectativas razonables de las personas e infringe la legislación de la Unión en materia de protección de datos y, posiblemente, otras normas aplicables que especifican los tipos de datos y fuentes que se consideran pertinentes y necesarios para la evaluación o la clasificación. El cumplimiento de esta condición requerirá una evaluación caso por caso, en la que se tendrán en cuenta la finalidad de la evaluación y los contextos en los que se recabaron y generaron los datos.

Ejemplos de trato perjudicial o desfavorable en contextos sociales que no guardan relación prohibidos en virtud del artículo 5, apartado 1, letra c), inciso i), del Reglamento de Inteligencia Artificial

- Las autoridades tributarias nacionales utilizan una herramienta predictiva de IA en todas las declaraciones tributarias de los contribuyentes de un país para seleccionar aquellas que deberán examinarse de forma más exhaustiva. La herramienta de IA utiliza variables pertinentes, como los ingresos anuales, los activos (bienes inmuebles, automóviles, etc.) o datos sobre los familiares de los beneficiarios, pero también datos no relacionados, como los hábitos sociales de los contribuyentes o sus conexiones a internet, con el objetivo de seleccionar a personas concretas para las inspecciones.
- Una agencia de asistencia social utiliza un sistema de IA para estimar la probabilidad de fraude de los beneficiarios de prestaciones familiares sobre la base de características recabadas o inferidas a partir de contextos sociales sin relación o pertinencia aparente para evaluar el fraude, como tener un cónyuge de una determinada nacionalidad u origen étnico, disponer de conexión a internet, el comportamiento en plataformas sociales, el rendimiento en el lugar de trabajo, etc.[122] En cambio, los datos pertinentes para la concesión de las prestaciones y que han sido recabados de forma lícita podrían utilizarse para determinar el riesgo de fraude, ya que

[122] Para ver una comparación entre sistemas nacionales similares de prestaciones y la puntuación ciudadana, véase Hadwick, D. y Lan, S., «Lessons to Be Learned from the Dutch Childcare Allowance Scandal: A Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany» [«Lecciones que aprender del escándalo holandés de la prestación por cuidado de hijos: una revisión comparativa de la gobernanza algorítmica de las administraciones tributarias de Países Bajos, Francia y Alemania», documento no disponible en español], *World Tax Journal*, vol. 13, n.º 4, Familiales (CNAF), 2021.

las autoridades públicas persiguen un objetivo legítimo cuando comprueban si las prestaciones sociales se conceden correctamente.

- Una agencia pública de empleo utiliza un sistema de IA para puntuar a las personas desempleadas sobre la base de una entrevista y una evaluación basada en la IA para determinar si deben recibir apoyo estatal para el empleo. Esta puntuación se basa en características personales pertinentes, como la edad y la educación, pero también en variables recabadas o inferidas a partir de datos y contextos que no guardan relación aparente con la finalidad de la evaluación, como el estado civil, datos de salud sobre enfermedades crónicas, adicciones, etc.[123]

Estas prácticas de puntuación inaceptables pueden distinguirse de las prácticas lícitas que evalúan a las personas para fines específicos de conformidad con el Derecho de la Unión y nacional, en particular cuando dichas normas, de conformidad con el Derecho de la Unión, especifican los datos que se consideran pertinentes y necesarios a efectos de la evaluación (véase la sección 4.3 «Fuera del ámbito de aplicación»).

Escenario 2: Trato desfavorable o perjudicial desproporcionado con respecto al comportamiento social

167) Otro supuesto alternativo contemplado en el artículo 5, apartado 1, letra c), inciso ii), del Reglamento de Inteligencia Artificial en el que puede prohibirse un sistema de puntuación de IA es si el trato resultante de la puntuación está injustificado o es desproporcionado en relación con la gravedad del comportamiento social. La gravedad del impacto y la injerencia en los derechos fundamentales de la persona afectada resultante de la puntuación ciudadana en relación con la gravedad del comportamiento social de la persona deben determinar si dicho trato es desproporcionado para el objetivo legítimo perseguido, teniendo en cuenta el principio general de proporcionalidad. Esto requiere una evaluación caso por caso, que debe tener en cuenta todas las circunstancias pertinentes del caso, así como consideraciones éticas generales y principios de equidad y justicia social relacionados con la evaluación del comportamiento social y la proporcionalidad del trato perjudicial. El trato también puede estar «injustificado», por ejemplo, si carece de un objetivo legítimo. La legislación sectorial nacional o de la Unión que establezca criterios y procedimientos específicos que regulen ese trato potencialmente perjudicial o desfavorable también puede ser pertinente para dicha evaluación.

Ejemplos de trato injustificado o desproporcionado en relación con el comportamiento prohibido en virtud del artículo 5, apartado 1, letra c), inciso ii), del Reglamento de Inteligencia Artificial

- Un organismo público utiliza un sistema de IA para elaborar los perfiles de familias con vistas a la detección precoz de menores en situación de riesgo basándose en criterios como la salud mental de los progenitores y el desempleo, así como la

[123] En Polonia se utilizó un sistema similar para elaborar los perfiles de los desempleados, que se abandonó tras ser declarado inconstitucional. Véase Szymielewicz, *Profiling the unemployed in Poland: Social and Political Implications of Algorithmic Decision Making* [«Elaboración del perfil de los desempleados en Polonia: implicaciones sociales y políticas de la toma de decisiones algorítmica», documento no disponible en español], Fundacja Panoptykon, 2015, p. 18.

información sobre el comportamiento social de los progenitores procedente de múltiples contextos. En función de la puntuación resultante, se selecciona a las familias para inspeccionarlas y se separa de ellas a los niños considerados «en situación de riesgo», incluso en caso de transgresiones leves cometidas por los padres, como faltar en ocasiones a las citas médicas o recibir multas de tráfico.

- Un municipio utiliza un sistema de IA para puntuar la fiabilidad de los residentes sobre la base de múltiples puntos de datos relacionados con su comportamiento social en diversos contextos. La puntuación generada para los residentes considerados «menos fiables» se utiliza para incluirlos en una lista negra; esto conlleva la revocación de prestaciones públicas, otras medidas punitivas graves y un mayor control o vigilancia. Entre los factores que se tienen en cuenta en la evaluación figuran la falta de voluntariado y las faltas leves, como no devolver los libros a la biblioteca a tiempo, dejar la basura en la calle fuera del día de recogida y retrasarse en el pago de los impuestos municipales.

Estas prácticas de puntuación ciudadana inaceptables pueden distinguirse de las prácticas lícitas que evalúan a las personas para un fin legítimo específico de conformidad con el Derecho de la Unión y nacional, en particular cuando dichas normas garantizan que el trato perjudicial o desfavorable está justificado o es proporcionado en relación con el comportamiento social (véase la sección 4.3 «Fuera del ámbito de aplicación»).

168) Ambas situaciones descritas en el artículo 5, apartado 1, letra c), incisos i) y ii), del Reglamento de Inteligencia Artificial también pueden ocurrir de forma simultánea.

Ejemplos de trato injustificado o desproporcionado en virtud del artículo 5, apartado 1, letra c), incisos i) y ii), del Reglamento de Inteligencia Artificial

- Una autoridad tributaria utiliza un sistema de IA para detectar fraudes en las prestaciones por hijos mediante la elaboración de perfiles y la asignación de beneficiarios sospechosos de fraude a categorías como «intencionalidad o negligencia grave» utilizando criterios como los bajos ingresos, la doble nacionalidad, el comportamiento social, etc. Sobre la base de la puntuación de riesgo, se examina el expediente de un beneficiario y, en numerosas ocasiones, se suspende su prestación por cuidado de hijos, recibe un aviso para que devuelva las prestaciones recibidas y ya no puede acogerse a los mecanismos habituales de cobro de deudas. Esta puntuación provoca el gran endeudamiento de muchas familias y da lugar a un trato injusto, discriminatorio y perjudicial para las personas y colectivos de personas[124], abocando a muchas familias a graves dificultades financieras.

- Una autoridad pública utiliza un sistema de IA para controlar el fraude en el proceso de concesión de prestaciones para el alojamiento de estudiantes que considera

[124] Para ver un ejemplo similar del escándalo en las prestaciones por cuidado de hijos en los Países Bajos, véase *Belastingdienst treft 232 Gezinnen met onevenredig harde actie*, 27.11.2019 [«La Administración Tributaria y Aduanera toma medidas desproporcionadamente severas contra 232 familias», no disponible en español]. Un tribunal neerlandés declaró en 2020 que el «Systeem Risico Indicatie» (SyRi) era ilícito. Véase también Geen powerplay maar fair play.Onevenredig harde aanpak van 232 Gezinnen met kinderopvangtoeslag [«No es un juego de poder, sino juego limpio. Medidas desproporcionadamente severas contra 232 personas con prestación por cuidado de los hijos», no disponible en español], 2017, p. 32.

indicadores como las conexiones a internet, la situación familiar o el nivel educativo de los beneficiarios como factores distintivos del riesgo de fraude, lo que no parece ni pertinente ni justificado.

- Un Gobierno introduce un sistema integral basado en la IA que supervisa y evalúa a los ciudadanos en función de su comportamiento en diferentes aspectos de la vida, como las interacciones sociales, las actividades en línea, los hábitos de compra y la puntualidad en el pago de facturas. Las personas con una puntuación más baja se enfrentan a restricciones de acceso a los servicios públicos, a unos tipos de interés más elevados en los préstamos y a dificultades para viajar, alquilar apartamentos e incluso encontrar empleo. El sistema da lugar a una vigilancia excesiva de las personas y a un trato perjudicial en contextos que no guardan relación con el comportamiento social utilizado para determinar la puntuación social (por ejemplo, la actividad en las redes sociales influye en las oportunidades de empleo), al tiempo que impone sanciones excesivas por infracciones menores (por ejemplo, desventajas sociales y financieras para infracciones relativamente leves).

Estas prácticas de puntuación ciudadana inaceptables pueden distinguirse de las prácticas lícitas que evalúan a las personas para fines legítimos específicos que no cumplen estas condiciones y son conformes al Derecho de la Unión y nacional, en particular cuando dichas normas garantizan que el trato perjudicial o desfavorable está justificado o es proporcionado y se utilizan datos procedentes de contextos sociales relacionados (véase la sección 4.3 «Fuera del ámbito de aplicación»).

169) La prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial también puede comprender los casos en los que se otorgan concesiones o se da un trato preferente a determinadas personas o colectivos de personas, ya que esto implica un trato menos favorable a otras personas [por ejemplo, en el caso de los programas de apoyo al empleo, el acceso (no) prioritario a la vivienda o la reinstalación].

4.2.3. Con independencia de que sean proporcionados o utilizados por personas públicas o privadas

170) Como ya se ha señalado, el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial prohíbe las prácticas inaceptables de puntuación ciudadana que posibilita la IA, con independencia de que el sistema de IA o la puntuación sean proporcionados o utilizados por personas públicas o privadas. Si bien la puntuación en el sector público puede tener graves consecuencias para las personas debido al desequilibrio de poder y a la dependencia de los servicios públicos, también pueden producirse consecuencias igualmente perjudiciales en el sector privado, donde las prácticas de puntuación son cada vez más frecuentes en las empresas y en otras entidades.

A continuación, varios ejemplos:

- Una compañía de seguros recopila de un banco información sobre los gastos y otros datos financieros que no guardan relación con la determinación de la admisibilidad de

los candidatos para obtener un seguro de vida y que se utilizan para determinar el precio de la prima que debe pagarse por dicho seguro. Un sistema de IA analiza esta información y, sobre esta base, recomienda si se debe rechazar un contrato o fijar primas de seguro de vida más elevadas para una persona en particular o un grupo de clientes.

- Una agencia de crédito privada utiliza un sistema de IA para determinar la solvencia de las personas y decidir si concede un préstamo para vivienda a una persona basándose en características personales no relacionados.

Estas prácticas de puntuación ciudadana inaceptables pueden distinguirse de las prácticas lícitas que evalúan a las personas para fines legítimos específicos que no cumplen estas condiciones y son conformes al Derecho de la Unión y nacional, en particular cuando dichas normas garantizan que el trato perjudicial o desfavorable está justificado o es proporcionado y se utilizan datos procedentes de contextos sociales relacionados (véase la sección 4.3 «Fuera del ámbito de aplicación»).

171) En el caso de los controles efectuados por las autoridades de vigilancia del mercado competentes, corresponde al proveedor y al responsable del despliegue del sistema de IA, cada uno en el marco de sus responsabilidades, demostrar que la práctica de IA es legítima y está justificada; esto lo harán, en particular, siendo transparentes sobre el funcionamiento del sistema de IA y facilitando información sobre los tipos de datos y las fuentes de datos, garantizando que solo se traten aquellos relacionados con el contexto social en el que se utiliza la puntuación a efectos de la evaluación o clasificación, que el sistema funcione según lo previsto y que cualquier trato perjudicial o desfavorable resultante esté justificado y sea proporcionado al comportamiento social. El cumplimiento de la legislación aplicable y las garantías adecuadas y proporcionadas integradas en el sistema y aplicadas durante su funcionamiento ayudarán a evitar que se aplique la prohibición, permitiendo al mismo tiempo la utilización de sistemas de IA para la evaluación o clasificación de personas con fines legítimos y beneficiosos como, por ejemplo, mejorar la eficacia de los procesos, la calidad del servicio, la seguridad, etc. (véase la sección 4.3 «Fuera del ámbito de aplicación»).

172) Cumplir los requisitos aplicables a los sistemas de IA de alto riesgo (por ejemplo, en el ámbito de los servicios y prestaciones públicos esenciales, la calificación crediticia y la evaluación de solvencia, la migración, etc.) también puede ayudar a garantizar que los sistemas de IA utilizados para fines de evaluación y clasificación en esos ámbitos de alto riesgo no constituyan prácticas de puntuación ciudadana inaceptables que los proveedores y los responsables del despliegue deben tener en cuenta a la hora de cumplir sus respectivas obligaciones (por ejemplo, en materia de gestión de riesgos, transparencia, gobernanza de datos, evaluación de impacto relativa a los derechos fundamentales, supervisión humana, seguimiento, etc.).

4.3. Fuera del ámbito de aplicación

173) La prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial solo se aplica a la puntuación de personas físicas o colectivos de

personas; se excluye así, en principio, la puntuación de las entidades jurídicas cuando la evaluación no se base en características personales o de la personalidad o en el comportamiento social de las personas, aunque en algunos casos las personas puedan verse indirectamente afectadas por la puntuación (por ejemplo, todos los ciudadanos de un municipio cuando se repartan fondos). No obstante, si las entidades jurídicas se han evaluado sobre la base de una puntuación global que agrega la evaluación o clasificación de un colectivo de personas físicas en función de su comportamiento social o de sus características personales o de la personalidad y esa puntuación afecta directamente a dichas personas (por ejemplo, a todos los empleados de una empresa o a los estudiantes de una determinada escuela cuyo comportamiento haya sido evaluado), la práctica puede entrar en el ámbito de aplicación del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial si se cumplen todas las demás condiciones. Esto dependerá de una evaluación caso por caso.

174) La puntuación ciudadana basada en la IA como «valor de probabilidad» y pronóstico también debe distinguirse de las calificaciones individuales de los usuarios que evalúan la calidad de un servicio (por ejemplo, cuando se evalúa a un conductor en una plataforma digital de uso compartido de vehículos o a un anfitrión en una plataforma en línea de alojamientos). Dichas calificaciones son la mera suma de puntuaciones humanas individuales en las que no interviene necesariamente la IA, a menos que los datos se combinen con otra información y sean analizados por el sistema de IA a efectos de la evaluación o clasificación de personas que cumplan todas las condiciones del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial.

175) Además, la puntuación de las personas físicas no está siempre prohibida: solo lo está en los casos limitados en los que se cumplen acumulativamente todas las condiciones del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial, como se ha analizado anteriormente. En el considerando 31 del Reglamento de Inteligencia Artificial, en particular, se menciona que la prohibición «no debe afectar a prácticas lícitas de evaluación de las personas físicas que se efectúen para un fin específico de conformidad con el Derecho de la Unión y nacional». Por ejemplo, la calificación crediticia, la puntuación de riesgos y la suscripción son elementos fundamentales de los servicios de las empresas financieras y de seguros. Estas prácticas, junto con otras prácticas legítimas (a saber, mejorar la calidad y la eficiencia de los servicios, garantizar una tramitación más eficiente de las reclamaciones, llevar a cabo evaluaciones específicas de los empleados, prevenir y detectar el fraude, garantizar el cumplimiento del Derecho o puntuar el comportamiento de los usuarios en las plataformas en línea), no están prohibidas en sí mismas, siempre que sean lícitas y conformes al Reglamento de Inteligencia Artificial y a otras disposiciones aplicables del Derecho de la Unión y nacional, que deben ser conformes con el Derecho de la Unión.

176) En otras palabras, no están prohibidos los sistemas de IA que evalúan o clasifican a las personas para generar una puntuación ciudadana de manera lícita y para un fin específico en el contexto relacionado con aquel en el que se recabaron los datos personales utilizados para la puntuación, siempre que cualquier trato perjudicial o

desfavorable derivado del uso de la puntuación esté justificado y sea proporcionado a la gravedad del comportamiento social[125].

177) Así pues, el cumplimiento de la legislación sectorial de la Unión (como en el ámbito de la calificación crediticia, la lucha contra el blanqueo de capitales, etc.), que especifica el tipo de datos que pueden considerarse pertinentes y necesarios y, por tanto, utilizarse para el fin legítimo específico de la evaluación y garantiza que el tratamiento esté justificado y sea proporcionado al comportamiento social puede garantizar que la práctica de IA quede fuera del ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial.

Ejemplos de prácticas de puntuación legítimas conformes con el Derecho de la Unión y nacional que quedan fuera del ámbito de aplicación del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial

- Los sistemas de puntuación del crédito financiero utilizados por los prestamistas o las agencias de información crediticia para evaluar la solvencia financiera o las deudas pendientes de un cliente, proporcionar una puntuación crediticia o determinar su evaluación de solvencia, que se basan en los ingresos y gastos del cliente y otras circunstancias financieras y económicas, quedan fuera del ámbito de aplicación del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial si son pertinentes para la finalidad legítima de la calificación crediticia y si cumplen la legislación en materia de protección de los consumidores[126] que especifica el tipo de datos y las garantías necesarias para garantizar un trato justo de los consumidores en las evaluaciones de solvencia.

- Las empresas tienen un interés legítimo en evaluar a los clientes para detectar fraude financiero; estas prácticas no se ven afectadas por la prohibición si la evaluación se basa en datos pertinentes, como el comportamiento transaccional y los metadatos en el contexto de los servicios, el historial y otros factores procedentes de fuentes objetivamente pertinentes para determinar el riesgo de fraude y si el trato perjudicial está justificado y es proporcionado como consecuencia del comportamiento fraudulento.

- La información recopilada a través de dispositivos telemáticos que muestra que un conductor excede los límites de velocidad o no conduce de forma segura, utilizada por una aseguradora que ofrece tarifas telemáticas en relación con el comportamiento de alto riesgo al volante del tomador del seguro, puede utilizarse para aumentar la prima, debido al mayor riesgo de accidente que entraña dicho comportamiento, siempre que el aumento de la prima sea proporcional a ese comportamiento arriesgado.

- La recogida y el tratamiento de datos que son pertinentes y necesarios para la finalidad legítima prevista de los sistemas de IA (por ejemplo, datos de salud y datos sobre esquizofrenia recabados de diversas fuentes para diagnosticar a los pacientes) quedan

[125] Considerando 31 del Reglamento de Inteligencia Artificial.

[126] Véanse, en particular, la Directiva (UE) 2023/2225, de 18 de octubre de 2023, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 2008/48/CE, y las Directrices de la Autoridad Bancaria Europea sobre originación y seguimiento de préstamos de 29 de mayo de 2020, EBA/GL/2020/06.

fuera del ámbito de aplicación del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial, en particular porque tratan datos pertinentes y necesarios y, por lo general, no implican un trato perjudicial o desfavorable injustificado de determinadas personas físicas.

- Las plataformas en línea que elaboran perfiles de los usuarios por motivos de seguridad en sus servicios, basándose en datos que resultan pertinentes para el contexto y la finalidad de la evaluación, quedan fuera del ámbito de aplicación del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial si la evaluación no da lugar a un trato perjudicial desproporcionado en relación con la gravedad del comportamiento indebido del usuario.
- La publicidad comercial personalizada que posibilita la IA queda fuera del ámbito de aplicación cuando se basa en datos pertinentes (por ejemplo, las preferencias de los usuarios), se hace de conformidad con el Derecho de la Unión en materia de protección de los consumidores, protección de datos y servicios digitales y no da lugar a un trato perjudicial o desfavorable desproporcionado en relación con la gravedad del comportamiento social del usuario (por ejemplo, precios diferenciales abusivos e injustos).
- Los sistemas de IA que utilizan datos recogidos en campamentos de refugiados (por ejemplo, los relativos al cumplimiento de las normas de comportamiento) para tomar decisiones sobre reasentamiento o empleo no se ven afectados por la prohibición, puesto que estos datos son pertinentes a efectos de la evaluación, y siempre que se cumplan los procedimientos contemplados en el Derecho de la Unión aplicable en materia de migración para garantizar que el tratamiento esté justificado y sea proporcionado.
- La puntuación que posibilita la IA de una plataforma de compras en línea que ofrece ciertas ventajas a los usuarios con un sólido historial de compras y una baja tasa de devoluciones (como, por ejemplo, un proceso de solicitud de devoluciones más rápido o reembolsos sin devolución) queda fuera del ámbito de aplicación del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial; en este caso, las ventajas están justificadas y son proporcionadas, ya que recompensan los comportamientos positivos y los otros usuarios siguen teniendo acceso al proceso estándar de devolución.
- La evaluación y puntuación de personas mediante IA por parte de la policía y otras autoridades garantes del cumplimiento del Derecho que recopilan datos sobre el comportamiento social de las personas en múltiples contextos quedan fuera del ámbito de aplicación del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial cuando dichos datos son pertinentes para los fines específicos de prevención, detección, enjuiciamiento y sanción de delitos, así como cuando el trato perjudicial está justificado y es proporcionado de conformidad con el Derecho penal y policial sustantivo y de procedimiento de la Unión y nacional. En este contexto, también es pertinente tener en cuenta la prohibición del artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, que impone condiciones adicionales más

específicas para las evaluaciones de riesgos que posibilita la IA y las predicciones de la probabilidad de que una persona cometa un delito, que no deben basarse únicamente en la elaboración de perfiles o en la evaluación de los rasgos de la personalidad (véase la sección 5).

4.4. Relación con otros actos jurídicos de la Unión

178) Los proveedores y los responsables del despliegue deben evaluar detenidamente si se aplica otra normativa nacional y de la Unión a cualquier sistema de puntuación de IA que utilice en sus actividades; en particular, deben examinar si existe legislación más específica que regule estrictamente los tipos de datos que pueden considerarse pertinentes y necesarios y, por tanto, se usan con fines de evaluación específicos, así como si hay normas y procedimientos más específicos para garantizar un trato justificado y justo.

179) Las prácticas de puntuación ciudadana que posibilita la IA llevadas a cabo por entidades privadas que actúan como comerciantes en las relaciones entre las empresas y los consumidores también pueden infringir la legislación de la Unión en materia de protección de los consumidores, es decir, la Directiva 2005/29/CE relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores (en lo sucesivo, «Directiva sobre las prácticas comerciales desleales»). La Directiva sobre las prácticas comerciales desleales prohíbe las prácticas comerciales que sean contrarias a los requisitos de la diligencia profesional y distorsionen o puedan distorsionar de manera sustancial el comportamiento económico del consumidor medio o del miembro medio del grupo con respecto al producto de que se trate (artículo 5 de la Directiva sobre las prácticas comerciales desleales). Las prácticas de puntuación también pueden considerarse engañosas (artículos 6 a 7 de dicha Directiva), a reserva de que se evalúe caso por caso el impacto de la práctica comercial en la decisión del consumidor sobre una transacción.

180) La puntuación ciudadana, ya sea por parte de entidades públicas o privadas, también puede infringir la legislación de la Unión en materia de protección de datos, por ejemplo, en lo que respecta al fundamento jurídico para el tratamiento (licitud), los principios de protección de datos (por ejemplo, minimización y necesidad de datos, lealtad y transparencia) y cualquier otra obligación, incluidas las normas sobre las decisiones individuales totalmente automatizadas, cuando proceda.

181) Cuando la evaluación o clasificación se base en uno de los motivos protegidos contra la discriminación (como la edad, la religión, el origen racial o étnico, el sexo, etc.) o dé lugar, directa o indirectamente, a la discriminación de esos colectivos, dicha práctica también estará sujeta al Derecho de la Unión en materia de no discriminación.

182) La Directiva (UE) 2023/2225[127] sobre créditos al consumo también puede ser pertinente en este contexto. El artículo 18, apartado 3, de dicha Directiva exige que la evaluación de solvencia se lleve a cabo sobre la base de información pertinente y exacta sobre los

[127] Directiva 2008/48/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2008, relativa a los contratos de crédito al consumo y por la que se deroga la Directiva 87/102/CEE del Consejo (DO L 133 de 22.5.2008, p. 66).

ingresos y gastos del consumidor y otras circunstancias financieras y económicas que sean necesarias y proporcionadas en relación con la naturaleza, la duración, el valor y los riesgos del crédito para el consumidor. Dicha información puede incluir datos que demuestren ingresos u otras fuentes de reembolso, información sobre activos y pasivos financieros, o información sobre otros compromisos financieros. La Directiva prohíbe explícitamente la inclusión de categorías especiales de datos personales en la información y la obtención de información de las redes sociales. En las Directrices de la Autoridad Bancaria Europea sobre concesión y seguimiento de préstamos[128] se especifica mejor la información pertinente a efectos de las evaluaciones de solvencia. Esta especificación del tipo de datos en esta legislación sectorial con fines de evaluación específicos son consideraciones pertinentes que deben tenerse en cuenta al determinar si una práctica entra en el ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial.

183) Del mismo modo, los sistemas de IA utilizados para la evaluación y clasificación de personas a efectos de la lucha contra el blanqueo de capitales y la financiación del terrorismo también deben cumplir la legislación pertinente de la Unión sobre estas cuestiones.

5. ARTÍCULO 5, APARTADO 1, LETRA D), DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: EVALUACIÓN INDIVIDUAL DE RIESGOS Y PREDICCIÓN DE DELITOS

184) El artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial prohíbe los sistemas de IA que valoran o predicen el riesgo de que una persona física comenta un delito basándose únicamente en la elaboración de perfiles o en los rasgos y características de la personalidad.

185) A tenor de la última frase de la disposición, la prohibición no se aplica si el sistema de IA se utiliza para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se basa en hechos objetivos y verificables directamente relacionados con dicha actividad. Los sistemas de IA que quedan fuera del ámbito de aplicación de la prohibición, destinados a ser utilizados por las autoridades garantes del cumplimiento del Derecho, o en su nombre, o por las instituciones, órganos u organismos de la Unión en apoyo de las autoridades garantes del cumplimiento del Derecho para evaluar el riesgo de que una persona física cometa un delito o reincida en la comisión de un delito atendiendo no solo a la elaboración de perfiles o a la evaluación de rasgos y características de la personalidad o comportamientos delictivos pasados se clasifican como sistemas de IA de «alto riesgo» [anexo III, punto 6, letra d), del Reglamento de Inteligencia Artificial] y deben cumplir todos los requisitos y obligaciones pertinentes establecidos en el Reglamento de Inteligencia Artificial.

5.1. Justificación y objetivos

[128] Directrices sobre concesión y seguimiento de préstamos de la Autoridad Bancaria Europea, de 29 de mayo de 2020, EBA/GL/2020/06.

186) En el considerando 42 del Reglamento de Inteligencia Artificial se explica el contexto y la justificación de la prohibición establecida en el artículo 5, apartado 1, letra d), de dicho Reglamento, a saber, que las personas físicas deben ser juzgadas basándose en su comportamiento real y no en comportamientos predichos por una IA basados únicamente en la elaboración de sus perfiles o en los rasgos o características de su personalidad.

5.2. Conceptos fundamentales y componentes de la prohibición

> ***Según el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial:***
>
> Quedan prohibidas las siguientes prácticas de IA:
>
> d) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de un sistema de IA para realizar evaluaciones de riesgos de personas físicas con el fin de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad; esta prohibición no se aplicará a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se basa en hechos objetivos y verificables directamente relacionados con una actividad delictiva;

187) Deben cumplirse varias condiciones acumulativas para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial:

(i) La práctica debe suponer la «introducción en el mercado», la «puesta en servicio para este fin específico» o el «uso» de un sistema de IA.

(ii) El sistema de IA debe realizar evaluaciones de riesgos que valoren o predigan el riesgo de que una persona física cometa un delito.

(iii) La evaluación de riesgos o la predicción debe basarse únicamente en uno de los elementos siguientes, o en ambos:

  (a) la elaboración del perfil de una persona física, o

  (b) la evaluación de los rasgos y características de la personalidad de una persona física.

188) Para que se aplique la prohibición, deben cumplirse simultáneamente las tres condiciones. Ya se ha examinado la primera condición, a saber, la «introducción en el mercado», «puesta en servicio» o «utilización» de un sistema de IA en la sección 2.3. Así pues, la prohibición se aplica tanto a los proveedores como a los responsables del despliegue de sistemas de IA, cada uno dentro de sus respectivas responsabilidades de no introducir en el mercado, poner en servicio o utilizar dichos sistemas de IA para este fin específico. A continuación se analizan las otras dos condiciones para que se aplique la prohibición.

5.2.1. Evaluar el riesgo o predecir la probabilidad de que una persona cometa un delito

189) Las evaluaciones de riesgos para valorar o predecir el riesgo de que una persona cometa un delito se denominan «predicción de delitos» o «previsión de delitos». Si bien no existe una definición consensuada de «predicción de delitos» o «previsión de delitos»[129], estos términos se refieren en general a una serie de tecnologías avanzadas de IA y métodos analíticos aplicados a grandes cantidades de datos, a menudo históricos (como datos socioeconómicos, pero también antecedentes policiales, etc.), que se utilizan en combinación con teorías criminológicas para predecir la delincuencia y sirven como base para orientar las estrategias policiales y de garantía del cumplimiento del Derecho en la lucha contra la delincuencia, así como en su control y su prevención[130].

190) Los sistemas de IA de predicción de delitos detectan patrones dentro de los datos históricos, asociando indicadores con la probabilidad de que se cometa un delito y, a continuación, generan resultados predictivos en forma de puntuaciones de riesgo. Por ejemplo, estos sistemas pueden utilizarse para planificar unidades operativas policiales, supervisar situaciones de alto riesgo y realizar controles a personas que, según las predicciones, pueden cometer (de nuevo) delitos. Ofrecen a las autoridades garantes del cumplimiento del Derecho, especialmente a las que disponen de recursos limitados, posibilidades de aumentar su eficacia y adoptar un enfoque proactivo para detectar, desalentar y anticipar los delitos[131]. Sin embargo, usar datos históricos sobre delitos cometidos para predecir el comportamiento futuro de otras personas puede perpetuar o incluso reforzar los sesgos. Esto puede hacer que se «pasen por alto» circunstancias individuales cruciales cuando estas circunstancias no forman parte del conjunto de datos o no se tienen en cuenta en los algoritmos con los que funciona el sistema de IA en cuestión. Esto también puede socavar la confianza pública en las autoridades garantes del cumplimiento del Derecho y en el sistema judicial en general[132].

191) En principio, estas evaluaciones y predicciones de riesgos son prospectivas y se refieren a delitos futuros (aún no cometidos) o a delitos que, según las evaluaciones, corren el riesgo de cometerse en ese momento, incluso si se trata de una tentativa o de actividades preparatorias emprendidas con vistas a cometer un delito[133]. Pueden llevarse a cabo en cualquier fase de las actividades de garantía del cumplimiento del Derecho, como en la prevención y la detección de delitos, pero también durante la investigación, el enjuiciamiento y la ejecución de sanciones penales (incluso cuando las autoridades judiciales evalúan el riesgo de reincidencia, por ejemplo, en el contexto de la toma de

---

129 Véanse, por ejemplo, los sistemas mencionados en el manual de la Agencia de los Derechos Fundamentales de la Unión Europea, como el Criminality Awareness System (CAS) en los Países Bajos y Precobs en Alemania y Suiza, *Guía para prevenir la elaboración ilícita de perfiles en la actualidad y en el futuro*, Manual, 2018, p. 138.

130 Véase Europol, *AI and policing: The benefits and challenges of artificial intelligence for law enforcement. An Observatory Report from the Europol Innovation Lab* [«La inteligencia artificial y la labor policial: beneficios y desafíos para las autoridades garantes del cumplimiento del Derecho», documento no disponible en español], 23 de septiembre de 2024. Véase también Yang, F. «Predictive Policing» [«Policía predictiva», documento no disponible en español], en *Oxford Research Encyclopedia, Criminology and Criminal Justice*, Oxford University Press, 2019.

131 Por ejemplo, OxRec (Oficina neerlandesa de libertad condicional, «Reclassering Nederland»), *Prediction of violent reoffending in prisoners and individuals on probation: a Dutch validation study (OxRec) - PMC (nih.gov)* [«Predicción de la reincidencia violenta en reclusos y personas en libertad vigilada», documento no disponible en español].

132 Véase, por ejemplo, Agencia de los Derechos Fundamentales de la UE (8 de diciembre de 2022), *Bias in algoritms - Artificial intelligence and discrimination* [«Sesgos en los algoritmos — Inteligencia artificial y discriminación», documento no disponible en español»].Agencia de los Derechos Fundamentales de la Unión Europea.

133 Véase, a este respecto, el considerando 42 del Reglamento de Inteligencia Artificial, que se refiere a la «probabilidad de que cometan un delito» y a la «comisión de un delito real o potencial», en donde se utiliza el presente, y no el pasado.

decisiones sobre la imposición de la prisión provisional), así como en el marco del plan de reinserción social de las personas tras cumplir una condena penal[134].

192) La prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial no prohíbe las prácticas de predicción de delitos y de evaluación de riesgos como tales. Solo se aplica a los sistemas de IA destinados a realizar evaluaciones de riesgos para valorar o predecir el riesgo de que una persona física cometa un delito, cuando también se cumpla la tercera condición mencionada anteriormente. Además, como se ha señalado, la prohibición no se aplica a las situaciones contempladas en la exclusión expresa que figura la última frase del artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial.

5.2.2. Basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad

193) La tercera condición para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial es que la evaluación de riesgos para valorar o predecir el riesgo de que una persona física cometa un delito debe basarse únicamente en a) la elaboración del perfil de la persona o b) la evaluación de los rasgos y características de su personalidad.

194) La prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial se aplica con independencia de que el sistema de IA elabore perfiles o evalúe simultáneamente los rasgos y características de la personalidad de una sola persona física o de un colectivo de personas físicas, ya que el objetivo de la prohibición es proteger a toda persona respecto de quien se predice o evalúa el riesgo de cometer un delito.

a) Elaboración del perfil de una persona física

195) A diferencia del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial, en el artículo 5, apartado 1, letra d), se utiliza explícitamente el término «elaboración de perfiles». El artículo 3, punto 52, del Reglamento de Inteligencia Artificial define dicho término refiriéndose a su definición en el artículo 4, punto 4, del RGPD[135]. Uno de los elementos esenciales del concepto de elaboración de perfiles es el objetivo de «evaluar determinados aspectos personales»[136]. En el contexto del artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, la elaboración

---

134 Por ejemplo, el artículo 24, apartado 4, de la Directiva 2011/93/UE relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil exige que las personas que sean objeto de procesos penales o condenadas por actos relacionados con el abuso sexual de menores se sometan a una evaluación de su peligrosidad en materia de reincidencia.

135 El artículo 3, punto 4, de la Directiva sobre protección de datos en el ámbito penal, que es pertinente para la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, define la elaboración de perfiles de manera idéntica a como lo hace el artículo 4, punto 4, del RGPD, definiéndola como «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física». La misma definición figura también en el artículo 3, punto 5, del Reglamento (UE) 2018/1725, relativo al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión (DO L 295 de 21.11.2018, p. 39).

136 Véanse también las Directrices del Grupo de Trabajo del Artículo 29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento (UE) 2016/679, 6 de febrero de 2018, WP251rev.01, aprobadas por el CEPD, p.7. Véase también Agencia de los Derechos Fundamentales, *Guía para prevenir la elaboración ilícita de perfiles en la actualidad y en el futuro*, Manual, 2018, p. 138.

de perfiles se realiza con el fin de valorar o predecir el riesgo de que una persona cometa un delito.

196) El concepto de la denominada «elaboración de perfiles de grupo»[137] también puede ser pertinente en este contexto. Se refiere a la construcción de un perfil descriptivo y a su aplicación a un grupo determinado, por ejemplo, a determinadas categorías de autores de delitos (como terroristas, gánsteres, etc.), a partir de datos históricos sobre delitos cometidos anteriormente por otras personas. Estos perfiles de grupo pueden utilizarse más adelante para valorar y predecir el riesgo de que otras personas cometan delitos similares. Siempre que un sistema de IA haga una predicción y aplique dicho perfil (de grupo) a una persona concreta, esto constituye una elaboración de perfiles y, por tanto, puede entrar en el ámbito de aplicación de la prohibición del artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial.

b) Evaluación de los rasgos y características de la personalidad

197) La prohibición también se aplica si la evaluación de riesgos destinada a valorar o predecir el riesgo de que la persona cometa un delito se basa únicamente en la evaluación de los rasgos y características de su personalidad. Esta evaluación o predicción se suele incluir en el concepto de elaboración de perfiles, pero también podría considerarse una alternativa, en caso de que no se pueda establecer la elaboración de perfiles tal como se define en el artículo 4, punto 4, del RGPD.

198) Como se indica en la sección 4.2.1, letra c), los rasgos y características de la personalidad conforman una amplia categoría de características relativas a una persona física concreta, para la que no existe una taxonomía generalmente aceptada. En el considerando 42 del Reglamento de Inteligencia Artificial se ofrecen algunos ejemplos de rasgos y características de la personalidad que pueden evaluarse para predecir el riesgo de que una persona cometa un delito, como «la nacionalidad, el lugar de nacimiento, el lugar de residencia, el número de hijos, el nivel de endeudamiento o el tipo de vehículo». Se trata de una lista meramente ilustrativa y no exhaustiva.

*c) **«Únicamente»***

199) El artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial establece que las evaluaciones de riesgos contempladas en dicha disposición solo estarán prohibidas cuando se basen «únicamente» en la elaboración del perfil de una persona o en la evaluación de los rasgos y características de su personalidad. Del considerando 42 del Reglamento de Inteligencia Artificial se desprende claramente que el término «únicamente» se aplica tanto a la elaboración de perfiles como a la evaluación de los rasgos y características de la personalidad.

200) La condición de que la evaluación de riesgos debe basarse «únicamente» en la elaboración de perfiles o en la evaluación de los rasgos y características de la personalidad puede no cumplirse en determinadas situaciones.

---

137 Sobre la elaboración de perfiles de grupo, véase, por ejemplo, Agencia de los Derechos Fundamentales, *Guía para prevenir la elaboración ilícita de perfiles en la actualidad y en el futuro*, Manual, 2018, p. 21.

201) Como se desprende de la última frase del artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, tal situación se plantea, en cualquier caso, cuando el sistema de IA se utiliza para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se basa en hechos objetivos y verificables directamente relacionados con una actividad delictiva. Tal como se precisa en el considerando 42, en este contexto conviene pensar, en particular, pero no necesariamente de manera exclusiva, en una situación en la que ya existan motivos razonables para sospechar de la persona física de que se trate. Al fin y al cabo, en tales casos, normalmente se habrá llevado a cabo una valoración humana, basada en principio en hechos objetivos, verificables y pertinentes.

202) No obstante, también pueden darse otras situaciones, que siempre deberán evaluarse caso por caso. Por una parte, el uso del término «únicamente» deja abierta la posibilidad de que se tengan en cuenta otros elementos en la evaluación de riesgos, lo que hace que ya no se base solamente en la elaboración de perfiles o en la evaluación de rasgos o características de la personalidad. Por otra parte, para evitar que se eluda la prohibición y garantizar su eficacia, cualquier otro elemento de este tipo deberá ser real, sustancial y significativo para que pueda justificar la conclusión de que la prohibición no es aplicable. La lectura de la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial y la de la exclusión que figura en su última frase sugiere que, en particular, la existencia de determinados hechos objetivos y verificables previamente establecidos puede justificar esta conclusión.

A continuación, varios ejemplos:

- Una autoridad garante del cumplimiento del Derecho utiliza, para predecir comportamientos delictivos relacionados con delitos como el terrorismo, un sistema de IA que se basa únicamente en la edad, la nacionalidad, la dirección, el tipo de vehículo y el estado civil de las personas. Con este sistema, se considera que las personas tienen más probabilidades de cometer en el futuro delitos que no han cometido todavía, únicamente sobre la base de sus características personales. Puede suponerse que un sistema de este tipo está prohibido por el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial.

- Las autoridades tributarias nacionales utilizan una herramienta predictiva de IA para revisar todas las declaraciones tributarias de los contribuyentes a fin de predecir posibles delitos fiscales y detectar los casos que requieran una investigación más exhaustiva. Esto se hace únicamente sobre la base del perfil creado por el sistema de IA, que utiliza para su evaluación rasgos de la personalidad como la doble nacionalidad, el lugar de nacimiento o el número de hijos; también usa variables opacas, en particular la información inferida que es predictiva y, por tanto, no objetiva y difícil de verificar. Normalmente, un sistema de este tipo está sujeto a la prohibición del artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, ya que no existe una sospecha razonable de que una persona determinada está implicada en una actividad delictiva ni ningún otro hecho objetivo y verificable que la vincule a esa actividad delictiva. Este ejemplo también entra en el ámbito de aplicación de la

puntuación ciudadana prohibida en virtud del artículo 5, apartado 1, letra c), del Reglamento de Inteligencia Artificial, que implica un trato desfavorable sobre la base de datos procedentes de contextos sociales que no guardan relación.

- Un departamento de policía utiliza una herramienta de evaluación de riesgos basada en la IA para evaluar el riesgo de que niños pequeños y adolescentes estén implicados en «futuros delitos violentos y contra la propiedad». El sistema evalúa a los menores sobre la base de sus relaciones con otras personas y sus supuestos niveles de riesgo, es decir, se puede considerar que los menores presentan un mayor riesgo de cometer un delito simplemente por estar vinculados a otra persona con una evaluación de alto riesgo, como un hermano o un amigo. Los niveles de riesgo de los padres también pueden afectar al nivel de riesgo de un menor. Tras estas evaluaciones de riesgos, la policía «registra» a estos menores en sus sistemas, los vigilan por medio inspecciones adicionales y los deriva a servicios de «atención» a la juventud. También es probable que un sistema de este tipo entre en el ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial.

5.2.3. Exclusión de los sistemas de IA utilizados para apoyar la valoración humana que se basa en hechos objetivos y verificables directamente relacionados con una actividad delictiva

203) A tenor de la última frase del artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, la prohibición no se aplica a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona en una actividad delictiva que ya se basa en hechos objetivos y verificables directamente relacionados con una actividad delictiva. Aunque, como se ha señalado, la situación descrita en esta exclusión expresa no es necesariamente la única en la que no se aplica la prohibición, mencionarla explícitamente en esta disposición aporta seguridad jurídica al delimitar el ámbito de aplicación de la prohibición y dejar claro que, en cualquier caso, la prohibición no se aplica en este supuesto.

204) Cuando el sistema entra en el ámbito de aplicación de la exclusión y, por tanto, no está prohibido, se clasifica como un sistema de IA de alto riesgo [tal como se contempla en el anexo III, punto 6, letra d), del Reglamento de Inteligencia Artificial] si está destinado a ser utilizado por las autoridades garantes del cumplimiento del Derecho o en su nombre y, por tanto, está sujeto a los requisitos y garantías, incluida la supervisión humana (artículo 14 y artículo 26 del Reglamento de Inteligencia Artificial). Entre otras cosas, estos requisitos establecen que la supervisión humana debe confiarse a personas con las competencias, la formación y la autoridad necesarias, que deben ser capaces de comprender adecuadamente las capacidades y limitaciones del sistema de IA, interpretar correctamente sus resultados de salida y hacer frente al riesgo de sesgo de automatización. Para evaluar adecuadamente la información de salida del sistema de IA, estas personas deben contar con procedimientos claros y formación, así como con las competencias y la autoridad necesarias. En este caso concreto, su valoración humana debe garantizar que toda predicción o evaluación por parte de la IA del riesgo de que

una persona cometa un delito se basa en hechos objetivos y verificables vinculados a una actividad delictiva. Estas personas también deben intervenir a fin de evitar consecuencias negativas o riesgos, así como para detener el uso del sistema de IA si no funciona según lo previsto.

205) Además, el concepto de «intervención humana» ha sido objeto de la jurisprudencia del TJUE, en particular en el contexto de la toma de decisiones exclusivamente automatizada que predice el riesgo de que los pasajeros aéreos estén implicados en delitos graves. Esta jurisprudencia también puede ser pertinente para la aplicación del concepto de «valoración humana» empleado en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial.

En el asunto Ligue des droits humains[138], el TJUE examinó la legalidad del uso de un sistema avanzado de IA para el tratamiento sistemático de los datos del registro de nombres de los pasajeros (PNR) de los viajeros aéreos a fin de evaluar la probabilidad de que estén implicados en actividades terroristas y otros delitos graves.

El TJUE interpretó la norma de la Directiva (UE) 2016/681 («Directiva PNR»), que prohíbe las decisiones jurídicas perjudiciales basadas únicamente en el tratamiento automatizado y exige una **valoración humana** y una revisión **individuales** de cualquier coincidencia positiva por medios no automatizados para detectar falsos positivos y garantizar resultados no discriminatorios.

Según el TJUE, esta valoración humana**,** en la que debe basarse todo resultado del tratamiento automatizado de datos PNR, debe estar basada en criterios objetivos que permitan evaluar si una coincidencia positiva afecta a una persona que pueda estar implicada, en este caso concreto, en delitos terroristas o delitos graves, y garantizar el carácter no discriminatorio del tratamiento automatizado.

206) En cuanto al contenido de la exclusión, uno de sus elementos centrales es que el sistema de IA se debe utilizar para apoyar la valoración humana, no para llevar a cabo la evaluación de riesgos, como sucede en las situaciones que contempla la prohibición. No obstante, para que se aplique la exclusión, dicha valoración humana debe, además, estar ya basada en hechos objetivos y verificables directamente relacionados con una actividad delictiva

5.2.4. Medida en que las actividades de los agentes privados pueden entrar en el ámbito de aplicación

207) Además de las autoridades garantes del cumplimiento del Derecho, que en principio son las principales responsables del despliegue de sistemas de IA de predicción de delitos, las actividades de las entidades privadas también pueden, en algunos casos, estar contempladas en la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial. Ello resulta del hecho de que, atendiendo a su tenor literal, la prohibición no se aplica exclusivamente a las autoridades garantes

[138] Sentencia del Tribunal de Justicia de 21 de junio de 2022, Ligue des droits humains, C-817/19, ECLI:EU:C:2022:491.

del cumplimiento del Derecho. Además, de lo contrario, la prohibición podría eludirse fácilmente, lo que cuestionaría su eficacia.

208) En estas circunstancias, cabe presumir que la prohibición se aplica, en particular, cuando el Derecho confía a agentes privados el ejercicio de la autoridad pública y las competencias públicas para la prevención, investigación, detección o enjuiciamiento de delitos o ejecución de sanciones penales[139]. También se puede solicitar explícitamente a los agentes privados, caso por caso, que actúen en nombre de las autoridades garantes del cumplimiento del Derecho y realicen predicciones del riesgo de que una persona cometa un delito. En tales casos, las actividades de dichos agentes privados también podrían entrar en el ámbito de aplicación de la prohibición, si se cumplen las condiciones aplicables y la exclusión no se aplica.

> Por ejemplo, una autoridad garante del cumplimiento del Derecho puede pedir a una empresa privada que ofrece programas informáticos avanzados de análisis de la delincuencia basados en la IA que analice una gran cantidad de datos procedentes de múltiples fuentes y bases de datos (registros nacionales, operaciones bancarias, datos de comunicaciones, datos geoespaciales, etc.) para predecir o valorar el riesgo de que las personas puedan cometer delitos relacionados con la trata de seres humanos. Si se cumplen todos los criterios del artículo 5, apartado 1, letra d), ese escenario de uso podría prohibirse.

209) Además, la prohibición puede aplicarse a las entidades privadas que valoran o predicen el riesgo de que una persona cometa un delito cuando sea objetivamente necesario para el cumplimiento de una obligación legal a la que esté sujeto dicho operador privado de valorar o predecir el riesgo de que las personas cometan delitos específicos, como, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o la financiación del terrorismo.

> Por ejemplo, un banco tiene la obligación, en virtud de la legislación de la Unión en materia de lucha contra el blanqueo de capitales[140], de examinar a los clientes y de elaborar sus perfiles en relación con delitos de blanqueo de capitales. Si el banco utiliza un sistema de IA para cumplir sus obligaciones, debe hacerlo basándose únicamente en los datos especificados en dicha legislación, que sean objetivos y verificables, a fin de garantizar que existe una posibilidad razonable de que las personas identificadas como sospechosas comentan delitos de blanqueo de capitales. De conformidad con esta legislación[141], las predicciones también deben someterse a una evaluación y comprobación humanas para garantizar la precisión y la idoneidad de dichas valoraciones. El cumplimiento de esta legislación garantiza que el uso de sistemas de IA de predicción individual de delitos con fines de lucha contra el blanqueo de capitales queda fuera del ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial.

---

139 Véase la definición de «autoridades garantes del cumplimiento del Derecho» en el artículo 3, punto 45, del Reglamento de Inteligencia Artificial.

140 Reglamento (UE) 2024/1624, de 31 de mayo de 2024, relativo a la lucha contra el blanqueo de capitales.

141 Artículo 20 del Reglamento (UE) 2024/1624.

210) Sin embargo, teniendo en cuenta la atención prestada a las evaluaciones de riesgos relativas específica y exclusivamente a la comisión de delitos, que se desprende claramente de la redacción de la prohibición y de su finalidad, tal como se explica en el considerando 42, si una entidad privada elabora perfiles de sus clientes para sus operaciones comerciales regulares y su seguridad o para proteger sus intereses financieros (por ejemplo, detectar irregularidades financieras) sin el propósito de valorar o predecir el riesgo de que el cliente cometa un delito específico, no debe considerarse que las actividades de las entidades privadas entran en el ámbito de aplicación de la prohibición del artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial.

211) En otras palabras, si la legislación no ha encomendado a entidades privadas que realicen determinadas tareas específicas de garantía del cumplimiento del Derecho en las que actúen en nombre de las autoridades garantes del cumplimiento del Derecho o estén sujetas a obligaciones jurídicas específicas como las descritas anteriormente, no se considera que entre en el ámbito de aplicación de la prohibición el uso de sistemas de IA para llevar a cabo evaluaciones de riesgos en el curso de sus operaciones comerciales normales y con el fin de proteger sus propios intereses privados, aunque dichas evaluaciones de riesgos puedan referirse al riesgo de que se cometan delitos como una circunstancia meramente accidental y secundaria.

5.3. Fuera del ámbito de aplicación

5.3.1. Predicciones de delitos basadas en la ubicación, los datos geoespaciales o el lugar

212) Las predicciones de delitos basadas en la ubicación, los datos geoespaciales o el lugar se centran en el lugar o la ubicación del delito o en la probabilidad de que se cometa un delito en esas zonas. En principio, este tipo de actividad policial no implica una evaluación de una persona concreta. Por lo tanto, quedan fuera del ámbito de aplicación de la prohibición.

Ejemplos de predicciones de delitos basadas en la ubicación, los datos geoespaciales o el lugar

- Un sistema de policía predictiva basado en la IA asigna una puntuación que mide la probabilidad de que se cometan delitos en diferentes zonas de una ciudad basándose en las tasas de delincuencia previas en cada zona y en otra información, como mapas callejeros, para destacar el elevado riesgo de que se produzcan determinados tipos de delitos (por ejemplo, robos con fuerza, agresiones con arma blanca, etc.) y ayudar a las autoridades garantes del cumplimiento del Derecho a determinar dónde enviar menos más o menos patrullas o dónde aumentar o reducir la presencia policial para llevar a cabo actividades policiales de proximidad que frenen o disuadan las actividades delictivas.

- Una autoridad aduanera utiliza herramientas de análisis de riesgos basadas en la IA para predecir la probabilidad de la localización de estupefacientes o mercancías ilícitas, basándose, por ejemplo, en las rutas de tráfico conocidas.

- Un departamento de policía utiliza sistemas basados en la IA para detectar y localizar disparos en tiempo real. El sistema utiliza sensores acústicos situados en zonas urbanas para identificar los sonidos de disparos y triangular su posición; esto aporta a los agentes datos utilizables que pueden resultar de utilidad para detectar e investigar los delitos.

213) Sin embargo, la distinción entre los sistemas de predicción de delitos basados en la ubicación y los sistemas de predicción individuales que evalúan el riesgo de que una persona cometa un delito no siempre resultan evidentes. En la medida en que un sistema de IA lleve a cabo una actividad de policía predictiva basada en la ubicación y tenga en cuenta la puntuación del riesgo de la ubicación como un aspecto de la elaboración de perfiles de una persona, debe considerarse que dicho sistema está basado en personas y que, en principio, está cubierto por el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, aunque pueda quedar fuera del ámbito de aplicación de la prohibición por otros motivos.

Por ejemplo, si la información geoespacial o la información basada en la ubicación o el lugar está vinculada a información relativa a una persona (como el lugar de residencia de una persona concreta) y el sistema de IA evalúa el riesgo de que esa persona pueda cometer un delito basándose únicamente en la elaboración de su perfil, incluido su lugar de residencia, en donde hay una elevada delincuencia, debe considerarse que ese sistema está basado en la persona.

5.3.2. Sistemas de IA que apoyan las valoraciones humanas basados en hechos objetivos y verificables directamente relacionados con una actividad delictiva

214) El artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial establece que la prohibición no se aplica a los sistemas de IA utilizados para apoyar la valoración humana de la implicación de una persona física en una actividad delictiva que ya se basa en hechos objetivos y verificables directamente relacionados con una actividad delictiva. En tal caso, las evaluaciones y predicciones del riesgo de que una persona cometa un delito tampoco se basarían <u>únicamente</u> en la elaboración de perfiles o en la evaluación de características personales y, por tanto, no estarían prohibidas.

Algunos ejemplos de sistemas de IA que quedan fuera del ámbito de aplicación de la prohibición por este motivo:

- Un sistema de IA se utiliza para la elaboración de perfiles y la categorización de un comportamiento real (como un comportamiento peligroso en una multitud que hace sospechar de forma razonable que alguien está preparando un delito y que es probable que lo cometa) y la clasificación de la IA está sujeta a una valoración humana pertinente. En este caso, la evaluación de riesgos realizada por el ser humano con el apoyo de la IA no se basa únicamente en los rasgos personales o la elaboración de perfiles, sino en hechos objetivos y verificables relacionados con la amenaza de comportamiento delictivo de esa persona, que ha sido revisado por un ser humano antes de que se tomen medidas.

- La policía investiga el riesgo de un posible robo a mano armada y sospecha de dos personas. Esta sospecha se basa en varios hechos verificables y objetivos, como la participación verificable en grupos de chat de la red oscura para la compra de armas. Un sistema de IA que combina información policial predictiva geoespacial o basada en el lugar con información del reconocimiento automático de matrículas de vehículos pertenecientes a los sospechosos apoya la valoración humana, en el marco de la investigación, basada en hechos verificables y objetivos directamente relacionados con una actividad delictiva específica.

- Un sistema de IA se utiliza para evaluar el riesgo de que un preso deba recibir el beneficio de la liberación anticipada. El perfil de IA de la persona afectada o la evaluación de los rasgos y características de su personalidad solo respaldan la valoración humana de hechos objetivos y verificables relacionados con delitos anteriores y comportamientos demostrados pertinentes para la rehabilitación.

- Un juez celebra una audiencia para valorar si se impone prisión provisional a una persona acusada de un delito grave para determinar si pueden aplicarse medidas no privativas de libertad. La decisión se basa en una evaluación de la existencia de motivos válidos para imponer la prisión provisional, como la probabilidad de que el sospechoso o acusado cometa otro delito si no es detenido o de que se fugue u obstaculice el correcto desarrollo de la investigación. Para ayudar en este proceso, el juez utiliza una herramienta de evaluación de riesgos basada en la IA, entrenada con datos que incluyen, en particular, los antecedentes penales de personas en asuntos similares y otros factores como el grupo de edad, el comportamiento social, los ingresos y la situación laboral.

- Un sistema de IA se utiliza para apoyar la evaluación de un agente humano sobre el riesgo de que una persona que cumple una pena no privativa de libertad infrinja las condiciones de la libertad o se fugue, sobre la base de comportamientos delictivos pasados y hechos objetivos que generan sospechas, como el cumplimiento de las condiciones de la libertad, los resultados de la evaluación psicológica y las recomendaciones de otros servicios comunitarios a los que puede recurrir la persona. Sobre la base de esta información, el agente decide si mantiene el *statu quo* o revisa las condiciones de la libertad.

- Las autoridades aduaneras utilizan sistemas de IA para evaluar el riesgo de que las mercancías que entran en la UE no cumplan la legislación aplicable en la frontera (por ejemplo, incumplimiento de la prohibición de importar drogas ilícitas, infracción de sanciones a la exportación u otras actividades ilegales) para determinar las situaciones en las que debe llevarse a cabo un control aduanero. El sistema de IA evalúa la información objetiva y verificable facilitada a las autoridades aduaneras en relación con las mercancías y sus cadenas de suministro (por ejemplo, la naturaleza y el valor de las mercancías, el número de contenedor, los medios de transporte para ocultar otras mercancías o los conocimientos previos sobre la conformidad de las mercancías de la descripción y el origen en cuestión con los requisitos aplicables a su importación a la Unión o su exportación desde la Unión). En determinados casos, también puede

tratar información sobre la implicación previa del importador o exportador en irregularidades relacionadas con la importación de mercancías, su pertenencia a organizaciones delictivas o la existencia de antecedentes penales por tráfico de drogas. Estos sistemas quedan fuera del ámbito de aplicación de la prohibición porque cualquier predicción de la probabilidad de que una persona física participe en la importación o exportación de mercancías ilícitas no se basa únicamente en la elaboración de perfiles, sino en información objetiva y verificable sobre las mercancías y la participación previa del importador o exportador en actividades delictivas, y está sujeta a una revisión humana para determinar si la situación requiere un control aduanero o una medida de reducción del riesgo.

5.3.3. Sistemas de IA utilizados para predicciones y evaluaciones de delitos en relación con entidades jurídicas

215) La prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial se aplica únicamente a las predicciones y las evaluaciones de riesgos individuales de personas físicas, por lo que normalmente quedan excluidos los sistemas de predicción de delitos que elaboran perfiles de entidades jurídicas como empresas u organizaciones no gubernamentales.

A continuación, varios ejemplos:

- Una autoridad tributaria o aduanera utiliza un sistema de IA para analizar grandes cantidades de datos relativos a transacciones y declaraciones fiscales y datos aduaneros de empresas para evaluar el riesgo de que cometan un fraude fiscal o aduanero que constituya un delito.
- Los sistemas de IA se utilizan para ayudar a las autoridades aduaneras a identificar las situaciones en las que se debe dar a las entidades jurídicas la instrucción de no enviar mercancías ilícitas a la UE.

216) Al mismo tiempo, puede haber casos límite en los que una persona física actúe a través de una entidad jurídica como «empresario individual» o como profesional independiente (por ejemplo, un abogado). En tales circunstancias, la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial puede aplicarse siempre que se cumplan todas las condiciones, ya que el sistema de IA elabora perfiles de una persona física concreta y valora o predice el riesgo de que cometa un delito, aunque sea con fines relacionados con la actividad comercial de dicha persona física.

5.3.4. Sistemas de IA utilizados para predicciones individuales de infracciones administrativas

217) La prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial solo se aplica a la predicción de delitos, lo que excluye de su ámbito de aplicación las infracciones administrativas, cuyo procedimiento sancionador es, en principio, menos intrusivo para los derechos y libertades fundamentales de las personas.

Por ejemplo, una autoridad pública que utiliza la IA en el contexto de una investigación administrativa para evaluar el riesgo de que posibles autores de una infracción cometan infracciones leves (como infracciones de tráfico menores) o irregularidades en el marco de procesos fiscales, de contratación pública o de gastos no entraría en el ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, incluso en los casos en que pudiera recogerse información relativa a la posible implicación de personas físicas en delitos como resultado de las investigaciones y controles administrativos.

218) El carácter administrativo o penal de una infracción puede depender del Derecho de la Unión o nacional. La calificación nacional de las infracciones que no están directamente reguladas por el Derecho de la Unión está sujeta al control del TJUE, ya que el concepto de «delito» tiene un significado autónomo en el Derecho de la Unión y debe interpretarse de manera coherente en todos los Estados miembros. El TJUE ha llegado a la conclusión, en un contexto diferente, de que la calificación de las infracciones por parte de los Estados miembros no es determinante a este respecto[142]. Los criterios pertinentes utilizados para evaluar la naturaleza de la infracción (sea un delito o no) pueden encontrarse en la jurisprudencia pertinente del TJUE y del Tribunal Europeo de Derechos Humanos (TEDH).[143]

5.4. Relación con otros actos jurídicos de la Unión

219) La relación de la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial con la Directiva sobre protección de datos en el ámbito penal y el RGPD es pertinente al evaluar la legalidad del tratamiento de datos personales en virtud de la legislación de la Unión en materia de protección de datos, como el RGPD y la Directiva sobre protección de datos en el ámbito penal. En particular, el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial impone a las autoridades garantes del cumplimiento del Derecho, a otras autoridades públicas y a entidades privadas incluidas en el ámbito de aplicación de la prohibición una prohibición específica de valorar o predecir el riesgo de que una persona física cometa un delito basándose únicamente en la elaboración del perfil de una persona física o en la evaluación de los rasgos y características de su personalidad. Por lo que se refiere a la Directiva sobre protección de datos en el ámbito penal, el artículo 5,

142 Véase, por ejemplo, la sentencia del Tribunal de Justicia (Gran Sala) de 14 de noviembre de 2013. Procedimiento relativo a la ejecución de una sanción pecuniaria impuesta a Marián Baláž, asunto C-60/12, ECLI:EU:C:2013:733.

143 Según la jurisprudencia del TJUE, corresponde a los órganos jurisdiccionales nacionales determinar si una sanción no penal puede considerarse «penal» a la luz de los denominados «criterios Engel». Véase: Sentencia del Tribunal Europeo de Derechos Humanos de 8 de junio de 1976, Engel y otros / Países Bajos, solicitud n.º 5100/71, 5101/71, 5102/71, 5354/72 y 5370/72, CE:ECHR:1976:0608JUD000510071, apartado 82. Estos criterios, elaborados originalmente por el Tribunal Europeo de Derechos Humanos (TEDH) y refrendados posteriormente por el TJUE, son alternativos y no acumulativos. Al examinar si una sanción tiene carácter penal, el órgano jurisdiccional nacional competente debe evaluar: (1) la calificación de las disposiciones pertinentes en Derecho interno; (2) la naturaleza intrínseca de la infracción; y (3) la gravedad de la sanción. Al evaluar la naturaleza de la infracción, se tendrá en cuenta, entre otras cosas, si el procedimiento ha sido incoado por un organismo público con facultades coercitivas legales, si la norma jurídica tiene una finalidad punitiva o disuasoria, si la norma jurídica tiene por objeto proteger los intereses generales de la sociedad normalmente protegidos por el Derecho penal o si la imposición de una sanción depende de la declaración de culpabilidad. Por lo que se refiere a la gravedad de la sanción, debe tomarse como referencia la pena máxima contemplada en el Derecho nacional. Estos criterios son alternativos y no necesariamente acumulativos. Véase Tribunal Europeo de Derechos Humanos, *Guía del artículo 6 del Convenio Europeo de Derechos Humanos, Derecho a un proceso equitativo (parte penal)*, actualizada el 29 de febrero de 2024. Véase también la sentencia del TJUE de 5 de junio de 2012, Bonda, C-489/10, ECLI:EU:C:2012:319, apartado 37 y ss.; y la sentencia del TJUE de 26 de febrero de 2013, Åkerberg Fransson, C-617/10, ECLI:EU:C:2013:105, apartado 35.

apartado 1, letra d), del Reglamento de Inteligencia Artificial se entiende sin perjuicio del artículo 11, apartado 3, de dicha Directiva, que prohíbe la elaboración de perfiles que dé lugar a una discriminación (directa o indirecta).

220) La relación de la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial con la Directiva (UE) 2016/343 sobre la presunción de inocencia también es pertinente, ya que ambos actos se refieren [directamente en el caso de la Directiva e indirectamente en el caso del Reglamento de Inteligencia Artificial (véase su considerando 42)] al derecho fundamental a la presunción de inocencia hasta que se pruebe su culpabilidad conforme la ley[144]. Si bien la Directiva se aplica desde el momento en que una persona es sospechosa de haber cometido un delito o se le ha acusado de ello[145], el Reglamento de Inteligencia Artificial tiene un ámbito de aplicación más amplio y se aplica ya en la fase de predicción y prevención de la delincuencia, antes de que se abra una investigación penal formal contra una persona determinada, e incluso en los casos en que dichas predicciones y evaluaciones de riesgos sean realizadas por agentes privados que entren en el ámbito de aplicación del artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial y no por las autoridades garantes del cumplimiento del Derecho competentes, incluidas las autoridades judiciales.

221) Incluso en los casos en que no se aplique la prohibición establecida en el artículo 5, apartado 1, letra d), del Reglamento de Inteligencia Artificial, es importante destacar que el Derecho de la Unión y nacional aplicable sigue aplicándose de forma plena, en particular la legislación en materia de protección de datos, el Derecho procesal penal, las leyes de policía y las garantías que pueden restringir aún más el uso de sistemas de IA de predicción individual de delitos o imponer condiciones adicionales a dicho uso.

6. ARTÍCULO 5, APARTADO 1, LETRA E), DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: EXTRACCIÓN NO SELECTIVA DE IMÁGENES FACIALES

222) El artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial prohíbe la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión.

6.1. Justificación y objetivos

223) La extracción no selectiva de imágenes faciales de internet y de circuitos cerrados de televisión interfiere gravemente con los derechos de las personas a la intimidad y a la protección de datos y les priva del derecho a permanecer en el anonimato. Por lo tanto, el considerando 43 del Reglamento de Inteligencia Artificial justifica la prohibición establecida en su artículo 5, apartado 1, letra e), sobre la base del «sentimiento de

144 La presunción de inocencia es un derecho fundamental consagrado en el artículo 48 de la Carta de los Derechos Fundamentales de la UE.

145 Como especificó el TJUE, no es necesario que las autoridades competentes informen a esta persona de su condición de sospechoso o acusado para que se aplique la Directiva.

vigilancia masiva» y los riesgos de «graves violaciones de los derechos fundamentales, incluido el derecho a la intimidad».

6.2. Conceptos fundamentales y componentes de la prohibición

> ***Según el artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial:***
>
> Quedan prohibidas las siguientes prácticas de IA:
>
> e) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA que creen o amplíen bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión;

224) Deben cumplirse varias condiciones acumulativas para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial:

(i) La práctica debe suponer la «introducción en el mercado», la «puesta en servicio para ese fin concreto» o el «uso» de un sistema de IA;

(ii) con el fin de crear o ampliar bases de datos de reconocimiento facial;

(iii) la base de datos se alimenta mediante el uso de herramientas de IA para la extracción no selectiva; y

(iv) las imágenes proceden de internet o de circuitos cerrados de televisión.

225) Para que se aplique la prohibición, deben cumplirse simultáneamente las cuatro condiciones. Ya se ha examinado el primer elemento de la introducción en el mercado, la puesta en servicio o el uso del sistema de IA en la sección 2.3. Así pues, la prohibición se aplica tanto a los proveedores como a los responsables del despliegue de sistemas de IA, cada uno dentro de sus respectivas responsabilidades de no introducir en el mercado, poner en servicio o utilizar dichos sistemas de IA. A continuación se describen y analizan con más detalle los criterios específicos relativos a la prohibición de la extracción no selectiva. La prohibición se aplica a las herramientas de extracción que se introducen en el mercado o se ponen en servicio «para este fin específico» de extracción no selectiva de imágenes faciales de internet o de circuitos cerrados de televisión. Esto significa que la prohibición no se aplica a las herramientas de extracción con las que se puede crear o ampliar una base de datos de reconocimiento facial, sino únicamente a las herramientas de extracción no selectiva.

6.2.1. Bases de datos de reconocimiento facial

226) La prohibición establecida en el artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial comprende los sistemas de IA utilizados para crear o ampliar bases de datos de reconocimiento facial. En este contexto, debe entenderse por «base de datos» cualquier conjunto de datos o información que esté especialmente organizado para la búsqueda y recuperación rápidas por un ordenador. Una base de datos de reconocimiento facial es capaz de cotejar un rostro humano de una imagen digital o una imagen de vídeo con una base de datos de caras, comparar dicha imagen con las de la

base de datos y determinar si existe una coincidencia probable entre ambas. Dicha base de datos de reconocimiento facial puede ser temporal, centralizada o descentralizada. El artículo 5, apartado 1, letra e), no exige que la base de datos se utilice únicamente para el reconocimiento facial; basta con que la base de datos pueda utilizarse para el reconocimiento facial.

6.2.2. Mediante la extracción no selectiva de imágenes faciales

227) La «extracción» se refiere generalmente al uso de rastreadores web, bots u otros medios para extraer automáticamente datos o contenidos de diferentes fuentes, incluidos circuitos cerrados de televisión, sitios web o redes sociales. Estas herramientas son programas informáticos programados para analizar bases de datos, extraer información y utilizarla para otros fines.

228) «No selectiva» se refiere a una técnica que funciona como una «aspiradora» que absorbe la mayor cantidad posible de datos e información, sin centrarse específica e individualmente en la persona o las personas que son objeto de la extracción. En la extracción se recogen indistintamente datos o contenidos. Así pues, el concepto de «no selectiva» significa que la extracción no se centra específicamente en una persona determinada o en un colectivo de personas determinado. El respeto de la exclusión voluntaria de protocolos de internet como robot.txt no afecta al carácter no selectivo de la extracción.

229) Si una herramienta de extracción tiene instrucciones de recoger imágenes o vídeos que contengan únicamente los rostros humanos de determinadas personas o de un colectivo predefinido de personas, la extracción para, por ejemplo, encontrar a un delincuente concreto o para identificar a un grupo de víctimas, se consideraría selectiva. Este tipo de extracción no está contemplada en la prohibición establecida en el artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial.

230) Por ejemplo, la recogida selectiva de imágenes centrada en una categoría de víctimas, en donde se usan rastreadores para recoger imágenes de víctimas que los tratantes de personas publican o anuncian en los canales de las redes sociales no está contemplada en la prohibición. La extracción no selectiva debe interpretarse de manera que no permita eludir la prohibición. La extracción de imágenes de internet o de circuitos cerrados de televisión para crear una base de datos paso a paso, seleccionando cada vez colectivos específicos de personas u otros criterios, debe entrar en el ámbito de aplicación de la prohibición del artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial si el resultado final es funcionalmente el mismo que si se pretendiera realizar desde el principio una extracción no selectiva.

231) La extracción no selectiva está prohibida cuando los sistemas combinan búsquedas selectivas de imágenes o vídeos con búsquedas no selectivas.

6.2.3. De internet y circuitos cerrados de televisión

232) Para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial, las imágenes faciales pueden proceder de internet o de circuitos cerrados de televisión. Por lo que respecta a internet, el hecho de que una

persona haya publicado imágenes de su rostro en una plataforma de redes sociales no significa que haya dado su consentimiento para que dichas imágenes se incluyan en una base de datos de reconocimiento facial. Algunos ejemplos de la extracción de imágenes faciales procedentes de circuitos cerrados de televisión son las imágenes obtenidas por cámaras de vigilancia utilizadas en lugares como aeropuertos, calles, parques, etc.

Ejemplo:

Una empresa de programas informáticos de reconocimiento facial recoge imágenes de caras. Las fotografías que posee la empresa se han extraído de las redes sociales (por ejemplo, Facebook, YouTube, Twitter, Venmo) mediante un «extractor automatizado de imágenes» que realiza búsquedas en internet y localiza las imágenes en las que aparecen rostros humanos. Recoge dichas imágenes y toda la información asociada, como la fuente de la imagen (URL), la geolocalización y, a veces, los nombres de las personas. A continuación, se extraen los rasgos faciales de las imágenes y se transforman en representaciones matemáticas, que se codifican mediante *hash* para su indexación y comparaciones futuras. Cuando un usuario carga la imagen de una persona en el sistema de IA, este determinará si esa imagen coincide con una de las caras de la base de datos. La imagen cargada experimentará la misma transformación matemática que las imágenes extraídas.

233) Si un sistema de IA recibe la imagen de una persona y busca correspondencias faciales en internet, es decir, actúa como un «motor de búsqueda de imágenes inverso», esto se considerará extracción selectiva. Además, cabe preguntarse si las correspondencias aparecerían en una «base de datos».

6.3. Fuera del ámbito de aplicación

234) La prohibición establecida en el artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial no se aplica a la extracción no selectiva de datos biométricos distintos de las imágenes faciales, como las muestras de voz. La prohibición tampoco se aplica cuando en la extracción no se utilizan sistemas de IA. También quedan fuera del ámbito de aplicación las bases de datos de imágenes faciales que no se utilizan para el reconocimiento de personas, como las que se utilizan para entrenar o probar un modelo de IA, cuando no se identifica a las personas.

235) La prohibición establecida en el artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial no se aplica a los sistemas de IA que recogen grandes cantidades de imágenes faciales de internet para desarrollar modelos de IA que generen nuevas imágenes de personas ficticias, ya que dichos sistemas no darían lugar al reconocimiento de personas reales. Estos sistemas de IA podrían entrar en el ámbito de aplicación de los requisitos de transparencia del artículo 50 del Reglamento de Inteligencia Artificial.

236) La prohibición establecida en el artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial comprende los sistemas de IA utilizados para crear o ampliar bases de datos de reconocimiento facial. Las bases de datos faciales existentes creadas antes del comienzo de la aplicación de la prohibición, que no se amplían mediante la

extracción no selectiva que posibilita la IA, así como el uso de estas bases de datos, deben cumplir las normas de la Unión aplicables en materia de protección de datos.

237) La prohibición establecida en el artículo 5, apartado 1, letra e), del Reglamento de Inteligencia Artificial se refiere a la creación o ampliación de bases de datos de reconocimiento facial. El acto concreto de identificación biométrica está sujeto a normas específicas en el Reglamento de Inteligencia Artificial y en otra legislación pertinente de la Unión.

6.4. Relación con otros actos jurídicos de la Unión

238) En relación con la legislación de la Unión en materia de protección de datos, la extracción no selectiva de material de internet o de circuitos cerrados de televisión para crear o ampliar bases de datos de reconocimiento facial, es decir, el tratamiento de datos personales (recogida de datos y uso de bases de datos) sería ilícito y no podría invocarse ninguna base jurídica en virtud del RGPD, el RPDUE y la Directiva sobre protección de datos en el ámbito penal.

7. ARTÍCULO 5, APARTADO 1, LETRA F), DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: RECONOCIMIENTO DE EMOCIONES

239) El artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial prohíbe que los sistemas de IA infieran las emociones de una persona física en los lugares de trabajo y en los centros educativos, excepto cuando el uso del sistema esté destinado a fines médicos o de seguridad. Los sistemas de reconocimiento de emociones que no entran en el ámbito de aplicación de la prohibición se consideran de alto riesgo de conformidad con el anexo III, punto 1, letra c), del Reglamento de Inteligencia Artificial. El artículo 50, apartado 3, del Reglamento de Inteligencia Artificial establece determinados requisitos de transparencia para el uso de sistemas de reconocimiento de emociones.

7.1. Justificación y objetivos

240) La tecnología de reconocimiento de emociones evoluciona rápidamente e incluye diferentes tecnologías y operaciones de tratamiento para detectar, recoger, analizar y categorizar emociones de las personas, así como para reaccionar a ellas, interactuar con ellas y aprender de dichas emociones. Esta tecnología también se denomina «tecnología del afecto». El reconocimiento de emociones puede utilizarse en diversos sectores y ámbitos para una amplia gama de aplicaciones[146], como el análisis del comportamiento de los clientes[147] y la publicidad personalizada y el *neuromarketing*[148]; en el sector del entretenimiento, por ejemplo, puede servir para hacer recomendaciones personalizadas

[146] El uso de emociones con fines económicos también se denomina *emotionomics* [«emocionomía»].

[147] Véase, por ejemplo, Mangano, G., Ferrari, A., Rafale, C., Vezzetti, E. y Marcolin, F., «Willingness of sharing facial data for emotion recognition: a case study in the insurance market» [«Disposición a compartir datos faciales para el reconocimiento de emociones: un estudio de caso en el mercado de seguros», documento no disponible en español], *AI & Society*, 2023.

[148] Véase Lee, N., Broderick, A. J. y Chamberlain, M.L., «What is 'neuromarketing'?A discussion and agenda for future research»[«¿Qué es el *neuromarketing*? Una reflexión y propuestas para la investigación futura», documento no disponible en español], *International Journal of Psychophysiology*, vol. 63, n.º 2, 2007, pp. 199-204, en donde se define el *neuromarketing* como un campo de estudio consistente en la «aplicación de métodos neurocientíficos para analizar y entender el comportamiento humano en relación con los mercados y los intercambios de *marketing*» (p. 200).

o predecir las reacciones a las películas; en la medicina y la asistencia sanitaria, para detectar la depresión o el autismo o prevenir el suicidio; en la educación, para conocer el nivel de atención o de participación de los alumnos (alumnos y estudiantes de diferentes edades); en el ámbito laboral, como acompañamiento en el proceso de contratación o para supervisar las emociones o el desinterés de los empleados, pero también con fines de bienestar para «hacer que los trabajadores sean más felices»[149]; en el contexto de la garantía del cumplimiento del Derecho y la seguridad pública, puede emplearse en los detectores de mentiras o para detectar emociones en grandes acontecimientos; así como para muchos otros fines.

241) A menudo se cuestiona la eficacia o la precisión del reconocimiento de emociones[150]. En el considerando 44 del Reglamento de Inteligencia Artificial se explica que existe «una gran preocupación respecto a la base científica de los sistemas de IA que procuran detectar o deducir las emociones, especialmente porque la expresión de las emociones varía de forma considerable entre culturas y situaciones, e incluso en una misma persona. Algunas de las deficiencias principales de estos sistemas son la fiabilidad limitada, la falta de especificidad y la limitada posibilidad de generalizar». También se explica que el reconocimiento de emociones puede «tener resultados discriminatorios» e «invadir los derechos y las libertades de las personas afectadas», en particular los derechos a la intimidad, a la dignidad humana y a la libertad de pensamiento. Esto desempeña un importante papel en las relaciones asimétricas, especialmente en el contexto del lugar de trabajo y de las instituciones de educación y formación, en las que tanto los trabajadores como los estudiantes se encuentran en situaciones especialmente vulnerables. Al mismo tiempo, el reconocimiento de emociones en contextos de uso específicos, como la seguridad y la asistencia médica (por ejemplo, para el tratamiento sanitario y el diagnóstico), tiene beneficios.[151]

7.2. Conceptos fundamentales y componentes de la prohibición

Según el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial:

Quedan prohibidas las siguientes prácticas de IA:

f) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de IA para inferir las emociones de una persona física en los lugares de

149 Véase Ackerman, E. y Strickland, E., «Are you Ready for Workplace Brain Scanning? Extracting and using brain data will make workers happier and more productive, backers say» [«¿Está preparado para el escaneo cerebral en el puesto de trabajo? Los impulsores de esta tecnología afirman que la extracción y el uso de datos cerebrales aumentará la felicidad y productividad de los trabajadores», documento no disponible en español], *IEEE Spectrum*, 19 de noviembre de 2022, https://spectrum.ieee.org/neurotech-workplace-innereye-emotiv. Los autores explican que «los sensores detectan la actividad eléctrica en diferentes zonas del cerebro, y los patrones de esa actividad pueden correlacionarse en gran medida con distintos sentimientos o respuestas fisiológicas, como el estrés, la concentración o una reacción a estímulos externos».

150 Véase, por ejemplo, Stanley, J., *«Experts Say 'Emotion Recognition' lacks Scientific Foundation»* [«Según los expertos, el reconocimiento de emociones carece de base científica», documento no disponible en español], *ACLU*, 18 de julio de 2019, que remite a un estudio de Feldman Barrett, L., Adolphs, R., Marsella, S., Martínez, A. M. y Pollak, S. D., «Emotional Expressions Reconsidered:Challenges to Inferring Emotion From Human Facial Movements» [«Replanteamiento de las expresiones emocionales: desafíos para deducir emociones a partir de los movimientos faciales humanos», documento no disponible en español], *Psychological Science in the Public Interest*, 2019, pp.iii-90.

151 Véase, por ejemplo, El Kaliouby, R., Picard, R. y Baron-Cohen, S., «Affective Computing and Autism» [«Computación afectiva y autismo», documento no disponible en español], *Annals New York Academy of Sciences*, 2007, pp. 228-248

trabajo y en los centros educativos, excepto cuando el sistema de IA esté destinado a ser instalado o introducido en el mercado por motivos médicos o de seguridad.

242) Deben cumplirse varias condiciones acumulativas para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial:

(i) La práctica debe suponer la «introducción en el mercado», la «puesta en servicio para este fin específico» o el «uso» de un sistema de IA;

(ii) el sistema de IA debe deducir las emociones[152];

(iii) opera en los lugares de trabajo o en las instituciones de educación y formación; y

(iv) se excluyen de la prohibición los sistemas de IA con fines médicos o de seguridad.

243) Para que se aplique la prohibición, deben cumplirse simultáneamente las cuatro condiciones. Ya se ha examinado el primer elemento, a saber, la «introducción en el mercado», «puesta en servicio» o «uso» de un sistema de IA en la sección 2.3. Así pues, la prohibición se aplica tanto a los proveedores como a los responsables del despliegue de sistemas de IA, cada uno dentro de sus respectivas responsabilidades de no introducir en el mercado, poner en servicio o utilizar dichos sistemas de IA. A continuación se describen y analizan con más detalle otras condiciones relativas a la prohibición.

7.2.1. Sistemas de IA para deducir las emociones

a) Sistemas de IA para deducir las emociones frente a sistemas de reconocimiento de emociones

244) El artículo 3, punto 39, del Reglamento de Inteligencia Artificial define los «sistemas de reconocimiento de emociones» como sistemas de IA destinados a distinguir e inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos; La prohibición establecida en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial no se refiere a los «sistemas de reconocimiento de emociones», sino únicamente a los «sistemas de IA para inferir las emociones de una persona física». El considerando 44 aclara además que dicha prohibición comprende los sistemas de IA «para detectar o deducir las emociones».

245) Generalmente, la identificación suele ser un requisito previo de la deducción, de modo que debe entenderse que la prohibición incluye tanto los sistemas de IA que identifican emociones o intenciones como los que las deducen[153]. Por razones de coherencia, también es importante interpretar que la prohibición establecida en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial tiene un ámbito de aplicación similar al de las normas aplicables a otros sistemas de reconocimiento de emociones [anexo III, punto 1, letra c), y artículo 50 del Reglamento de Inteligencia Artificial] y limitar esta prohibición a las inferencias basadas en los datos biométricos de una persona. Por lo tanto, la definición que figura en el artículo 3, punto 39, del

[152] O la tecnología es capaz de deducir las emociones (es decir, al introducirla en el mercado).
[153] Véase también el considerando 18 del Reglamento de Inteligencia Artificial.

Reglamento de Inteligencia Artificial de los sistemas de reconocimiento de emociones debe considerarse pertinente en relación con su artículo 5, apartado 1, letra f).

b) Identificación e inferencia de emociones o intenciones

246) La «identificación» se produce cuando el tratamiento de los datos biométricos (por ejemplo, de la voz o de una expresión facial) de una persona física permite comparar e identificar directamente una emoción con otra que haya sido programada previamente en el sistema de reconocimiento de emociones. La «inferencia» se produce cuando el propio sistema deduce información generada por procesos analíticos y de otro tipo. En tal caso, la información sobre la emoción no se basa únicamente en datos recogidos sobre la persona física, sino que se deduce de otros datos, en particular de estrategias de aprendizaje automático que aprenden de los datos cómo detectar emociones[154].

c) Emociones

247) A efectos del artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial, el concepto de emociones o intenciones debe entenderse en un sentido amplio y no interpretarse de manera restrictiva. En el considerando 18 del Reglamento de Inteligencia Artificial se ofrece información detallada y se mencionan emociones «como la felicidad, la tristeza, la indignación, la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión». Estos ejemplos no son exhaustivos.

248) La prohibición no debe eludirse aludiendo a actitudes, e incluye los casos en los que el sistema de IA considera, sobre la base de los datos biométricos, que una persona está mostrando, por ejemplo, una actitud de enojo.

249) En el considerando 18 del Reglamento de Inteligencia Artificial se aclara que no forman parte de las emociones o intenciones «los estados físicos, como el dolor o el cansancio, como, por ejemplo, los sistemas utilizados para detectar el cansancio de los pilotos o conductores profesionales con el fin de evitar accidentes». Además, precisa que los sistemas de reconocimiento de emociones no incluyen «la mera detección de expresiones, gestos o movimientos que resulten obvios, salvo que se utilicen para distinguir o deducir emociones», lo que debe entenderse que también se aplica al artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial. Esas expresiones pueden ser expresiones faciales básicas, como un ceño fruncido o una sonrisa; gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como una voz alzada o un susurro. Sin embargo, el uso de estas expresiones o gestos que resultan obvios para identificar o inferir emociones o intenciones está incluido en la prohibición.

A continuación, varios ejemplos: - Constatar que una persona sonríe no es reconocimiento de emociones.

[154] Véase el considerando 12 del Reglamento de Inteligencia Artificial. Por lo tanto, los datos inferidos también suelen ser el resultado de procesos analíticos basados en la probabilidad (macrodatos), destinados a encontrar correlaciones y patrones en los conjuntos de datos.

- Detectar que una persona está enferma no es reconocimiento de emociones.

- Que un organismo de radiodifusión televisiva utilice un dispositivo que permite registrar el número de veces que sus presentadores de informativos sonríen a la cámara no es reconocimiento de emociones.

- Llegar a la conclusión de que una persona está feliz no es reconocimiento de emociones. Que un sistema de IA deduzca que un empleado está descontento, triste o enfadado con los clientes (por ejemplo, a partir de gestos corporales, un ceño fruncido o la ausencia de sonrisa) es «reconocimiento de emociones».

- Que los sistemas infieran a partir de la voz o de gestos corporales que un estudiante está furioso y a punto de mostrarse violento es «reconocimiento de emociones».

- Usar sistemas de reconocimiento de IA para inferir el cansancio de un piloto profesional o de un conductor para alertarles y sugerirles cuándo frenar para evitar accidentes no es «reconocimiento de emociones», ya que el reconocimiento de emociones no contempla estados físicos como el dolor o el cansancio.

d) En función de sus datos biométricos

250) Según la definición del artículo 3, punto 39, del Reglamento de Inteligencia Artificial, solo los sistemas de IA que distinguen o infieren las emociones o las intenciones a partir de los datos biométricos son sistemas de reconocimiento de emociones[155].

251) Las características personales de las que pueden extraerse datos biométricos son atributos físicos o del comportamiento. La biometría fisiológica emplea atributos físicos, estructurales y relativamente estáticos de una persona, como sus impresiones dactilares, el patrón de sus iris, los contornos de su rostro o la geometría de las venas de sus manos. Algunas modalidades son microscópicas, pero siguen presentando estructuras biológicas y químicas que pueden adquirirse e identificarse, como, por ejemplo, el ADN y el olor[156]. La biometría del comportamiento registra las características distintivas de los movimientos, los gestos y las capacidades motrices de las personas mientras realizan una tarea o una serie de tareas. Esto significa que se recogen y analizan los movimientos humanos, como caminar (análisis del modo de andar) o el contacto de los dedos sobre un teclado (pulsaciones de tecla). La biometría del comportamiento agrupa diversas modalidades que presentan movimientos repetidos, voluntarios e involuntarios y ritmos o presiones asociados a las características corporales, que van desde la firma, el modo de andar, la voz y las pulsaciones de tecla hasta el seguimiento ocular y los latidos del corazón[157], los electroencefalogramas

155 Artículo 3, punto 34, del Reglamento de Inteligencia Artificial: se definen los «datos biométricos» como «los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos» (véase también el considerando 18 del Reglamento de Inteligencia Artificial). Sobre las inferencias de emociones a partir de la voz y el habla.

156 Physiological and Behavioural Biometrics [«Biometría fisiológica y conductual», página no disponible en español] - Biometrics Institute

157 Physiological and Behavioural Biometrics [«Biometría fisiológica y conductual», página no disponible en español] - Biometrics Institute

(EEG)[158] o los electrocardiogramas (ECG)[159]. Los datos biométricos de entrada pueden ser de una modalidad, como imágenes faciales, o de múltiples modalidades, como, por ejemplo, información facial combinada con electroencefalogramas (EEG). En el considerando 18 se mencionan, a modo de ejemplo, las expresiones faciales, gestos como el movimiento de las manos o características de la voz de una persona.

A continuación, varios ejemplos:

- Un sistema de IA que infiere emociones de un texto escrito (análisis de contenido o sentimientos) para definir el estilo o el tono de un determinado artículo no se basa en datos biométricos y, por tanto, no entra en el ámbito de aplicación de la prohibición.
- Un sistema de IA que infiere emociones de las pulsaciones de tecla (forma de teclear), expresiones faciales, posturas corporales o movimientos se basa en datos biométricos y entra en el ámbito de aplicación de la prohibición.

252) Por lo tanto, la definición de datos biométricos del Reglamento de Inteligencia Artificial es amplia e incluye todo dato biométrico utilizado para el reconocimiento de emociones, la categorización biométrica u otros fines[160].

7.2.2. Limitación de la prohibición a los lugares de trabajo y a los centros educativos

253) La prohibición establecida en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial se limita a los sistemas de reconocimiento de emociones «en los lugares de trabajo y en los centros educativos». Como se aclara en el considerando 44 del Reglamento de Inteligencia Artificial, esta limitación tiene por objeto abordar el desequilibrio de poder en el contexto del trabajo o la educación.

a) «Lugares de trabajo»

254) El concepto de «lugares de trabajo» debe interpretarse en sentido amplio. Se refiere a cualquier espacio físico o virtual específico en el que las personas físicas llevan a cabo las tareas y responsabilidades asignadas por su empleador o por la organización a la que están afiliadas, por ejemplo en el caso del autoempleo. Esto incluye cualquier entorno en el que se realice el trabajo, y puede variar considerablemente en función de la naturaleza del mismo: desde espacios interiores como oficinas, fábricas y almacenes hasta espacios de acceso público, como tiendas, estadios o museos, así como lugares al

158 Véase Supervisor Europeo de Protección de Datos, TechDispatch 1/2024 – Neurodatos, 3.6.2024, en el que se debate el uso de datos cerebrales y la tecnología relacionada, así como las implicaciones jurídicas, en particular la propuesta de nuevos «neuroderechos», incluida la intimidad e integridad mentales. En O'Sullivan, S., Chneiweiss. H., Pierucci, A. y Rommelfanger, K. *«Neurotechnologies and Human Rights Framework: Do we need new Human Rights?»* [«Neurotecnologías y el marco de derechos humanos: ¿necesitamos nuevos derechos humanos?», documento no disponible en español], Informe de la OCDE y el Consejo de Europa, 9.11.2021, p.33, se analiza el estado actual de la técnica y los aspectos jurídicos de la neurotecnología.

159 Véase Hasnul, M.A.; Aziz, N.A.A.; Alelyani, S.; Mohana, M. y Aziz, A.A «Electrocardiogram-Based Emotion Recognition Systems and Their Applications in Healthcare» [«Sistemas de reconocimiento de emociones basados en electrocardiogramas y sus aplicaciones en la asistencia sanitaria», documento no disponible en español], *Sensors*, 2021.

160 En el Reglamento de Inteligencia Artificial, la definición de datos biométricos no incluye la expresión «que permitan o confirmen la identificación única» (el uso funcional de datos biométricos), contrariamente a la definición de datos biométricos del RGPD que incluye este requisito. La definición de datos biométricos del RGPD se aplica, en el marco de las normas de protección de datos, al tratamiento de datos personales [y cuando, por ejemplo, sea aplicable el artículo 9, apartados 1 y 2, del RGPD].

aire libre o vehículos, además de emplazamientos de trabajo temporales o móviles. Esto es independiente de la condición de empleado, contratista, becario, voluntario, etc.[161]. También debe entenderse que el concepto de «lugares de trabajo» del artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial se aplica a los candidatos durante el proceso de selección y contratación, como sucede con otras disposiciones de dicho Reglamento relativas a la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA en el ámbito del empleo, la gestión de los trabajadores y el acceso al autoempleo, ya que existe un desequilibrio de poder y el carácter intrusivo del reconocimiento de emociones puede ya aplicarse en la fase de contratación.

Por ejemplo:

- Está prohibido que un centro de llamadas utilice cámaras web y sistemas de reconocimiento de voz para controlar las emociones de su empleado, como el enfado[162]. Si solo se utilizan con fines de formación personal, los sistemas de reconocimiento de emociones están permitidos si los resultados no se comparten con las personas responsables de recursos humanos y no pueden afectar a la evaluación, la promoción, etc. de la persona formada, siempre que no se eluda la prohibición y que el uso del sistema de reconocimiento de emociones no tenga ningún impacto en la relación laboral.
- El uso de sistemas de reconocimiento vocal por parte de un centro de llamadas para hacer un seguimiento de las emociones de sus clientes, como el enojo o la impaciencia, para, por ejemplo, ayudar a los empleados a lidiar con determinados clientes enfadados, no está prohibido por el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial.
- Los sistemas de IA que controlan el tono emocional en los equipos de trabajo híbridos mediante la identificación e inferencia de las emociones a partir de la voz y las imágenes durante las videollamadas híbridas, que normalmente servirían para favorecer la concienciación social, la gestión de las dinámicas emocionales y la prevención de conflictos, están prohibidos.
- El uso de sistemas de IA de reconocimiento de emociones durante el proceso de contratación está prohibido.
- El uso de sistemas de IA de reconocimiento de emociones durante el período de prueba está prohibido.
- Que un supermercado utilice cámaras para hacer un seguimiento de las emociones de sus empleados, como la felicidad, está prohibido.

[161] Véanse también los considerandos en relación con los sistemas de IA de alto riesgo en el lugar de trabajo, como el considerando 56, que realiza una interpretación amplia. Véase también la lista de sistemas de IA de alto riesgo que figura en el anexo III, en donde se hace referencia, en el apartado 4, al autoempleo. El autoempleo también está ampliamente cubierto por la legislación de la Unión contra la discriminación.

[162] Ejemplo tomado de Boyd, K. y Andalibi, N., Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work [«Reconocimiento automático de emociones en el lugar de trabajo: cómo las tecnologías propuestas anticipan posibles futuros del trabajo», documento no disponible en español], en Nichols, J. (ed.), *Proceedings of the ACM on Human-Computer Interaction*, 2023.

- Que un supermercado o un banco utilice cámaras con el objetivo de detectar a clientes sospechosos para, por ejemplo, determinar que alguien está a punto de cometer un robo no está prohibido por el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial si se garantiza que no se hace un seguimiento de los empleados y que existen garantías suficientes.

b) «Centros educativos»

255) La referencia a los **centros educativos** es amplia y debe entenderse que comprende tanto los centros públicos como los privados. No hay limitaciones en cuanto a los tipos o edades de alumnos o estudiantes o de un entorno específico (en línea, presencial, de forma mixta[163], etc.). Por ejemplo, los centros de educación y formación de todos los niveles entran en el ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial, incluidos los centros de formación profesional, es decir, aquellos en los que los estudiantes aprenden capacidades que requieren el uso de sus manos[164] y una formación permanente[165]. Los centros educativos suelen estar acreditados o autorizados por las autoridades educativas nacionales pertinentes o las autoridades equivalentes. Una característica fundamental es que los centros educativos pueden expedir un certificado; la participación es una condición previa para obtenerlo. Debe entenderse que la prohibición también se aplica a los candidatos durante el proceso de admisión.

Por ejemplo:

- Una aplicación basada en la IA que utilice el reconocimiento de emociones para aprender una lengua en línea fuera de un centro educativo no está prohibida por el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial. En cambio, si un centro educativo obliga a los estudiantes a utilizar la aplicación, el uso de dicho sistema de reconocimiento de emociones está prohibido.
- No está prohibido que un centro educativo utilice un programa de seguimiento ocular basado en la IA cuando examina a los alumnos en línea para rastrear el punto visual y el movimiento ocular (el punto de fijación de la mirada, por ejemplo, para detectar si se utiliza material no autorizado), ya que el sistema no distingue ni infiere emociones. En cambio, el uso del sistema para detectar emociones, como la agitación emocional y la ansiedad, entraría en el ámbito de aplicación de la prohibición.
- Está prohibido que un centro educativo utilice un sistema de IA de reconocimiento de emociones para deducir el interés y la atención de los estudiantes. En cambio, si solo se utiliza con fines de aprendizaje en el contexto de un juego de rol (por ejemplo, para

163 Debe entenderse que el aprendizaje mixto adopta más de un enfoque en el proceso de educación y formación, como la combinación de herramientas de aprendizaje digital (incluido el aprendizaje por internet) y no digital.

164 Véase, por ejemplo, la evaluación de impacto que acompaña a la propuesta de la Comisión, en la que se mencionó que los usos específicos de IA por parte de las instituciones de formación profesional suponen una injerencia considerable en una amplia gama de derechos fundamentales, por ejemplo, en la evaluación: Comisión Europea, *Commission Staff Working Document. Impact Assessment. Annexes, SWD(2021)84 final, Part2/2* [«Documento de trabajo de los servicios de la Comisión, Evaluación de impacto. Anexos, SWD(2021)84 final, Parte 2/2», documento no disponible en español], p. 43. Véase también Tuomi, I., *The use of Artificial Intelligence (AI) in education* [«El uso de la inteligencia artificial (IA) en la educación», documento no disponible en español], Parlamento Europeo, 2020, pp. 9-10.

165 Véase el artículo 14 de la Carta.

formar a los actores o a los profesores), los sistemas de reconocimiento de emociones están permitidos si los resultados no pueden afectar a la evaluación o certificación de la persona que recibe la formación.

- Está prohibido que un centro educativo utilice un sistema de IA de reconocimiento de emociones durante las pruebas de acceso para nuevos estudiantes.
- No está prohibido utilizar un sistema de IA que permite detectar a los estudiantes que hablan entre ellos a través de sus teléfonos u otros canales durante las clases en línea de un centro educativo, ya que no deduce emociones. En cambio, el uso del sistema para detectar emociones, como la agitación emocional, la ansiedad y el interés, entraría en el ámbito de aplicación de la prohibición.
- Está prohibido que un centro educativo utilice un sistema de IA de reconocimiento de emociones tanto para los profesores (lugar de trabajo) como para los estudiantes (educación).

7.2.3. Excepciones por motivos médicos o de seguridad

256) La prohibición establecida en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial contiene una excepción explícita para el uso de sistemas de reconocimiento de emociones en los lugares de trabajo y en los centros educativos por motivos médicos o de seguridad, como los sistemas de uso terapéutico[166]. A la luz del objetivo del Reglamento de Inteligencia Artificial de garantizar un alto nivel de protección de los derechos fundamentales, esta excepción debe interpretarse restrictivamente.

257) En particular, los usos terapéuticos deben entenderse como los usos de dispositivos médicos con marcado CE. Además, esta excepción no comprende el uso de sistemas de reconocimiento de emociones para detectar aspectos generales del bienestar. El seguimiento general de los niveles de estrés en el lugar de trabajo no está permitido desde el punto de vista de la salud o la seguridad. Por ejemplo, un sistema de IA destinado a detectar el desgaste profesional o la depresión en el lugar de trabajo o en centros educativos no estaría contemplado en la excepción y seguiría estando prohibido.

258) Debe entenderse que la noción de motivos de seguridad dentro de esta excepción se aplica únicamente en relación con la protección de la vida y la salud, y no para otros intereses como, por ejemplo, proteger los bienes contra el robo o el fraude.

259) De esta interpretación restrictiva de la excepción se desprende que cualquier uso con fines médicos y de seguridad debe limitarse siempre a lo estrictamente necesario y proporcionado, en particular en cuanto a la duración, la aplicación personal y la escala, y debe ir acompañado de garantías suficientes. Estas garantías podrían incluir, por ejemplo, un informe previo de expertos, por escrito y motivado en relación con el caso de uso específico. La necesidad debe evaluarse sobre una base objetiva en relación con la finalidad médica y de seguridad, y no referirse a las «necesidades» del empleador o

[166] Considerando 44 del Reglamento de Inteligencia Artificial.

del centro educativo. En esta evaluación se debe indagar si existen medios alternativos menos intrusivos que permitan alcanzar el mismo objetivo.

260) Los empleadores y los educadores solo deben utilizar sistemas de reconocimiento de emociones por motivos médicos y de seguridad en caso de que exista una necesidad explícita[167]. Los datos recogidos y tratados en este contexto no pueden utilizarse para ningún otro fin. Esto es especialmente importante, dado que se ha demostrado que el uso de programas informáticos de gestión con IA en el trabajo tiene un impacto potencialmente negativo en la salud y la seguridad de los trabajadores. El seguimiento continuo a través de dispositivos ponibles, por ejemplo, puede aumentar el estrés laboral y repercutir en la productividad[168].

261) El considerando 18 del Reglamento de Inteligencia Artificial excluye de la definición de sistemas de reconocimiento de emociones los estados físicos, como el dolor o el cansancio; por ello, algunos sistemas de IA utilizados por razones de seguridad ya no estarían incluidos en dicha definición, como, por ejemplo, los sistemas utilizados para detectar el cansancio de los pilotos o conductores profesionales con el fin de evitar accidentes.

262) Otras normas, incluidas las normas de protección de datos, siguen siendo aplicables a los sistemas de reconocimiento de emociones que cumplan las condiciones de la excepción contemplada en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial[169].

263) Los sistemas de reconocimiento de emociones que se clasifiquen como sistemas de alto riesgo de conformidad con el artículo 6, apartado 2, y el anexo III, apartado 1, letra c), del Reglamento de Inteligencia Artificial deben cumplir los requisitos de alto riesgo establecidos en el capítulo III, sección 2, del Reglamento de Inteligencia Artificial y la obligación de transparencia de su artículo 50, apartado 3.

Por ejemplo:

El reconocimiento de emociones puede utilizarse por motivos médicos para ayudar a empleados o a estudiantes con autismo y mejorar la accesibilidad de las personas ciegas o sordas[170]. Estos usos entrarían en el ámbito de aplicación de la excepción por motivos médicos del artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial.

167 De conformidad con la legislación laboral de la UE, si se introducen estas nuevas tecnologías, los empleadores también deben consultar a los trabajadores o a sus representantes, respetando los procedimientos nacionales. Si no se respetan estos requisitos de procedimiento, dichos sistemas no pueden introducirse basándose en el Reglamento de Inteligencia Artificial como tal. También necesitarán un consentimiento desde el punto de vista de la legislación en materia de protección de datos, que sigue siendo aplicable.

168 Wolters Kluwer, «The Interconnection between the AI Act and the EU's Occupational Safety and Health Legal Framework - Global Workplace Law & Policy» [«La interconexión entre el Reglamento de Inteligencia Artificial y el marco jurídico de la UE en materia de salud y seguridad en el lugar de trabajo - Global Workplace Law & Policy», documento no disponible en español] (kluwerlawonline.com).

169 A partir de diciembre de 2026, se aplicará la Directiva (UE) 2024/2831 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativa a la mejora de las condiciones laborales en el trabajo en plataformas.

170 Los sistemas podrían resultar de utilidad para ayudar a los empleados o a los estudiantes o alumnos a comprender las emociones de sus compañeros, por ejemplo.

En cambio, el reconocimiento de emociones para evaluar el bienestar de los estudiantes o los empleados, los niveles de motivación y la satisfacción laboral o de aprendizaje no se considera un «uso por motivos médicos» y estaría prohibido.

Se prohibiría a un empleador que utilizase dispositivos o asistentes digitales posibilitados por la IA en el lugar de trabajo para medir la ansiedad basándose en los niveles de estrés medidos o para medir el aburrimiento de sus empleados, a menos que el elevado nivel de estrés o la falta de concentración suponga un peligro específico como, por ejemplo, si se manejan máquinas peligrosas o se manipulan sustancias químicas peligrosas. En este último caso, el empleador no puede utilizar los datos para otros fines, como para evaluar el rendimiento laboral del empleado.

7.3. Legislación más favorable de los Estados miembros

264) El artículo 2, apartado 11, del Reglamento de Inteligencia Artificial establece que la Unión o los Estados miembros podrán mantener o introducir «disposiciones legales, reglamentarias o administrativas que sean más favorables a los trabajadores en lo que atañe a la protección de sus derechos respecto al uso de sistemas de IA por parte de los empleadores». También puede permitirse o fomentarse la adopción de convenios colectivos que sean más favorables para los trabajadores.

Por ejemplo, los Estados miembros pueden adoptar leyes que establezcan que, en los lugares de trabajo, el uso de sistemas de reconocimiento de emociones con fines médicos no está autorizado.

7.4. Fuera del ámbito de aplicación

265) Como se ha mencionado anteriormente, quedan fuera del ámbito de aplicación:

- los sistemas de IA que deducen emociones y sentimientos que no se basan en datos biométricos,
- los sistemas de IA que infieren estados físicos como el dolor y el cansancio.

266) Los sistemas de reconocimiento de emociones utilizados en todos los demás ámbitos distintos de los lugares de trabajo y los centros educativos no entran en el ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial. Sin embargo, estos sistemas se consideran sistemas de IA de alto riesgo[171]. Al mismo tiempo, estos sistemas pueden prohibirse en determinados casos en virtud del artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial (manipulación y explotación perjudiciales) o en virtud de otras disposiciones de Derecho de la Unión. El resto de la legislación aplicable, como la legislación de la Unión en materia de protección de datos, protección de los consumidores, etc., sigue siendo aplicable a dichos sistemas.

Por ejemplo:

Los sistemas de reconocimiento de emociones utilizados en un contexto comercial para dirigirse a los clientes no entran en el ámbito de aplicación de la prohibición del

[171] Artículo 6, apartado 2, del Reglamento de Inteligencia Artificial y anexo III, apartado 1, letra c).

artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial, tanto si se basan en datos biométricos como si no. Por lo tanto, la prohibición no se aplica a, por ejemplo, los sistemas de IA que permiten el reconocimiento de emociones a partir de la pulsación de tecla o de los mensajes de voz de los clientes (como mensajes de chat, el uso de asistentes de voz virtuales), utilizados en la comercialización en línea de aplicaciones para mostrar mensajes personalizados y con fines publicitarios, incluso en los entornos inteligentes («vallas publicitarias inteligentes»).

No obstante, dichas prácticas pueden estar contempladas en las prohibiciones de manipulación y explotación perjudiciales establecidas en el artículo 5, apartado 1, letras a) y b), del Reglamento de Inteligencia Artificial[172] si se cumplen todas las condiciones para que se apliquen dichas prohibiciones.

a) Otros sistemas que quedan fuera del ámbito de aplicación

267) Por «control de multitudes» se entiende, en general, el control y el seguimiento del comportamiento de los grupos para mantener el orden (público) y la seguridad de los eventos. A menudo se asocia a las grandes multitudes (por ejemplo, partidos de fútbol, conciertos, etc.) o a lugares concretos, como aeropuertos o trenes. Los sistemas de control de multitudes pueden funcionar sin deducir las emociones de las personas; por ejemplo, pueden analizar el nivel de ruido y el estado de ánimo generales en un lugar determinado. En tal caso, el sistema no entraría en el ámbito de aplicación del artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial, ya que no deduce las emociones de una persona física (determinada).

268) Sin embargo, puede haber casos en los que estos sistemas de control de multitudes deduzcan las emociones de las personas, como, por ejemplo, detectando si hay muchas expresiones faciales de enfado. Por regla general, estos sistemas de IA no entrarían en el ámbito de aplicación de la prohibición del artículo 5, apartado 1, letra f), del Reglamento de Inteligencia Artificial, ya que no se suelen utilizar en el lugar de trabajo ni en los centros educativos.

269) También quedan fuera del ámbito de aplicación los sistemas que se utilizan en el ámbito médico, como los robots asistenciales, los sistemas de reconocimiento de emociones utilizados por los médicos durante un reconocimiento en su lugar de trabajo y los monitores de voz que analizan las llamadas de emergencia.

270) Estos sistemas suelen examinar a las personas que se encuentran en un contexto laboral, como el personal de seguridad en un estadio de fútbol o en una estación central (en donde se utilizan estos sistemas para reconocer comportamientos agresivos), o los empleados del sector médico. En estos casos, los responsables del despliegue deben aplicar garantías para evitar el control de los empleados, pero no puede evitarse por completo que tales sistemas también deduzcan las emociones de dichos empleados. Dado que el objetivo principal del sistema no es evaluar las emociones de los empleados, debe considerarse que estos sistemas quedan fuera del ámbito de aplicación

[172] Estas situaciones también podrían estar prohibidas por otras normas, como por la legislación en materia de protección de datos o de los consumidores.

de la prohibición. Los responsables del despliegue de dichos sistemas siguen siendo responsables de garantizar que los empleados no se vean afectados por su uso.

8. ARTÍCULO 5, APARTADO 1, LETRA G), DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: CATEGORIZACIÓN BIOMÉTRICA DE DETERMINADAS CARACTERÍSTICAS «SENSIBLES»

271) El artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial prohíbe los sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual. Esta prohibición no incluye el etiquetado, el filtrado ni la categorización de conjuntos de datos biométricos adquiridos de conformidad con el Derecho nacional o de la Unión, que pueden utilizarse, por ejemplo, con fines de garantía del cumplimiento del Derecho[173].

8.1. Justificación y objetivos

272) De la información biométrica puede extraerse, deducirse o inferirse, incluso sin el conocimiento de las personas afectadas, una gran variedad de información, en particular información «sensible», para clasificarlas. Esto puede dar lugar a un trato injusto y discriminatorio como, por ejemplo, los casos en que se deniega un servicio porque se considera que alguien es de una determinada raza. Los sistemas de categorización biométrica basados en la IA destinados a incluir a las personas físicas en categorías o colectivos específicos relacionados con aspectos como la orientación sexual o política o la raza menoscaban la dignidad humana y presentan un riesgo significativo para otros derechos fundamentales, como el derecho a la intimidad y la no discriminación. Por lo tanto, están prohibidos por el artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial.

8.2. Conceptos fundamentales y componentes de la prohibición

Según el artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial:

Quedan prohibidas las siguientes prácticas de IA:

g) la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual; esta prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basado en datos biométricos ni la categorización de datos biométricos en el ámbito de la garantía del cumplimiento del Derecho;

[173] Considerando 30 del Reglamento de Inteligencia Artificial.

273) Deben cumplirse varias condiciones acumulativas para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial:

(i) La práctica debe suponer la «introducción en el mercado», la «puesta en servicio para este fin específico» o el «uso» de un sistema de IA;

(ii) el sistema debe ser un sistema de categorización biométrica;

(iii) las personas físicas deben clasificarse individualmente;

(iv) sobre la base de sus datos biométricos;

(v) para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual.

274) Para que se aplique la prohibición, deben cumplirse simultáneamente las cinco condiciones. La primera condición, a saber, la «introducción en el mercado», la «puesta en servicio» o la «utilización» de un sistema de IA, se analiza en la sección 2.3. Así pues, la prohibición se aplica tanto a los proveedores como a los responsables del despliegue de sistemas de IA, cada uno dentro de sus respectivas responsabilidades de no introducir en el mercado, poner en servicio o utilizar dichos sistemas de IA. A continuación se describen y analizan con más detalle las otras condiciones para la aplicación de la prohibición[174].

275) La prohibición no incluye el etiquetado o filtrado de conjuntos de datos biométricos adquiridos lícitamente, en particular con fines de garantía del cumplimiento del Derecho.

8.2.1. Sistema de categorización biométrica

276) «La categorización [...] de un individuo por un sistema biométrico es típicamente el proceso de establecer si sus datos biométricos pertenecen a un grupo con características predefinidas [...]. [N]o es importante identificar o verificar al individuo, sino asignarle automáticamente a una categoría determinada. Por ejemplo, una pantalla de publicidad podrá mostrar diferentes anuncios dependiendo del individuo que la mira, basándose en su edad o sexo»[175]. Las personas también pueden ser categorizadas simplemente por razones estadísticas, sin que sean identificadas y sin que ese sea el objetivo.

277) En el artículo 3, punto 40, del Reglamento de Inteligencia Artificial se define «sistema de categorización biométrica» como un sistema de IA destinado a incluir a las personas físicas en categorías específicas en función de sus datos biométricos, a menos que sea accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas. Como se explica en la sección 7.2.1, letra d), los «datos biométricos» se definen en el artículo 3, punto 34, del Reglamento de Inteligencia Artificial. En particular, los datos biométricos comprenden características conductuales basadas en características biométricas. El ámbito de aplicación de la categorización biométrica

[174] Para la condición de «sistema de IA», la «introducción en el mercado», la «puesta en servicio para este fin específico» o el «uso», véase *más arriba*.

[175] Véase el *Dictamen 3/2012 sobre la evolución de las tecnologías biométricas* del Grupo de Trabajo del Artículo 29 y, WP193, 27.4.2012, p. 6.

excluye la categorización en función de la ropa o los accesorios, como bufandas o cruces, así como la actividad en las redes sociales.

278) La categorización biométrica puede basarse en categorías de características físicas, como los rasgos y la forma de la cara o el color de la piel, en función de las cuales se incluye a las personas en categorías específicas. Algunas de estas categorías pueden tener un carácter especialmente «sensible» o ser características protegidas por el Derecho de la Unión en materia de no discriminación, como la raza. Sin embargo, la categorización biométrica también puede basarse en el ADN o en aspectos conductuales, como el análisis las pulsaciones de tecla o el modo de andar de una persona[176].

279) Para quedar fuera del ámbito de aplicación de la definición de categorización biométrica en el Reglamento de Inteligencia Artificial, deben cumplirse acumulativamente dos condiciones: ser «accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas».

280) Según el considerando 16 del Reglamento de Inteligencia Artificial, una característica meramente accesoria es una característica intrínsecamente vinculada a otro servicio comercial, lo que significa que la característica no puede utilizarse, por razones técnicas objetivas, sin el servicio principal y que la integración de dicha característica o funcionalidad no es un medio para eludir la aplicabilidad de las normas de dicho Reglamento.

Por ejemplo, según el artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial, están permitidos los siguientes usos de la IA:

- Los filtros que clasifican las características faciales o corporales utilizados en los mercados en línea para permitir a un consumidor previsualizar cómo le quedaría un producto podrían constituir una característica accesoria de este tipo, ya que solo pueden utilizarse en relación con el servicio principal, que consiste en vender un producto.
- Los filtros integrados en los servicios de redes sociales que clasifican las características faciales o corporales a fin de que los usuarios puedan añadir o modificar imágenes o vídeos también podrían considerarse una característica accesoria, ya que dichos filtros no pueden utilizarse sin el servicio principal de las redes sociales, que consiste en compartir contenidos en línea.

Por el contrario, estos son algunos ejemplos de usos que estarían prohibidos:

- Un sistema de IA categoriza a las personas activas en una plataforma de redes sociales en función de su supuesta orientación política, mediante el análisis de los datos biométricos de las fotografías que han subido a la plataforma, para enviarles mensajes políticos específicos. Si bien un sistema de este tipo solo puede ser accesorio a la publicidad política, no sería «estrictamente necesario por razones técnicas objetivas»,

[176] Véase, por ejemplo, el *Dictamen 3/2012 sobre la evolución de las tecnologías biométricas* del Grupo de Trabajo del Artículo 29 y, WP193, 27.4.2012, pp. 16-17. El Grupo se refiere aquí al «reconocimiento ligero» (p. 18), es decir, la «detección de comportamientos o necesidades específicas de las personas».

por lo que no se cumplen las condiciones para excluirlo de la definición de categorización biométrica.

- Un sistema de IA que categoriza a las personas activas en una plataforma de redes sociales en función de su supuesta orientación sexual mediante el análisis de los datos biométricos de las fotografías compartidas en dicha plataforma y, sobre esa base, les ofrece publicidad se consideraría una categorización biométrica en el sentido del Reglamento de Inteligencia Artificial. Además, en este caso no existe una necesidad estricta de este «servicio accesorio», por lo que no se aplica la exclusión de la prohibición.

8.2.2. Las personas se clasifican individualmente sobre la base de sus datos biométricos

281) El uso de datos biométricos para categorizar a las personas físicas es un elemento fundamental para que se aplique la prohibición [véase la sección 8.2.1 y el apartado 7.2.1.d)].

282) Además, para que se aplique la prohibición, las personas físicas deben clasificarse «individualmente». Si esta no es la finalidad o el resultado de la categorización biométrica, la prohibición no se aplica, como, por ejemplo, si se clasifica a todo un colectivo sin tener en cuenta al individuo.

Estos son algunos ejemplos de categorización individual:

- Sistemas de IA que llevan a cabo una «estimación de atributos» (datos demográficos), como, por ejemplo, «edad, género, etnia», sobre la base del aspecto físico, como la cara, la altura o el color de la piel, los ojos y el pelo (o una combinación de ambos).
- Sistemas de IA capaces de clasificar a las personas y de distinguirlas en función de un rasgo concreto (como una cicatriz bajo el ojo derecho, por ejemplo) o porque tienen un tatuaje en su mano derecha.

Estos casos de uso son ejemplos de categorización biométrica individual. Para que estos ejemplos entren en el ámbito de aplicación de la prohibición del artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial, deben cumplirse todas las condiciones de dicha disposición.

8.2.3. Para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual

283) El artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial prohíbe únicamente los sistemas de categorización biométrica que tengan el objetivo de deducir o inferir un número limitado de características sensibles: raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual.

Estos son algunos ejemplos de sistemas prohibidos por el artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial:

- un sistema de categorización biométrica que afirma ser capaz de deducir la raza de una persona a partir de su voz. No es lo mismo que un sistema que clasifica a las personas en función del color de la piel o los ojos, o de un sistema que analiza el ADN de las víctimas de delitos en función de su origen; estos sistemas no estarían prohibidos.
- un sistema de categorización biométrica que afirma ser capaz de deducir la orientación religiosa de una persona a partir de sus tatuajes o su rostro.

8.3. Fuera del ámbito de aplicación

284) La prohibición establecida en el artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial no se aplica a los sistemas de IA que etiquetan o filtran conjuntos de datos biométricos adquiridos lícitamente, como imágenes, basados en datos biométricos, en particular en el ámbito de la garantía del cumplimiento del Derecho; Esto se explica con más detalle en el considerando 30 del Reglamento de Inteligencia Artificial[177].

285) Los sistemas de categorización biométrica pueden etiquetar o filtrar los conjuntos de datos biométricos precisamente para garantizar que los datos representan por igual a todos los grupos demográficos y que, por ejemplo, no se sobrerrepresenta a un grupo específico. Si los datos utilizados para el entrenamiento de un algoritmo están sesgados en contra de un colectivo específico (es decir, si existen diferencias sistemáticas en los datos entre los colectivos debido a la forma en que se recogen los datos o si los datos están históricamente sesgados), el algoritmo puede replicar este sesgo, lo que puede dar lugar a una discriminación ilícita contra personas o colectivos de personas[178]. Por este motivo, el etiquetado basado en determinada información sensible protegida puede ser necesario para garantizar datos de alta calidad, precisamente para evitar la discriminación. El Reglamento de Inteligencia Artificial puede incluso exigir que las operaciones de etiquetado se ajusten a los requisitos establecidos en dicho Reglamento para los sistemas de IA de alto riesgo[179]. Por lo tanto, dicho etiquetado o filtrado de datos biométricos está explícitamente exento de la prohibición establecida en el artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial. La prohibición solo es de aplicación cuando se categorizan los datos biométricos para inferir la raza, las opiniones políticas, la afiliación sindical, las convicciones religiosas o filosóficas, la vida sexual o la orientación sexual.

Estos son algunos ejemplos de etiquetado o filtrado permitidos:

- el etiquetado de datos biométricos para evitar los casos en los que un miembro de un colectivo étnico tiene menos posibilidades de ser invitado a una entrevista de trabajo

177 Considerando 30 del Reglamento de Inteligencia Artificial: «Dicha prohibición no debe aplicarse al etiquetado, al filtrado ni a la categorización lícitos de conjuntos de datos biométricos adquiridos de conformidad con el Derecho nacional o de la Unión en función de datos biométricos, como la clasificación de imágenes en función del color del pelo o del color de ojos, que pueden utilizarse, por ejemplo, en el ámbito de la garantía del cumplimiento del Derecho».

178 *Ibid*.

179 Véanse, por ejemplo, los artículos 10 y 17 del Reglamento de Inteligencia Artificial.

porque el algoritmo ha sido «entrenado» con datos en los que ese colectivo concreto obtiene peores resultados que otros[180].

- la categorización de los pacientes usando imágenes en función del color de la piel o de los ojos puede ser importante para los diagnósticos médicos, como, por ejemplo, los diagnósticos de cáncer.

286) El artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial también establece que la prohibición de dicha disposición no se aplica al etiquetado o filtrado de conjuntos de datos adquiridos lícitamente en el ámbito de la garantía del cumplimiento del Derecho[181].

Esto se refiere, por ejemplo, al uso por parte de las autoridades garantes del cumplimiento del Derecho de un sistema de IA que permita etiquetar y filtrar un conjunto de datos sospechosos de contener material de abuso sexual de menores. En una fase inicial, las autoridades se servirían de los sistemas de IA para que les ayudasen a detectar y eliminar los datos sensibles de las imágenes. Además, el filtrado y etiquetado en función del género, la edad o los datos biométricos como el color de los ojos y del pelo, las cicatrices y las marcas podrían ayudar a identificar a las víctimas o a establecer relaciones con otros casos. Del mismo modo, está permitido filtrar y etiquetar las manos de los agresores sobre la base de características específicas como la longitud de los dedos o cualquier marca o tatuaje distintivos que ayuden a identificar a los posibles sospechosos.

8.4. Relación con otras disposiciones del Derecho de la Unión

287) El Reglamento de Inteligencia Artificial[182] clasifica como de alto riesgo[183] los sistemas de IA destinados a ser utilizados para la categorización biométrica conforme a atributos o características sensibles protegidos por el artículo 9, apartado 1, del RGPD sobre la base de datos biométricos, en la medida en que no estén prohibidos en virtud del Reglamento de Inteligencia Artificial.

288) El artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial restringe aún más las posibilidades de un tratamiento lícito de datos personales en el marco de la legislación de la Unión en materia de protección de datos, como el RGPD, la Directiva sobre protección de datos en el ámbito penal y el RPDUE. En particular, el artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial excluye las posibilidades de categorización biométrica de las personas físicas sobre la base de sus datos biométricos, tal como se definen en dicho Reglamento, para inferir la raza, las opiniones políticas, la afiliación sindical, las convicciones religiosas o filosóficas, la vida sexual o la orientación sexual, sin perjuicio de la excepción para el etiquetado o filtrado de

180 Agencia de los Derechos Fundamentales de la Unión Europea, *# BigData. Discrimination in data supported decision making* [«#Macrodatos. Discriminación en la toma de decisiones basada en datos», documento no disponible en español], Luxemburgo, 2018, 14, p. 5.

181 Las disposiciones del Reglamento de Inteligencia Artificial relativas al uso de sistemas de categorización biométrica para la garantía del cumplimiento del Derecho se basan en el artículo 16 del TFUE. Véase también el considerando 3 del Reglamento de Inteligencia Artificial.

182 Considerando 54 y anexo III, punto 1, letra b), del Reglamento de Inteligencia Artificial.

183 Considerando 54 y anexo III, punto 1, letra b), del Reglamento de Inteligencia Artificial.

conjuntos de datos biométricos adquiridos lícitamente, en particular en el ámbito de la garantía del cumplimiento del Derecho, tal como se ha descrito anteriormente. Además, la prohibición establecida en el artículo 5, apartado 1, letra g), del Reglamento de Inteligencia Artificial es coherente con el artículo 11, apartado 3, de la Directiva sobre protección de datos en el ámbito penal, que prohíbe explícitamente toda «elaboración de perfiles» que dé lugar a una discriminación sobre la base de categorías especiales de datos personales, como la raza, el origen étnico, la orientación sexual, las opiniones políticas o las convicciones religiosas.

9. ARTÍCULO 5, APARTADO 1, LETRA H), DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL: SISTEMAS DE IDENTIFICACIÓN BIOMÉTRICA REMOTA EN TIEMPO REAL CON FINES DE GARANTÍA DEL CUMPLIMIENTO DEL DERECHO

289) El artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial prohíbe el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público y con fines de garantía del cumplimiento del Derecho, con las excepciones limitadas taxativamente definidas en el Reglamento de Inteligencia Artificial En concreto, el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial contempla tres situaciones en las que puede permitirse el uso de dichos sistemas cuando así lo autorice la legislación nacional y cuando se cumplan las condiciones y garantías establecidas en el artículo 5, apartados 2 a 7, del Reglamento de Inteligencia Artificial.

290) De conformidad con el artículo 5, apartado 5, del Reglamento de Inteligencia Artificial, los Estados miembros son libres de decidir si se permite en su territorio el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho y en cuál de las tres situaciones. De no existir una norma nacional que permita y regule dicho uso, las autoridades garantes del cumplimiento del Derecho y las entidades que actúan en su nombre no pueden utilizar tales sistemas con fines de garantía del cumplimiento del Derecho. Así pues, la existencia de una normativa nacional que cumpla los requisitos pertinentes del Reglamento de Inteligencia Artificial es un requisito previo para dicho uso.

291) El artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial prohíbe únicamente el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público y con fines de garantía del cumplimiento del Derecho, por lo que únicamente se refiere a los responsables del despliegue de dichos sistemas. La introducción en el mercado y la puesta en servicio de estos sistemas, así como el uso de otros sistemas de identificación biométrica remota, no están prohibidos, sino sujetos las normas para los sistemas de IA de alto riesgo de conformidad con el artículo 6, apartado 2, y el anexo III, letra a), del Reglamento de Inteligencia Artificial[184]. Cuando un Estado miembro autoriza el uso de sistemas de identificación biométrica remota en

[184] Además de las normas específicas aplicables al uso retroactivo de sistemas de identificación biométrica remota con fines de garantía del cumplimiento del Derecho (artículo 26, apartado 10, del Reglamento de Inteligencia Artificial).

tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los tres objetivos enumerados en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial, las normas aplicables a los sistemas de IA de alto riesgo también se aplican a dicho uso.

292) Por último, se aplican normas específicas al uso retroactivo de los sistemas de identificación biométrica remota con fines de garantía del cumplimiento del Derecho. Si bien este uso que no se hace en tiempo real no está prohibido, está sujeto a garantías adicionales para el despliegue de sistemas de IA de alto riesgo (artículo 26, apartado 10, del Reglamento de Inteligencia Artificial).

9.1. Justificación y objetivos

293) El considerando 32 del Reglamento de Inteligencia Artificial reconoce que los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho invaden los derechos y las libertades de las personas afectadas, en la medida en que puede afectar a la vida privada de una gran parte de la población, provocar la sensación de estar bajo una vigilancia constante y disuadir indirectamente a los ciudadanos de ejercer su libertad de reunión y otros derechos fundamentales. Las imprecisiones técnicas de los sistemas de IA destinados a la identificación biométrica remota de las personas físicas pueden dar lugar a resultados sesgados y tener efectos discriminatorios. Tales posibles resultados sesgados y efectos discriminatorios son especialmente pertinentes por lo que respecta a la edad, la etnia, la raza, el sexo o la discapacidad. Además, la inmediatez de las consecuencias y las escasas oportunidades para realizar comprobaciones o correcciones adicionales en relación con el uso de sistemas que operan «en tiempo real» acrecientan el riesgo que estos suponen para los derechos y las libertades de las personas afectadas en el contexto de actividades de garantía del cumplimiento del Derecho, o afectadas por estas.

294) Sin embargo, cuando el uso de dichos sistemas sea estrictamente necesario para lograr un interés público esencial y las situaciones en las que pueda producirse dicho uso estén enumeradas de manera limitativa y definidas con precisión, dicho uso compensa los riesgos para los derechos fundamentales (considerando 33 del Reglamento de Inteligencia Artificial). Para velar por que dichos sistemas se utilicen «de manera responsable y proporcionada», su uso está sujeto a las garantías y a las obligaciones y requisitos específicos del artículo 5, apartados 2 a 7, del Reglamento de Inteligencia Artificial.

9.2. Conceptos fundamentales y componentes de la prohibición

Artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial:

Quedan prohibidas las siguientes prácticas de IA:

h) el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho, salvo y en la

medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:

i) la búsqueda selectiva de víctimas concretas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas,

ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista,

iii) la localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años.

El párrafo primero, letra h), se entiende sin perjuicio de lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 en lo que respecta al tratamiento de datos biométricos con fines distintos de la garantía del cumplimiento del Derecho.

295) Deben cumplirse varias condiciones acumulativas para que se aplique la prohibición establecida en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial:

(i) El sistema de IA debe ser un sistema de identificación biométrica remota;

(ii) la actividad consiste en el «uso» de dicho sistema;

(iii)en «tiempo real»;

(iv)en espacios de acceso público, y

(v) con fines de garantía del cumplimiento del Derecho.

296) La segunda condición, es decir, el «uso» del sistema de IA, ya se ha analizado en la sección 2.3de las presentes directrices. A continuación se describen y analizan con más detalle las demás condiciones enumeradas anteriormente.

9.2.1. El concepto de identificación biométrica remota

297) Las tecnologías de reconocimiento biométrico detectan, recogen y transforman características físicas mensurables (como la distancia entre los ojos y su tamaño, la longitud de la nariz, etc.) o características conductuales (como el modo de andar o la voz) en datos biométricos legibles por máquina [véase la sección 7.2.1, letra d)]. Estos datos están disponibles en diferentes formas: imágenes o plantillas, que constituyen una representación matemática de las características más destacadas de una persona, utilizadas a efectos de reconocimiento. Las tecnologías de reconocimiento biométrico se utilizan con fines de verificación e identificación[185].

[185] Según la definición de la comunidad biométrica en la norma ISO/IEC 2382-37:2022 Tecnología de la información — Vocabulario, reconocimiento biométrico, término 37.01.03.

298) De acuerdo con el artículo 3, punto 41, del Reglamento de Inteligencia Artificial, un sistema de identificación biométrica remota es

> *un sistema de IA destinado a identificar a las personas físicas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia.*

299) Esta definición se refiere únicamente a la función de identificación de los sistemas de reconocimiento biométrico, lo que supone la ausencia de participación activa por parte de las personas afectadas (es decir, no hay una intervención activa) y la recogida de sus características, por lo general, a distancia. Para llevar a cabo la identificación, los datos biométricos recogidos se comparan con los datos biométricos ya almacenados en una base de datos de referencia (como un repositorio, por ejemplo, una base de datos delictivos que contiene imágenes faciales o plantillas de sospechosos).

a) Únicamente a efectos de identificación

300) El concepto de «identificación biométrica» se define en el artículo 3, punto 35, del Reglamento de Inteligencia Artificial como

> *el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos.*

301) El considerando 15 del Reglamento de Inteligencia Artificial aclara además que entre dichas características humanas pueden contarse

> *la cara, el movimiento ocular, la forma del cuerpo, la voz, la entonación, el modo de andar, la postura, la frecuencia cardíaca, la presión arterial, el olor o las características de las pulsaciones de tecla.*

302) Los sistemas de IA utilizados para seguir a personas físicas también pueden incluirse en la definición de identificación biométrica, como por ejemplo, cuando el objetivo es ver hacia qué dirección escapa un sospechoso. Esto puede deducirse del artículo 5, apartado 1, letra h), inciso iii), del Reglamento de Inteligencia Artificial, que permite la localización de personas sospechosas de haber cometido un delito. La localización es posible cuando se sigue a una persona.

303) Los sistemas de IA destinados a ser utilizados para la verificación biométrica quedan fuera del ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial[186]. La verificación biométrica (o autenticación) consiste en comparar los datos presentados en un sensor con otro conjunto de datos previamente registrados, almacenados en un dispositivo como un teléfono inteligente, un pasaporte o un documento de identidad. La finalidad de la verificación biométrica es comprobar que una determinada persona es quien afirma ser.

[186] Considerando 17 del Reglamento de Inteligencia Artificial.

Un ejemplo de verificación biométrica es la comparación de la cara de un pasajero escaneada en una puerta automática con la imagen facial de su pasaporte.

b) Carácter remoto

304) Según el artículo 3, punto 41, del Reglamento de Inteligencia Artificial, el carácter remoto se refiere a la capacidad de los sistemas biométricos de identificar a las personas sin su participación activa y generalmente a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia.

305) El uso de sistemas biométricos para confirmar la identidad de una persona física con la finalidad exclusiva de tener acceso a un servicio, desbloquear un dispositivo o tener acceso de seguridad a un local queda excluido del concepto de «remoto» (considerando 15 del Reglamento de Inteligencia Artificial). Esta modalidad se utiliza, por ejemplo, en los controles de acceso[187].

Por ejemplo, se despliega un sistema de identificación facial para permitir la entrada en una zona de acceso restringido (por ejemplo, en instalaciones de una central eléctrica) mediante una tecnología de escaneo facial; el sistema compara el rostro de la persona que se presenta delante de la cámara en la entrada con una imagen de referencia en una base de datos de referencia de personas autorizadas a entrar en el edificio.

306) El considerando 17 del Reglamento de Inteligencia Artificial aclara que dicha exclusión del ámbito de aplicación de la prohibición se justifica por el hecho de que tales sistemas probablemente tengan una repercusión menor en los derechos fundamentales de las personas físicas que los sistemas de identificación biométrica remota que puedan utilizarse para el tratamiento de los datos biométricos de un gran número de personas sin su participación activa. En dicho considerando se aclara que los sistemas de identificación biométrica remota suelen utilizarse para detectar a varias personas o su comportamiento de forma simultánea, a fin de simplificar considerablemente la identificación de personas sin su participación activa. Para que se trate de una participación activa, no basta con que se informe a las personas sobre la presencia de cámaras, sino que deben intervenir activa y conscientemente delante de una cámara instalada de manera que se fomente una participación activa.

A continuación, varios ejemplos:

- Sistemas de identificación biométrica remota que se utilizan en cámaras instaladas en paredes o techos de las estaciones de metro con fines de vigilancia. Dicho sistema cumple la condición de carácter remoto.

- Los sistemas que se utilizan para permitir el acceso a una estación de metro, como los billetes de metro biométricos, en los que las personas participan activamente y se

187 Por ejemplo, Ross, A. y Jain, A. K., «Biometrics, Overview» [«Biometría, una síntesis», documento no disponible en español], en Li, S.Z. y Jain A.K. (eds.), *Encyclopedia of Biometrics*, 1ª ed., Springer Science, New York, 2015, pp. 289-294.

acercan conscientemente al sensor biométrico para obtener acceso, no cumplen dicha condición.

307) Los sistemas de reconocimiento biométrico que procesan impresiones dactilares (sin contacto), el modo de andar, la voz, el ADN, las pulsaciones de tecla y otras señales conductuales (biométricas) también pueden constituir sistemas de identificación biométrica remota[188].

Por ejemplo:

- Puede desplegarse un sistema de tecnología biométrica de voz para identificar a una persona que está hablando. A continuación, el micrófono recoge la muestra biométrica.
- Puede utilizarse un sistema de reconocimiento del modo de andar a través de un circuito cerrado de televisión; los vídeos se comprueban automáticamente para encontrar coincidencias con plantillas previamente recogidas.
- Puede utilizarse la tecnología biométrica de pulsaciones de tecla para identificar a la persona que escribe un mensaje fraudulento.

Que estos sistemas se utilicen como ejemplos de sistemas de identificación biométrica remota no significa que estén prohibidos por el artículo 5 del Reglamento de Inteligencia Artificial.

308) En el caso de las cámaras corporales capaces de llevar a cabo una identificación biométrica remota, utilizadas por agentes de las autoridades garantes del cumplimiento del Derecho, se considerará que la grabación no selectiva durante una manifestación con cientos de participantes, por ejemplo, cumple la condición de carácter remoto.

c) Base de datos de referencia

309) La identificación no es posible sin una base de datos de referencia que contenga datos biométricos a efectos de comparación. Así pues, la existencia de una base de datos de referencia es **imprescindible** para realizar la comparación con fines de identificación[189].

Por ejemplo, en el caso de personas desaparecidas, la base de datos del Sistema de Información de Schengen[190] podría utilizarse como base de datos de referencia a efectos de reconocimiento facial (una vez que esté operativa).

9.2.2. En tiempo real

310) «En tiempo real» significa que el sistema recoge y procesa datos biométricos «de manera instantánea, casi instantánea o, en cualquier caso, sin una importante

188 Dictamen conjunto 5/2021 del CEPD-SEPD, p. 11; Consejo de la Unión Europea, «Dictamen del Servicio Jurídico», 12302/22, 12 de septiembre de 2022, apartado 33, y considerando 15 del Reglamento de Inteligencia Artificial.

189 Considerando 34 del Reglamento de Inteligencia Artificial.

190 Descripciones relativas a personas desapareadas (artículo 32 de la Decisión SIS II); Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II)

demora»[191]. Todas las etapas del tratamiento, es decir, la recogida, la comparación y la identificación de datos biométricos, se producen de forma simultánea o casi simultánea, lo que puede incluir una «demora mínima limitada» para evitar que se eluda la prohibición mediante el uso retroactivo de sistemas de identificación biométrica remota[192]. El concepto de «sin una demora significativa» no se define en el Reglamento de Inteligencia Artificial; deberá evaluarse caso por caso. Dado que los dispositivos utilizados para la identificación remota en tiempo real o en diferido son cada vez más los mismos con diferentes funcionalidades, la distinción entre ambos es de carácter temporal. En términos generales, se considera que la demora es significativa cuando, como mínimo, es probable que la persona haya abandonado el lugar en donde se recogieron los datos biométricos.

311) En general, los sistemas en tiempo real se utilizan en un lugar determinado para facilitar una reacción rápida, y no para identificar a las personas *a posteriori*. Proporcionan al usuario del sistema un medio de seguimiento y control de los movimientos de las personas sometidas a vigilancia.

a) Un sistema de IA realiza un control de todos los asistentes que entran en una sala de conciertos: identificación biométrica remota en tiempo real.

b) Un sistema graba a todos los asistentes que llegan a un concierto. Se produce un incidente durante el concierto y, una vez finalizado, se utiliza el sistema de identificación en el material de vídeo para identificar al autor de la infracción: identificación biométrica remota en diferido.

312) Cuando una autoridad garante del cumplimiento del Derecho toma de forma encubierta una fotografía de una persona con un dispositivo móvil y la carga en una base de datos para hacer una búsqueda inmediata, en función de las circunstancias, podrá aplicarse la prohibición establecida en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial.

9.2.3. En espacios de acceso público

313) En el artículo 3, punto 44, del Reglamento de Inteligencia Artificial se definen los **espacios de acceso público** como

> *cualquier lugar físico, de propiedad privada o pública, al que pueda acceder un número indeterminado de personas físicas, con independencia de que deban cumplirse determinadas condiciones de acceso y con independencia de las posibles restricciones de capacidad.*

314) En el considerando 19 del Reglamento de Inteligencia Artificial se enumeran varios elementos característicos de dichos espacios:

- El espacio debe ser accesible para un número indeterminado de personas, con independencia de posibles restricciones de capacidad o de seguridad, como la adquisición de una entrada o un título de transporte, el registro previo o tener una

[191] Considerando 17 del Reglamento de Inteligencia Artificial.
[192] Artículo 3, punto 42, del Reglamento de Inteligencia Artificial.

determinada edad. La posibilidad de acceder a un espacio a través de una puerta que no está cerrada con llave no significa que el espacio sea de acceso público, si hay indicios o circunstancias que sugieran lo contrario (como una señal que restrinja el acceso). Además, el acceso a un espacio puede limitarse a determinadas personas, conforme a lo definido en el Derecho, en relación con la seguridad pública o la decisión de la persona que ejerza la autoridad pertinente sobre el espacio.

Estos son algunos ejemplos de espacios de acceso público, en principio:

- el lugar de un concierto por el que los participantes pagan un precio de entrada;
- el lugar de un evento en el que se organiza una feria comercial dirigida a participantes mayores de 50 años.

Un espacio cerrado por una puerta, aunque no esté cerrada con llave, como la entrada con portón de una zona residencial vallada en donde hay varias viviendas, no se considera normalmente un espacio de acceso público. En cambio, un parque dentro de una residencia vallada que tiene un horario de apertura al público y no impone restricciones de acceso durante ese horario se considera, por lo general, un espacio de acceso público durante esas horas y un espacio cerrado fuera de ese horario.

- El carácter público o privado del espacio es irrelevante, es decir, no es necesario que un espacio sea de propiedad pública para que pueda considerarse un espacio de acceso público.

Por ejemplo, el espacio puede pertenecer a una entidad privada, a una entidad pública o una entidad pública gestionada por una privada, sin que ello afecte a la naturaleza del espacio.

- El espacio no se utiliza para una actividad específica; una zona de acceso público no es necesariamente un espacio vinculado a un servicio público. Además, en un espacio vinculado a un servicio público puede haber espacios no accesibles al público, como las oficinas de los funcionarios que trabajan en un ayuntamiento.

Los espacios de acceso público pueden utilizarse, por ejemplo, para actividades comerciales, como, tiendas, restaurantes, cafés, etc.; de prestación de servicios, como bancos, actividades profesionales (una consulta médica o una oficina de contabilidad), hostelería (un hotel, por ejemplo), etc.; deportivas, como piscinas, gimnasios, estadios, etc.; de transporte, como estaciones de autobús, metro y ferrocarril, aeropuertos, medios de transporte, etc.; de entretenimiento, como cines, teatros, museos, salas de conciertos y conferencias, etc.; de ocio o de otro tipo, como vías y plazas públicas, parques, bosques, parques infantiles[193].

[193] Considerando 19 del Reglamento de Inteligencia Artificial.

315) Los siguientes espacios no constituyen espacios de acceso público en el sentido del artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial:

- Los espacios en línea, ya que no son espacios físicos en el sentido del artículo 3, letra 44, del Reglamento de Inteligencia Artificial.

> Por ejemplo, las salas para chatear, las redes sociales o las plataformas en línea, etc., quedan, por tanto, excluidas del ámbito de aplicación de la prohibición.

- Determinados espacios concebidos para que accedan a ellos un número limitado de personas, como las fábricas, las empresas y los lugares de trabajo con control de entrada o limitaciones a los empleados o proveedores de servicios pertinentes, ya que se pretende que solo estas personas puedan acceder a ellos[194].

> Por ejemplo, un lugar de trabajo accesible con una tarjeta de acceso no se considera, en principio, un espacio de acceso público, mientras que una oficina sin controles de entrada puede serlo.

- **Ni las prisiones ni las zonas en que se realizan inspecciones fronterizas** son espacios de acceso público[195].

316) Por ejemplo, un paso fronterizo no es un espacio de acceso público, pero, en principio, la calle que conduce a dicho paso o un bosque en las proximidades sí lo es.

317) Algunos espacios pueden tener una doble función. Por ejemplo, un aeropuerto se considera, en términos generales, un espacio de acceso público en lo que respecta a sus zonas comunes; sin embargo, la zona destinada al control fronterizo (en donde se encuentran los funcionarios de aduanas y se realizan los controles de pasaportes o documentos de identidad) queda excluida del ámbito de aplicación de la prohibición.

318) Tal como se precisa en el considerando 19 del Reglamento de Inteligencia Artificial, determinar si un espacio es accesible al público debe hacerse sobre la base de un análisis caso por caso.

9.2.4. Con fines de garantía del cumplimiento del Derecho

319) La prohibición establecida en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial se aplica al uso de sistemas de identificación biométrica remota con fines de garantía del cumplimiento del Derecho, independientemente de la entidad, autoridad u organismo que lleve a cabo las actividades de garantía del cumplimiento del Derecho.

320) La «garantía del cumplimiento del Derecho» se define en el artículo 3, punto 46, del Reglamento de Inteligencia Artificial como «las actividades realizadas por las

194 Considerando 19 del Reglamento de Inteligencia Artificial.

195 Considerando 19 del Reglamento de Inteligencia Artificial. En un contexto diferente, el control fronterizo se ha definido como la actividad realizada en las fronteras, de conformidad con el Reglamento (UE) 2016/399 (Código de fronteras Schengen) y a efectos de este, en respuesta exclusivamente a la intención de cruzar la frontera o al propio acto de cruzarla. No se incluye en el espacio de control fronterizo la denominada «zona fronteriza», que puede extenderse hasta un máximo de 50 kilómetros a ambos lados de la frontera.

autoridades garantes del cumplimiento del Derecho, o en su nombre, para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas». Estos fines son los mismos que los que se enumeran en el artículo 1 de la Directiva sobre protección de datos en el ámbito penal[196]. Así pues, cualquier interpretación de estos fines en relación con la Directiva sobre protección de datos en el ámbito penal también puede ser pertinente para interpretar el concepto de «garantía del cumplimiento del Derecho» utilizado en el Reglamento de Inteligencia Artificial.

321) Entre los fines de garantía del cumplimiento del Derecho pueden contarse la investigación, la detección y el enjuiciamiento de delitos. También se incluyen las actividades relacionadas con la prevención de delitos, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, antes de que se haya cometido realmente un delito. Por ejemplo, la policía puede adoptar «medidas coercitivas [...] en manifestaciones, grandes acontecimientos deportivos y disturbios» en el contexto de la prevención de la delincuencia[197]. Por último, también se incluye en estas actividades la ejecución de sanciones, como las penas.

322) De conformidad con el artículo 3, punto 46, del Reglamento de Inteligencia Artificial, las actividades de garantía del cumplimiento del Derecho pueden ser llevadas a cabo por las autoridades garantes del cumplimiento del Derecho o en su nombre. Las autoridades garantes del cumplimiento del Derecho se definen con más detalle en el artículo 3, punto 45, del Reglamento de Inteligencia Artificial del mismo modo que se definen las autoridades nacionales competentes en la Directiva sobre protección de datos en el ámbito penal[198]. Esta definición incluye a las autoridades garantes del cumplimiento del Derecho y a los organismos o entidades facultados (que pueden ser entidades privadas):

(a) toda autoridad pública competente para la prevención, la investigación, la detección o el enjuiciamiento de delitos o la ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas, o

Por ejemplo, estas autoridades públicas incluyen las autoridades garantes del cumplimiento del Derecho y a las autoridades de la justicia penal (como los fiscales) cuando llevan a cabo una tarea de garantía del cumplimiento del Derecho.

(b) cualquier otro organismo o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento

196 Algunas actividades de las autoridades garantes del cumplimiento del Derecho quedan excluidas del ámbito de aplicación de la Directiva sobre protección de datos en el ámbito penal, como las tareas administrativas (por ejemplo, en relación con los recursos humanos), que se realizan fuera de marco de la garantía del cumplimiento del Derecho. Entran en el ámbito de aplicación del RGPD. Véase el considerando 19 del RGPD.

197 Considerando 12 de la Directiva sobre protección de datos en el ámbito penal.

198 Artículo 3, punto 7, de la Directiva sobre protección de datos en el ámbito penal.

de delitos o ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas;

323) En virtud del Reglamento de Inteligencia Artificial, otras entidades, organismos o personas pueden ejercer actividades de garantía del cumplimiento del Derecho cuando el Derecho del Estado miembro les haya confiado el ejercicio de la autoridad pública y las competencias públicas para los fines enumerados anteriormente.

324) Por «en nombre de» se entiende que una autoridad garante del cumplimiento del Derecho ha delegado una actividad de garantía del cumplimiento del Derecho (o parte de ella) en otra entidad o persona, incluidas entidades privadas, o ha solicitado, en casos concretos, a otra entidad o persona que actúe en apoyo de las actividades de garantía del cumplimiento del Derecho. En ambos casos, las autoridades garantes del cumplimiento del Derecho deben dar instrucciones sobre todos los aspectos importantes y supervisar a la otra entidad, ya que este requisito es inherente al concepto de actuar «en nombre» de una persona.

Estos son algunos ejemplos de delegación de tareas en otros organismos:

- Las empresas de transporte público a las que las autoridades garantes del cumplimiento del Derecho solicitan que garanticen la seguridad en las redes de transporte público bajo su supervisión y siguiendo sus instrucciones.
- Las federaciones deportivas a las que las autoridades garantes del cumplimiento del Derecho solicitan que sigan sus instrucciones y actúen bajo su supervisión para garantizar la seguridad en los acontecimientos deportivos.
- Los bancos a los que las autoridades garantes del cumplimiento del Derecho solicitan que lleven a cabo determinadas acciones para «combatir determinados delitos en casos específicos» bajo su supervisión y siguiendo sus instrucciones.

Estas actividades entran en la definición de «con fines de garantía del cumplimiento del Derecho», ya que dichas entidades actúan «en nombre de» las autoridades garantes del cumplimiento del Derecho. Si dichas entidades actúan «en su propio nombre» a la hora de detectar y combatir delitos (como el fraude o el blanqueo de capitales), no se considera que están sujetas a la prohibición del artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial.

325) Las actividades de esos otros organismos o entidades entran en la definición de «garantía del cumplimiento del Derecho» únicamente si se les ha encomendado una tarea de garantía del cumplimiento del Derecho específica.

9.3. Excepciones a la prohibición

326) El Reglamento de Inteligencia Artificial establece tres excepciones a la prohibición general del uso de la identificación biométrica remota en tiempo real en espacios de

acceso público con fines de garantía del cumplimiento del Derecho. En el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial se enumeran exhaustivamente tres objetivos para los que puede autorizarse la identificación biométrica remota en tiempo real; el artículo 5, apartados 2 a 7 del Reglamento de Inteligencia Artificial, por su parte, establece las condiciones y garantías para dicha autorización. El artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial no constituye en sí mismo una base jurídica para el uso en tiempo real de sistemas de identificación biométrica remota en espacios de acceso público. Por el contrario, solo una normativa nacional de un Estado miembro que cumpla, en particular, los requisitos del artículo 5, apartados 2 a 7, del Reglamento de Inteligencia Artificial puede permitir el uso de la identificación biométrica remota en tiempo real, tal como se establece en el artículo 5, apartado 2, del Reglamento de Inteligencia Artificial. Por consiguiente, a falta de una normativa de un Estado miembro que autorice el uso de identificación biométrica remota en tiempo real para uno o varios de esos objetivos, dicho uso está prohibido a partir del 2 de febrero de 2025.

9.3.1. Justificación y objetivos

327) Los objetivos establecidos en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial tienen por objeto permitir el uso de determinadas herramientas de IA y de investigación con fines de garantía del cumplimiento del Derecho. Esos objetivos son los siguientes:

> i) la búsqueda selectiva de víctimas de tres delitos graves concretos y de personas desaparecidas [protección];
>
> ii) la prevención de amenazas inminentes para la vida o la seguridad física o de una amenaza real de atentados terroristas [prevención]; y
>
> iii) la localización o identificación de sospechosos y autores de determinados delitos graves enumerados en el anexo II [enjuiciamiento/investigación].

328) En estos escenarios, el legislador de la Unión ha equilibrado las necesidades de seguridad de la sociedad y el riesgo que los sistemas de identificación biométrica remota en tiempo real representan para los derechos fundamentales de las personas a las que se aplican dichos sistemas. De conformidad con el considerando 33 del Reglamento de Inteligencia Artificial, los objetivos para los que se permite el uso de sistemas de identificación biométrica remota en tiempo real con fines de garantía del cumplimiento del Derecho en espacios de acceso público deben definirse de manera estricta, exhaustiva y precisa; asimismo, deben usarse cuando exista una «necesidad estricta» de lograr «un interés público esencial» que «compense los riesgos» para los derechos fundamentales. Queda prohibido cualquier otro uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho que no figure en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial.

Por ejemplo, está prohibido que la policía utilice sistemas de identificación biométrica remota en tiempo real para identificar a un ladrón y comparar sus imágenes faciales con

imágenes almacenadas en bases de datos delictivos, ya que no se corresponde con ninguno de los objetivos enumerados en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial.

9.3.2. Búsqueda selectiva de las víctimas de tres delitos graves y de personas desaparecidas

329) De conformidad con el artículo 5, apartado 1, letra h), inciso i), del Reglamento de Inteligencia Artificial, se permite el uso de la identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho, siempre que dicho uso sea estrictamente necesario y se cumplan las condiciones establecidas en el artículo 5, apartados 2 a 7, del Reglamento de Inteligencia Artificial, para la búsqueda selectiva de víctimas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como para la búsqueda de personas desaparecidas.

a) Búsqueda selectiva de las víctimas de tres delitos graves

330) El escenario descrito en el artículo 5, apartado 1, letra h), inciso i), del Reglamento de Inteligencia Artificial tiene por objeto ayudar a las autoridades garantes del cumplimiento del Derecho a buscar víctimas de tres delitos graves.

331) Una búsqueda selectiva implicaría la localización e identificación de las víctimas.

Tres tipos de delitos

332) La búsqueda selectiva de víctimas concretas de tres delitos graves está contemplada en el escenario descrito en el artículo 5, apartado 1, letra h), inciso i), del Reglamento de Inteligencia Artificial: el secuestro, la trata y la explotación sexual de seres humanos[199].

Si, por ejemplo, se secuestra a un menor y existen indicios concretos de que el secuestrador pretende trasladarlo de un lugar a otro en coche, la policía puede utilizar un sistema de identificación biométrica remota en tiempo real para la búsqueda selectiva de dicho menor, pero debe definir un perímetro de despliegue y la duración de uso para identificarlo.

b) Búsqueda de personas desaparecidas

333) El primer escenario también contempla la búsqueda de una persona desaparecida[200].

334) Puede hacerse una distinción entre menores desaparecidos y adultos desaparecidos, ya que la desaparición voluntaria de un adulto desaparecido no siempre activará una

---

199 El secuestro, la trata de seres humanos y la explotación sexual son tres delitos que pueden motivar la emisión de una orden de detención europea para detener y trasladar a un sospechoso de haber cometido un delito o a un condenado al país que emitió dicha orden. Los tres delitos afectan principalmente, aunque no exclusivamente, a mujeres y niños. Según la Dirección General de Migración y Asuntos de Interior de la Comisión Europea, casi el 40 % de las víctimas son ciudadanos de la UE, y la mayoría son mujeres y niños objeto de trata con fines de explotación sexual. El número de hombres víctimas casi se ha duplicado en diez años. Los hombres son víctimas de trata con fines de trabajo y mendicidad forzosos, mientras que la mayoría de las mujeres y de los niños son objeto de trata con fines de explotación sexual. https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/together-against-trafficking-human-beings_en

200 El concepto de «persona desaparecida» no se define a escala de la UE. Sin embargo, en las Conclusiones del Consejo de diciembre de 2021 sobre la intensificación de la cooperación policial transfronteriza en el ámbito de las personas desaparecidas, el Consejo toma como referencia la definición de «persona desaparecida» tanto en la Recomendación CM/Rec (2009)12 del Consejo de Europa como en las normativas nacionales. Conclusiones del Consejo (2021) 14808/21, apartado 11, página 4.

búsqueda. Las normas aplicables relativas a la desaparición de menores varían considerablemente de un Estado miembro a otro[201]. En cualquier caso, el artículo 5, apartado 1, letra h), inciso i), del Reglamento de Inteligencia Artificial solo permite el uso de un sistema de identificación biométrica remota en tiempo real para buscar a personas desaparecidas con fines de garantía del cumplimiento del Derecho.

335) La desaparición de un adulto no siempre activa una búsqueda de la policía, ya que los adultos tienen derecho a desaparecer. Una búsqueda podría estar vinculada al estatuto jurídico de la persona («bajo curatela»), a su estado de salud (enfermedad mental), a la existencia de una nota de suicidio, pero también a una salida sin efectos personales. Si las circunstancias de la desaparición son motivo de preocupación, puede denunciarse ante la policía para que pueda iniciarse una búsqueda.

336) En algunos Estados miembros, la búsqueda de una persona desaparecida puede producirse en el marco de un procedimiento administrativo, y no con fines de garantía del cumplimiento del Derecho. Por ejemplo, cuando desaparece una persona vulnerable, pero no hay sospechas de delito ni otro fin de garantía del cumplimiento del Derecho, no se consideraría que el uso de sistemas de identificación biométrica remota en tiempo real para buscar a dicha persona se haría con fines de garantía del cumplimiento del Derecho y, por lo tanto, entraría en el ámbito de aplicación de las normas para dicho uso establecidas en el RGPD.

9.3.3. Prevención de amenazas inminentes para la vida o de atentados terroristas

337) En el artículo 5, apartado 1, letra h), inciso ii), del Reglamento de Inteligencia Artificial se incluye el segundo supuesto en el que se permite el uso de la identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho, siempre que dicho uso sea estrictamente necesario y se cumplan las condiciones establecidas en el artículo 5, apartados 2 a 7 del Reglamento de Inteligencia Artificial.

> *la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de una amenaza real y actual o real y previsible de un atentado terrorista.*

a) Amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas

338) En aplicación del artículo 2 de la Carta, que garantiza el derecho a la vida, la Unión y sus Estados miembros deben salvaguardar y, por tanto, proteger la vida de las personas. Los criterios del artículo 5, apartado 1, letra h), inciso ii), del Reglamento de Inteligencia Artificial relativos a la amenaza para la vida, que deben cumplirse para para permitir el uso de sistemas identificación biométrica remota en tiempo real en espacios de acceso público, exigen la existencia de una amenaza 1) específica, 2)

[201] Comisión Europea, Red Europea de Migración, «How do EU Member States treatment cases of missing non-accompanied minor?» [«¿Cómo tratan los Estados miembros de la UE los casos de menores no acompañados desaparecidos?», documento no disponible en español], Informe de la Red Europea de Migración, 2020.

importante y 3) inminente para la vida o la seguridad física de 4) personas físicas. No es necesario que la amenaza se limite a personas identificadas o a un colectivo, ya que se refiere a personas físicas en general.

339) El considerando 33 del Reglamento de Inteligencia Artificial aclara que una amenaza inminente para la vida o la seguridad física de las personas físicas puede también abarcar la amenaza inminente para una infraestructura crítica[202] «cuando la perturbación o destrucción de dichas infraestructuras críticas suponga una amenaza inminente para la vida o la seguridad física de una persona, también al perjudicar gravemente el suministro de productos básicos a la población o el ejercicio de la función esencial del Estado».

> Por ejemplo[203],
>
> Una perturbación grave y destrucción de infraestructuras críticas (por ejemplo, una central eléctrica, un sistema de suministro de agua o un hospital) pueden suponer una amenaza inminente para la vida o la seguridad física de una persona cuando existe un perjuicio grave derivado de la interrupción del suministro de productos básicos a la población (privación de electricidad o de agua potable durante un largo período de tiempo, en condiciones meteorológicas especialmente cálidas o frías, etc.).

340) Lo que constituye una amenaza inminente para la vida o la seguridad física de las personas físicas se define y se evalúa en última instancia a nivel del Estado miembro sobre la base de su legislación nacional, de conformidad con el Derecho de la Unión, en particular teniendo en cuenta los elementos clave y la justificación del artículo 5 del Reglamento de Inteligencia Artificial. Esto tendrá que establecerse o mencionarse en las normas que los Estados miembros deben adoptar para hacer uso de las excepciones a la prohibición de utilizar la identificación biométrica remota en tiempo real con fines de garantía del cumplimiento del Derecho en espacios de acceso público.

341) Una amenaza **inminente** para la vida o la seguridad física es una amenaza que puede producirse en cualquier momento y obliga a «**actuar sin demora**»[204]. Una amenaza **importante** para la seguridad física se refiere a lesiones corporales graves.

342) Una amenaza es específica si está claramente definida e individualizada y es concreta, en el sentido de que no debe ser hipotética ni estar relacionada con determinados peligros en general.

> Por ejemplo, se informa a la policía de que un antiguo alumno planea un ataque mortal en su antigua universidad para vengarse de varios antiguos compañeros. La policía recibe información sobre la inminencia del ataque, el centro objetivo y las armas que tiene previsto utilizar para ejecutar sus planes.

---

202 Según la definición del artículo 2, punto 4, de la Directiva (UE) 2022/2557.
203 Considerando 33 del Reglamento de Inteligencia Artificial.
204 Considerando 37 del Reglamento (UE) 2023/1543.

343) No es necesario que una amenaza específica sea intencionada. Las acciones no intencionadas también pueden suponer una amenaza para la vida o la seguridad física.

b) Amenaza real y actual o real y previsible de un atentado terrorista

344) Esta parte del segundo escenario descrito en el artículo 5, apartado 1, letra h), inciso ii), del Reglamento de Inteligencia Artificial consta de varios elementos: la existencia de una amenaza de atentado terrorista y las características de dicha amenaza, que deben ser reales y actuales o reales y previsibles.

Amenaza de un atentado terrorista

345) La evaluación de la existencia y la gravedad de la amenaza se hace a escala nacional, al valorar las circunstancias reales de una medida que debe adoptarse para salvaguardar la seguridad nacional y, más concretamente, en caso de atentado terrorista. El **nivel de amenaza terrorista se define a escala nacional** y varía de un Estado miembro a otro. Por ejemplo, los Países Bajos han establecido cinco niveles de amenazas;[205] Bélgica, cuatro;[206] Francia, tres; [207] y Suecia, cinco[208]. Sin embargo, el concepto de «amenaza real y actual o real y previsible», utilizado en el artículo 5, apartado 1, letra h), inciso ii), es un concepto autónomo del Derecho de la Unión y, por tanto, debe evaluarse, en principio, con independencia de las definiciones nacionales. La amenaza no se refiere al terrorismo en general, sino específicamente a una amenaza de atentado terrorista.

Características de la amenaza: real y actual o real y previsible

346) El umbral de gravedad que debe alcanzar una amenaza para permitir el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho se inspiró en la jurisprudencia del TJUE sobre las medidas de conservación de datos y registro de nombres de los pasajeros destinadas a velar por la seguridad nacional, en particular, contra los atentados terroristas. Según el TJUE, en estos contextos, «una amenaza para la seguridad nacional debe ser real y actual, o cuando menos previsible, lo que supone que surjan circunstancias suficientemente concretas»[209].

Prevención

347) Contrariamente a lo dispuesto en el artículo 5, apartado 1, letra h), inciso i), y en el artículo 5, apartado 1, letra h), inciso iii), del Reglamento de Inteligencia Artificial, en el escenario descrito en el artículo 5, apartado 1, letra h), inciso ii), no se especifica que el uso de identificación biométrica remota en tiempo real esté permitido para localizar o identificar a una persona concreta. Su objetivo es prevenir una amenaza particular. En consecuencia, el escenario también puede contemplar el uso de identificación biométrica remota en tiempo real para detectar y seguir a «terroristas en movimiento», es decir, varias personas vinculadas a la misma amenaza, si existen indicios concretos

205 https://www.government.nl/topics/counterterrorism-and-national-security/risk-of-an-attack-threat-level

206 https://cuta.belgium.be; https://crisiscenter.be/en/risks-belgium/security-risks/terrorism-and-extremism

207 https://www.sgdsn.gouv.fr/vigipirate#; https://www.sgdsn.gouv.fr/files/files/Vigipirate/20160130-np-sgdsn-pse-tackling-terrorism-together.pdf

208 https://www.krisinformation.se/en/hazards-and-risks/terrorism

209 Sentencia del Tribunal de Justicia de 20 de septiembre de 2022, SpaceNet, C-793/19 (asuntos acumulados C-793/19, C-794/19), ECLI:EU:C:2022:702, apartado 93.

de que dichas personas tienen previsto cometer un ataque terrorista, pero no está claro dónde.

Identificación biométrica remota en tiempo real para prevenir un atentado terrorista en un parque

Se informa a la policía de que una persona está corriendo en un parque, buscando a personas a las que atacar con un cuchillo mientras grita consignas extremistas violentas que suelen estar vinculadas a atentados terroristas y a organizaciones terroristas. Si el Estado miembro ha autorizado el uso de la identificación biométrica remota en tiempo real en el escenario descrito en el artículo 5, apartado 1, letra h), inciso ii), del Reglamento de Inteligencia Artificial, las autoridades garantes del cumplimiento del Derecho pueden utilizar la identificación biométrica remota en tiempo real para identificar y localizar a la persona en el parque y en sus inmediaciones para prevenir el ataque, siempre que se cumplan las demás condiciones del artículo 5, apartados 2 a 7, del Reglamento de Inteligencia Artificial.

9.3.4. Localización e identificación de sospechosos de determinados delitos

348) El artículo 5, apartado 1, letra h), inciso iii), del Reglamento de Inteligencia Artificial permite la «localización o identificación de una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación o un enjuiciamiento penales o de ejecutar una sanción penal por alguno de los delitos mencionados en el anexo II que en el Estado miembro de que se trate se castigue con una pena o una medida de seguridad privativas de libertad cuya duración máxima sea de al menos cuatro años».

El anexo II del Reglamento de Inteligencia Artificial contiene una lista exhaustiva de delitos graves para los que puede autorizarse el uso de la identificación biométrica remota en tiempo real para el objetivo mencionado. Dichos delitos son:

- terrorismo,
- trata de seres humanos,
- explotación sexual de menores y pornografía infantil,
- tráfico ilícito de estupefacientes o sustancias psicotrópicas,
- tráfico ilícito de armas, municiones y explosivos,
- homicidio voluntario, agresión con lesiones graves,
- tráfico ilícito de órganos o tejidos humanos,
- tráfico ilícito de materiales nucleares o radiactivos,
- secuestro, detención ilegal o toma de rehenes,
- delitos que son competencia de la Corte Penal Internacional,
- secuestro de aeronaves o buques,
- violación,

- delitos contra el medio ambiente,
- robo organizado o a mano armada,
- sabotaje,
- participación en una organización delictiva implicada en uno o varios de los delitos enumerados en esta lista.

a) Localización e identificación

349) Un Estado miembro puede permitir el uso de la identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho para localizar e identificar a una persona sospechosa de haber cometido un delito a fin de llevar a cabo una investigación penal, enjuiciar a dicha persona por el delito cometido o ejecutar una pena existente.

b) Sospechosos y autores de un delito

350) El artículo 5, apartado 1, letra h), inciso iii), del Reglamento de Inteligencia Artificial se refiere a dos categorías de personas: sospechosos y autores de un delito. Un sospechoso es una persona con respecto a la cual existen motivos fundados para creer que ha cometido un delito y ya se han reunido pruebas suficientes de su participación en este. Un autor de un delito es una persona acusada de haber cometido un delito o condenada por ello. Se aplican las mismas condiciones (el delito debe figurar en el anexo II y la pena máxima debe ser de al menos cuatro años) a la localización o identificación del cómplice de los delitos enumerados en el anexo II del Reglamento de Inteligencia Artificial.

c) Lista de delitos graves

351) Solo los delitos graves justifican el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho.

352) Los cinco primeros delitos enumerados en el anexo II del Reglamento de Inteligencia Artificial son los mismos que los «eurodelitos» enumerados en el artículo 83 del TFUE, mientras que los demás constituyen prioridades para la cooperación en materia de la garantía del cumplimiento del Derecho[210]. Algunos de ellos (por ejemplo, el secuestro o el tráfico ilícito de materiales nucleares o radiactivos) pueden estar relacionados con el terrorismo[211].

353) Aunque todos los delitos enumerados en el anexo II pueden motivar la emisión de una orden de detención europea contra un sospechoso o un autor de un delito, no es necesario que se haya emitido una para usar la identificación biométrica remota en tiempo real a fin de localizar e identificar a un sospechoso por uno de estos delitos graves.

[210] Prioridades de Europol.
[211] Véase el considerando 33 y la definición de «delitos de terrorismo» en el artículo 3 de la Directiva 2017/541.

354) Además, para utilizar la identificación biométrica remota en tiempo real a estos efectos, el delito correspondiente debe castigarse, en el Estado miembro de que se trate, con una pena de privación de libertad o una medida de seguridad privativa de libertad de una duración máxima de, al menos, cuatro años.

En un concurrido festival en una ciudad, las autoridades policiales despliegan tecnologías de reconocimiento facial en directo para supervisar los alrededores del festival e identificar a personas buscadas con órdenes de detención pendientes por tráfico ilícito de drogas y delitos sexuales. En diferentes entradas del festival, la policía utiliza imágenes de vídeo en directo de personas que pasan delante de una cámara móvil para comparar sus caras con una lista de vigilancia de caras de individuos sobre los que pese una orden de búsqueda.

En primer lugar, por lo que respecta a los tipos de delito, la identificación biométrica remota puede utilizarse en caso de tráfico ilícito de drogas. Sin embargo, los delitos sexuales no figuran en la lista de delitos, a menos que estén relacionados con la explotación sexual de menores, el material de abuso sexual de menores o la violación. La policía no está autorizada a desplegar tecnologías de reconocimiento facial en tiempo real de manera amplia y sin un objetivo concreto, es decir, con la esperanza de encontrar delincuentes buscados y retirarlos de las calles.

No sucede lo mismo si la policía ha recibido una descripción física acompañada de una fotografía de una persona buscada que es objeto de una orden de detención europea por tráfico de drogas y tiene motivos para creer que estará presente en el festival. En tales circunstancias, el uso de tecnologías de reconocimiento facial en tiempo real para identificar a una persona que constituya el objetivo puede quedar cubierto por el artículo 5, apartado 1, letra h), inciso iii), del Reglamento de Inteligencia Artificial.

Tras un grave atentado terrorista en un mercado navideño, que se cobró la vida de doce personas, la policía utiliza tecnologías de reconocimiento facial en tiempo real para identificar al autor y saber a dónde huye. En este contexto, utilizan también las tecnologías de reconocimiento facial en tiempo real de la estación de tren cercana y de las estaciones de destino de los trenes que salieron de allí poco después del atentado. En caso de atentado terrorista, el artículo 5, apartado 1, letra h), inciso iii), del Reglamento de Inteligencia Artificial permite dicho uso.

355) Puede establecerse un vínculo entre el artículo 5, apartado 1, letra h), inciso i), y el artículo 5, apartado 1, letra h), inciso iii), del Reglamento de Inteligencia Artificial para los delitos contemplados en el escenario descrito en el artículo 5, apartado 1, letra h), inciso i), del Reglamento de Inteligencia Artificial. Si bien los sistemas de identificación biométrica remota en tiempo real pueden desplegarse para encontrar a una víctima o a una persona desaparecida, también pueden utilizarse para localizar e identificar al autor o al sospechoso de un delito de trata de seres humanos, de explotación sexual en la medida en que afecte a menores [tal como figura en el anexo II

del Reglamento de Inteligencia Artificial)] y secuestro [incluye la figura del artículo 5, apartado 1, letra h), inciso i), del Reglamento de Inteligencia Artificial y la figura mencionada en su anexo II]. También puede establecerse un vínculo entre el artículo 5, apartado 1, letra h), inciso ii) y el artículo 5, apartado 1, letra h), inciso iii), del Reglamento de Inteligencia Artificial: los sistemas de identificación biométrica remota en tiempo real pueden utilizarse para prevenir una amenaza que entre en el ámbito de aplicación del artículo 5, apartado 1, letra h), inciso ii), y, si dicha amenaza se materializa, para identificar o localizar al autor «en movimiento».

10. GARANTÍAS Y CONDICIONES APLICABLES A LAS EXCEPCIONES (ARTÍCULO 5, APARTADOS 2 A 7, DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL)

10.1. Persona que constituya el objetivo y garantías (artículo 5, apartado 2, del Reglamento de Inteligencia Artificial)

Según el artículo 5, apartado 2, del Reglamento de Inteligencia Artificial:

«El uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), debe desplegarse para los fines establecidos en dicha letra, únicamente para confirmar la identidad de la persona que constituya el objetivo específico y tendrá en cuenta los siguientes aspectos:

(a) la naturaleza de la situación que dé lugar al posible uso, y en particular la gravedad, probabilidad y magnitud del perjuicio que se produciría de no utilizarse el sistema;

(b) las consecuencias que tendría el uso del sistema en los derechos y las libertades de las personas implicadas, y en particular la gravedad, probabilidad y magnitud de dichas consecuencias.

Además, el uso de sistemas de identificación biométrica remota "en tiempo real" en espacios de acceso público con fines de garantía del cumplimiento del Derecho para cualquiera de los objetivos mencionados en el apartado 1, párrafo primero, letra h), del presente artículo deberá cumplir garantías y condiciones necesarias y proporcionadas en relación con el uso de conformidad con el Derecho nacional que autorice dicho uso, en particular en lo que respecta a las limitaciones temporales, geográficas y personales. El uso del sistema de identificación biométrica remota "en tiempo real" en espacios de acceso público solo se autorizará si la autoridad garante del cumplimiento del Derecho ha completado una evaluación de impacto relativa a los derechos fundamentales según lo dispuesto en el artículo 27 y ha registrado el sistema en la base de datos de la UE de conformidad con el artículo 49. No obstante, en casos de urgencia debidamente justificados, se podrá empezar a utilizar tales sistemas sin el registro en la base de datos de la UE, siempre que dicho registro se complete sin demora indebida.».

356) El uso de sistemas de identificación biométrica remota en tiempo real para uno de los objetivos enumerados en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial está sujeto a determinadas garantías y condiciones, que se detallan en el artículo 5, apartados 2 a 7, de dicho Reglamento.

357) En primer lugar, el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho solo puede «confirmar la identidad de la persona que constituya el objetivo específico». Esta primera condición tiene por objeto equilibrar, por una parte, la gravedad de la situación y el perjuicio que resultaría de no utilizar el sistema y, por otra parte, el impacto de la tecnología en los derechos y libertades de las personas. Su objetivo es evitar la vigilancia masiva centrarse en una persona para el uso de la identificación biométrica remota en tiempo real. En consecuencia, el despliegue de un sistema de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho solo debe autorizarse para las personas que constituyan el objetivo.

358) El uso de la expresión «confirmar la identidad», en lugar de «identificar», se concibe como una garantía adicional para los derechos fundamentales que limita el riesgo de vigilancia indiscriminada e implica que la identificación de una persona en el sentido del artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial debe ser específica. Esta expresión debe entenderse en el sentido de que la identificación biométrica remota en tiempo real solo puede utilizarse para buscar a personas específicas respecto de las cuales las autoridades garantes del cumplimiento del Derecho tengan motivos para creer que son víctimas (o hayan sido informadas de ello) de los delitos enumerados en el artículo 5, apartado 1, letra h), inciso i), del Reglamento de Inteligencia Artificial o que participan en uno de los escenarios descritos en el artículo 5, apartado 1, letra h), inciso ii), o en el artículo 5, apartado 1, letra h), inciso iii), de dicho Reglamento. En la práctica, esto supone comparar los datos recogidos en tiempo real con los datos almacenados en la base de datos de referencia. Por lo que se refiere al uso del sistema de identificación biométrica remota en tiempo real en los escenarios descritos en el artículo 5, apartado 1, letra h), inciso ii), del Reglamento de Inteligencia Artificial y para llevar a cabo una investigación penal en el sentido de su artículo 5, apartado 1, letra h), inciso iii), no es necesario que las autoridades garantes del cumplimiento del Derecho conozcan la identidad de las personas que buscan antes de utilizar el sistema. Si disponen de indicios concretos e información sobre un atentado planeado por una organización terrorista (sin saber quién ejecutará el plan) en un momento y lugar determinados, el sistema de identificación biométrica remota puede utilizarse para identificar al autor del delito dentro del grupo terrorista, siempre que las autoridades garantes del cumplimiento del Derecho hayan creado una base de datos de referencia que contenga los datos biométricos de las personas que forman parte de dicho grupo. En los tres escenarios descritos en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial, «confirmar la identidad» también puede referirse a la localización de la persona en cuestión.

359) En segundo lugar, antes de utilizar el sistema, debe evaluarse la naturaleza de la situación que puede dar lugar al posible uso, en particular, la gravedad, la probabilidad y la magnitud del perjuicio que sufrirían las personas físicas, la sociedad y los fines de garantía del cumplimiento del Derecho si no se utilizara el sistema, teniendo en cuenta las consecuencias de la utilización del sistema para los derechos y libertades de las personas afectadas, especialmente la gravedad, la probabilidad y la magnitud de dichas consecuencias. En particular, debe evaluarse si las autoridades garantes del cumplimiento del Derecho o las entidades que actúan en su nombre disponen de soluciones alternativas menos intrusivas.

Por ejemplo, se prohíbe que las autoridades garantes del cumplimiento del Derecho utilicen sistemas de reconocimiento facial en tiempo real en la calle basándose en preocupaciones generales de seguridad, prevención de la delincuencia y hacinamiento: ello implicaría un seguimiento y una vigilancia constantes de todas las personas, no está limitado en el tiempo y, por tanto, no cumpliría los criterios para acogerse a la excepción de la prohibición establecida en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial.

360) El criterio de «**gravedad**», aplicado aquí en relación con los posibles perjuicios y consecuencias, implica una gradación de la injerencia en los derechos fundamentales en juego, que está vinculada al principio de proporcionalidad[212]. Algunas injerencias en los derechos fundamentales se consideran más graves que otras.

361) El criterio de «**magnitud**» se refiere, en particular, al número y a las categorías de personas afectadas por la injerencia, incluidos los menores y las personas vulnerables o marginadas.

362) Por último, con «**probabilidad**» se hace referencia a la probabilidad de que se produzca un suceso.

363) La evaluación de la gravedad, magnitud y probabilidad del perjuicio, así como de las consecuencias, debe formar parte de la evaluación de impacto relativa a los derechos fundamentales que la autoridad garante del cumplimiento del Derecho está obligada a llevar a cabo (véase más adelante). Cada evaluación se realizará caso por caso.

364) En tercer lugar, el uso en tiempo real de la identificación biométrica remota debe estar claramente limitado en términos de alcance geográfico, duración y persona que constituya el objetivo específico. Con ello se pretende garantizar que el sistema de identificación biométrica remota solo se utiliza cuando es estrictamente necesario.

365) En cuanto a la **restricción geográfica**, puede cubrir una o varias zonas geográficas sobre la base de «hechos objetivos y no discriminatorios». En el caso de la identificación biométrica, esto significa que la restricción geográfica se aplica a un perímetro claramente delimitado respecto del cual existen motivos para creer que se

[212] Sentencia del Tribunal de Justicia de 2 de octubre de 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, apartado 55, en la que el Tribunal afirma que el «acceso debe guardar relación con la gravedad de la injerencia en los derechos fundamentales en cuestión».

producirá el suceso. En circunstancias normales, esta delimitación no debe cubrir toda una ciudad o país; debe ser más específica.

366) Otra garantía está relacionada con el **ámbito personal** de la medida, es decir, la definición de las **categorías de personas afectadas**. Esto excluiría la identificación no selectiva e indiscriminada de personas, en ausencia de otros indicios de que se ha producido un incidente.

367) Por último, la **limitación temporal** es un período limitado a lo estrictamente necesario, pero que puede prorrogarse en caso de necesidad de conformidad con las normas aplicables. Por lo tanto, el uso de sistemas de identificación biométrica remota en tiempo real no puede tener una duración indefinida o vaga. El período debe determinarse en función de los indicios concretos que motiven el uso de sistemas de identificación biométrica remota.

368) En cuarto lugar, antes de su despliegue, las autoridades garantes del cumplimiento del Derecho que desplieguen el sistema de identificación biométrica remota en tiempo real deben haber llevado a cabo una evaluación de impacto relativa a los derechos fundamentales y haber registrado el sistema en la base de datos de la UE (excepto en un caso debidamente justificado).

10.1.1. Evaluación de impacto relativa a los derechos fundamentales

369) Las evaluaciones de impacto relativas a los derechos fundamentales llevadas a cabo de conformidad con el artículo 5, apartado 2, del Reglamento de Inteligencia Artificial deben cumplir las condiciones establecidas en su artículo 27. Esta disposición establece los requisitos relativos a las evaluaciones de impacto relativas a los derechos fundamentales aplicables a los sistemas de IA de alto riesgo.

370) En el período comprendido entre el momento en que las prohibiciones establecidas en el artículo 5 del Reglamento de Inteligencia Artificial son aplicables (tras el 2 de febrero de 2025), pero las disposiciones relativas a los sistemas de IA de alto riesgo aún no lo son (antes del 2 de agosto de 2026), los responsables del despliegue de sistemas de identificación biométrica remota en tiempo real que cumplan las condiciones para acogerse a una o varias de las excepciones del artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial deben aplicar los requisitos para la evaluación de impacto relativa a los derechos fundamentales establecidos en su artículo 27. Las siguientes orientaciones provisionales se refieren únicamente al uso de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho antes de que sean aplicables las obligaciones relativas a los sistemas de IA de alto riesgo y de que la Comisión adopte el modelo de evaluación de impacto relativa a los derechos fundamentales y proporcione orientaciones adicionales sobre la obligación contemplada en el artículo 27 del Reglamento de Inteligencia Artificial.

371) Una evaluación de impacto relativa a los derechos fundamentales es un nuevo tipo de evaluación de impacto que tiene por objeto determinar el impacto que determinados sistemas de IA de alto riesgo, en particular los sistemas de identificación biométrica

remota, pueden ejercer en los derechos fundamentales. Se trata de una herramienta de rendición de cuentas. Esta evaluación no sustituye a la actual evaluación de impacto relativa a la protección de datos que los responsables del tratamiento (es decir, los responsables del tratamiento de datos personales) deben llevar a cabo en virtud del artículo 27 de la Directiva sobre protección de datos en el ámbito penal, del artículo 35 del RGPD o del artículo 39 del RPDUE.

Por ejemplo, debe realizarse una evaluación de impacto relativa a la protección de datos cuando se traten datos biométricos mediante nuevas tecnologías que puedan acarrear un alto riesgo para los derechos y libertades de las personas físicas (como los circuitos cerrados de televisión, el reconocimiento facial de IA y las cámaras corporales) en espacios de acceso público.

372) Mientras que una evaluación de impacto relativa a la protección de datos se centra en los riesgos para los derechos y libertades de las personas que se derivan del tratamiento de sus datos personales, una evaluación de impacto relativa a los derechos fundamentales aborda, de manera más general, el posible impacto de los sistemas de IA en los derechos fundamentales de las personas. Así pues, el ámbito de aplicación de una evaluación de impacto relativa a los derechos fundamentales es más amplio en términos de actividades contempladas y derechos fundamentales evaluados. Cuando el sistema de IA trate datos personales (como es el caso de los sistemas de identificación biométrica remota), la evaluación de impacto relativa a los derechos fundamentales debe complementar la evaluación de impacto relativa a la protección de datos llevada a cabo por el responsable del despliegue como responsable del tratamiento de los datos[213], sin incluir aspectos ya tratados en esta última evaluación y evitando solapamientos. El análisis de la evaluación de impacto relativa a los derechos fundamentales en las presentes directrices se limita al uso autorizado de la identificación biométrica remota en tiempo real y tiene por objeto servir de orientación preliminar para los responsables del despliegue en este período temporal antes de que la Oficina de IA facilite un modelo[214].

373) La obligación de llevar a cabo la evaluación de impacto relativa a los derechos fundamentales de conformidad con el artículo 5, apartado 2, del Reglamento de Inteligencia Artificial se impone a los responsables del despliegue del sistema de identificación biométrica remota, y no a las entidades u organismos o a cualquier otra persona que actúe en su nombre. Si otros agentes actúan en nombre del responsable del despliegue o de la autoridad garante del cumplimiento del Derecho, deben colaborar en la preparación de la evaluación de impacto relativa a los derechos fundamentales aportando toda la información pertinente para garantizar que se lleva a cabo correctamente.

374) Esta evaluación debe realizarse antes del despliegue del sistema de identificación biométrica remota en tiempo real autorizado.

213 Artículo 27, punto 4, del Reglamento de Inteligencia Artificial.

214 Por consiguiente, el análisis no contempla el caso de los sistemas de IA de alto riesgo en general.

375) De conformidad con el artículo 27 del Reglamento de Inteligencia Artificial, una evaluación de impacto relativa a los derechos fundamentales debe incluir la siguiente información:

- Una descripción del uso de la identificación biométrica remota y de los procesos del responsable del despliegue para su uso, junto con la finalidad prevista de dicho uso.

En esta descripción, es conveniente precisar:

- el nombre del responsable del despliegue;

- los fines de garantía del cumplimiento del Derecho para los que se utilizará el sistema de identificación biométrica remota en tiempo real;

- la descripción de la base de datos de referencia con la que se comparará la identificación biométrica, en particular las fuentes de los datos biométricos (imágenes faciales, muestras de voz, etc.) que se utilizarán;

- la descripción de la tecnología subyacente al sistema para explicar su funcionamiento, indicando a la documentación disponible facilitada por el proveedor y el nombre de este[215];

- la base jurídica sobre la que se desplegará la identificación biométrica remota en tiempo real.

- El período y la frecuencia de uso.

De conformidad con el artículo 5, apartado 3, del Reglamento de Inteligencia Artificial, una autoridad judicial u otra autoridad independiente debe autorizar cada uso de un sistema de identificación biométrica remota en tiempo real para una de las excepciones permitidas antes de su despliegue. En cambio, en el caso de la evaluación de impacto relativa a los derechos fundamentales, los responsables del despliegue deben proporcionar una indicación general del período de uso y de la frecuencia previstos.

- Las categorías de personas y colectivos afectados por el sistema.

A efectos de la excepción contemplada en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial, la evaluación de impacto relativa a los derechos fundamentales debe distinguir entre:

- la persona que constituya el objetivo, que puede ser víctima, autora o sospechosa de un delito;

- las personas cuyos datos biométricos figuren en la base de datos de referencia, y

- las categorías de personas presentes en las zonas colindantes a aquella en la que se desplegará el sistema de identificación biométrica remota.

[215] Cuando entren en vigor las normas sobre sistemas de IA de alto riesgo, esto podrá hacerse indicando el número de registro del sistema en la base de datos de la UE y la información disponible para el sistema que figura en ella.

El uso de sistemas de identificación biométrica remota en tiempo real no solo afectará a los derechos fundamentales de la persona que constituya el objetivo: también se verán afectados los derechos de otras personas cuyos datos biométricos se utilicen con fines de comparación, de los transeúntes y de las personas que se encuentren por casualidad en la zona de búsqueda. La descripción del alcance geográfico de la zona o las zonas de búsqueda cubiertas por el sistema de identificación biométrica remota en tiempo real repercutirá en el número de personas afectadas por el sistema.

- Los riesgos específicos de perjuicio para las personas afectadas.

376) Entre los derechos fundamentales que pueden verse afectados por el uso de la identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho pueden contarse, en particular:

- el derecho a la vida privada y familiar, en particular la expectativa razonable de anonimato de las personas en los espacios públicos;
- el derecho a la protección de datos, ya que los sistemas de identificación biométrica remota se basan en el tratamiento de datos biométricos y otros datos personales (por ejemplo, nombres, números de identificación y datos sensibles, como el origen étnico) para identificar a personas concretas;
- la libertad de pensamiento, conciencia y religión, la libertad de expresión y la libertad de reunión y asociación en los espacios públicos donde se realizan las búsquedas, en los que el uso de los sistemas de identificación biométrica remota podría tener un efecto disuasorio, impidiendo a las personas ejercer plenamente sus derechos y libertades, ya que, si saben que están siendo vigiladas, podrían cambiar su comportamiento o incluso impedirles comportarse de una determinada manera;
- el derecho a la tutela judicial efectiva y a un juez imparcial;
- el derecho a la no discriminación si el sistema incorpora sesgos (de género, étnicos o raciales) y conduce a un error en la identificación de un sospechoso o autor de un delito;
- el derecho a la dignidad humana, debido al sentimiento de verse reducido a un objeto del sistema;
- la presunción de inocencia y los derechos de la defensa, dado que no puede adoptarse ninguna decisión que perjudique a una persona únicamente sobre la base de los resultados de salida del sistema de identificación biométrica remota en tiempo real;
- los derechos del niño, en caso de que la víctima, la persona desaparecida o el sospechoso sea un menor;
- los derechos de las personas mayores en el caso de una persona desaparecida.

Para evaluar los riesgos específicos de perjuicio que puedan afectar a las personas o colectivos afectados identificados, la evaluación de impacto relativa a los derechos fundamentales debe determinar los derechos fundamentales de dichas personas y

evaluar el impacto en sus derechos fundamentales, en particular su gravedad y magnitud, teniendo en cuenta a las personas potencialmente afectadas.

Esta parte de la evaluación de impacto relativa a los derechos fundamentales también debe incluir la evaluación de necesidad y la proporcionalidad del uso de un sistema de identificación biométrica remota en tiempo real, atendiendo a los objetivos y las circunstancias en que se pretende utilizar, en particular la existencia o ausencia de alternativas menos intrusivas. La evaluación de impacto relativa a los derechos fundamentales debe describir el rendimiento y el nivel de precisión del sistema, basándose en la documentación técnica y, si se dispone de ellos, en los datos de entrenamiento con los que se probó y desarrolló la tecnología para evitar sesgos y discriminación.

También debe determinar el impacto del uso de un sistema de identificación biométrica remota en tiempo real en los derechos fundamentales de todas las personas potencialmente afectadas, en particular del sospechoso o el autor del delito, la víctima buscada y otras personas presentes en los espacios de acceso público donde se llevan a cabo las búsquedas. En la medida en que el sistema trata los datos biométricos de estas personas, esto afectará a sus derechos a la vida privada y familiar y a la protección de datos, que se examinarán en el marco de la evaluación de impacto relativa a la protección de datos en relación con las actividades de tratamiento de datos. Para otras actividades relacionadas con el uso de los sistemas de identificación biométrica remota en tiempo real y la repercusión en otros derechos fundamentales, la evaluación de impacto relativa a los derechos fundamentales complementará a la evaluación de impacto relativa a la protección de datos. En función del contexto del despliegue, pueden verse perjudicados otros derechos fundamentales de estas personas, como sus derechos a la dignidad humana; a la libertad de pensamiento, conciencia y religión; a la libertad de reunión o de expresión; a la tutela judicial efectiva y a un juez imparcial; a la presunción de inocencia y a los derechos de la defensa, y a los derechos del niño.

El análisis en el marco de la evaluación de impacto relativa a los derechos fundamentales debe llevarse a cabo en un sentido abstracto, antes de la primera puesta en servicio del sistema de IA. En cada caso de uso de un sistema de identificación biométrica remota en tiempo real, deben concretarse más las consideraciones específicas dependientes del contexto que determinan el impacto de dicho uso en cada solicitud de autorización de uso del sistema de identificación biométrica remota dirigida a una autoridad judicial u otra autoridad administrativa independiente (véase la sección10.23.8.3).

- Medidas de supervisión humana

De conformidad con el artículo 5, apartado 3, del Reglamento de Inteligencia Artificial, no se adoptará ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota en tiempo real. Por consiguiente, en la evaluación de impacto relativa a los derechos fundamentales se deben describir los procedimientos

que se seguirán durante el funcionamiento del sistema y la manera en que se interpretarán los resultados de salida en el contexto del proceso de toma de decisiones. Los procedimientos deben proporcionar instrucciones sobre el despliegue del sistema de identificación biométrica remota, aclarar el papel de un agente humano en la verificación e interpretación de los resultados de salida e impartir formación sobre el funcionamiento del sistema. La persona encargada de la supervisión humana debe tener un nivel suficiente de «alfabetización, formación y autoridad en materia de IA»[216] para entender cómo funciona el sistema y saber cuándo tiene un bajo rendimiento o un mal funcionamiento.

En los artículos 14 y 26 del Reglamento de Inteligencia Artificial se mencionan otras consideraciones pertinentes para la supervisión humana y vigilancia, que deben describirse.

- Medidas de reducción de riesgos

Además de aplicar medidas de supervisión humana (también para evitar medidas discriminatorias), el responsable del despliegue debe explicar las medidas de recurso en caso de que se materialice un riesgo, en particular los procedimientos de gobernanza y los mecanismos de reclamación, como en el caso de una identificación errónea.

10.1.2. Registro de los sistemas de identificación biométrica remota autorizados

377) El artículo 5, apartado 2, del Reglamento de Inteligencia Artificial también obliga al responsable del despliegue de un sistema de identificación biométrica remota en tiempo real utilizado en espacios de acceso público con fines de garantía del cumplimiento del Derecho a registrar el sistema en la base de datos de la UE establecida en el artículo 49 de dicho Reglamento. Sin embargo, en casos de emergencia debidamente justificados (como una amenaza inminente), el despliegue puede comenzar incluso antes del registro, siempre que las autoridades garantes del cumplimiento del Derecho registren el sistema sin demora indebida. Por «sin demora indebida» debe entenderse «tan pronto como sea posible», teniendo en cuenta las circunstancias de la emergencia que impidieron el registro del sistema antes de su utilización. Para determinar si el registro cumple este criterio, se necesita una apreciación caso por caso. No puede definirse *a priori* con un plazo preciso. El retraso no debe estar motivado por una acción deliberada. De conformidad con el artículo 49, apartado 4, del Reglamento de Inteligencia Artificial, los sistemas de identificación biométrica remota utilizados con fines de garantía del cumplimiento del Derecho deben registrarse en una sección segura y no pública de la base de datos, limitarse la información y restringir el acceso a dicha información.

Por ejemplo, si el sistema se desplegó en una situación de amenaza inminente para la vida, como en el escenario de un tiroteo, y se solicita a las autoridades garantes del cumplimiento del Derecho que registren el sistema de identificación biométrica

[216] Considerando 91 del Reglamento de Inteligencia Artificial.

remota en las veinticuatro horas siguientes a su utilización, puede considerarse que se trata de un plazo razonable.

10.2. Necesidad de autorización previa

378) El artículo 5, apartado 3, del Reglamento de Inteligencia Artificial exige que cada uso de un sistema de identificación biométrica remota en tiempo real esté sujeto a una **autorización previa** y prohíbe las decisiones automatizadas tomadas **exclusivamente sobre la base de los resultados de salida de dicho sistema** y que produzcan efectos jurídicos adversos.

Según el artículo 5, apartado 3, del Reglamento de Inteligencia Artificial:

A los efectos del apartado 1, párrafo primero, letra h), y el apartado 2, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho estará supeditado a la concesión de una autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante del Estado miembro en el que vaya a utilizarse dicho sistema, que se expedirá previa solicitud motivada y de conformidad con las normas detalladas del Derecho nacional mencionadas en el apartado 5. No obstante, en una situación de urgencia debidamente justificada, se podrá empezar a utilizar tal sistema sin autorización siempre que se solicite dicha autorización sin demora indebida, a más tardar en un plazo de veinticuatro horas. Si se rechaza dicha autorización, el uso se interrumpirá con efecto inmediato y todos los datos, así como los resultados y la información de salida generados por dicho uso, se desecharán y suprimirán inmediatamente.

La autoridad judicial competente o una autoridad administrativa independiente cuya decisión sea vinculante únicamente concederá la autorización cuando tenga constancia, sobre la base de pruebas objetivas o de indicios claros que se le aporten, de que el uso del sistema de identificación biométrica remota «en tiempo real» es necesario y proporcionado para alcanzar alguno de los objetivos especificados en el apartado 1, párrafo primero, letra h), el cual se indicará en la solicitud, y, en particular, se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal. Al pronunciarse al respecto, esa autoridad tendrá en cuenta los aspectos mencionados en el apartado 2. Dicha autoridad no podrá adoptar ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota «en tiempo real».

10.2.1. Objetivo

379) Se exige una autorización previa («autorización *ex ante*») para todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho porque es necesario llevar a cabo una evaluación y tomar una decisión sobre si el uso previsto de dicho sistema para tales fines:

- es necesario y proporcionado para alcanzar uno de los objetivos especificados en el artículo 5, apartado 1, letra h), incisos i) a iii), es decir, la búsqueda selectiva de víctimas concretas, la prevención de amenazas específicas o la localización o identificación de autores de un delito; y

- se limita a lo estrictamente necesario en lo que se refiere al período de tiempo, así como al ámbito geográfico y personal.

380) Debido a estos requisitos, antes de que se despliegue cualquier sistema de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho, debe llevarse a cabo una doble evaluación de la necesidad y la proporcionalidad. En primer lugar, el usuario debe llevar a cabo una valoración al realizar una evaluación de impacto relativa a los derechos fundamentales, tal como se exige en el artículo 5, apartado 2, del Reglamento de Inteligencia Artificial. En segundo lugar, de conformidad con el artículo 5, apartado 3, de dicho Reglamento, una autoridad judicial o una autoridad administrativa independiente también debe evaluar la necesidad y la proporcionalidad del uso de dicho sistema dentro de los límites del Derecho nacional que constituye la base jurídica para tal uso, teniendo en cuenta la Carta y otras disposiciones de Derecho de la Unión. Por consiguiente, todo sistema de este tipo solo podrá utilizarse 1) tras una evaluación de impacto relativa a los derechos fundamentales y 2) cuando la autoridad nacional competente haya autorizado dicho uso.

381) El artículo 5, apartado 3, del Reglamento de Inteligencia Artificial debe leerse y entenderse en relación con su artículo 5, apartado 5: para autorizar el uso de un sistema de identificación biométrica remota en tiempo real, debe existir una norma de los Estados miembros de que se trate que autorice dicho uso[217]. Algunos Estados miembros ya disponen de un sistema de autorización previa para el uso de sistemas biométricos, establecido en virtud de otra normativa de la Unión o nacional, como la legislación en materia de protección de datos.

10.2.2. Principio fundamental: autorización previa por parte de una autoridad judicial o una autoridad administrativa independiente

382) El uso de sistemas de identificación biométrica remota en tiempo real que persigue uno de los objetivos enumerados en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial y que se hayan contemplado en el Derecho nacional de los Estados miembros de que se trate debe ser autorizado por una autoridad judicial o una autoridad administrativa independiente **antes de su uso**. Este es el principio fundamental,

383) pero existe una excepción en caso de urgencia. Esta excepción debe estar **debidamente justificada**[218]. Los casos de urgencia **se definen como** situaciones «en las que la necesidad de utilizar los sistemas de que se trate sea tan imperiosa que resulte **efectiva**

[217] Véase también el artículo 5, apartado 2, del Reglamento de Inteligencia Artificial: «[...] de conformidad con el Derecho nacional que autorice dicho uso […]».

[218] Ello quiere decir que «en esas situaciones las autoridades garantes del cumplimiento del Derecho deben solicitar dicha autorización e indicar los motivos por los que no han podido hacerlo antes, sin demora indebida y, como máximo, en un plazo de veinticuatro horas» (considerando 35 del Reglamento de Inteligencia Artificial).

y objetivamente imposible obtener una autorización antes de iniciar el uso del sistema de IA»[219]. En tales casos de urgencia, «el uso debe limitarse al **mínimo imprescindible** y **satisfacer las garantías y condiciones oportunas**, conforme a lo dispuesto en el Derecho nacional y según corresponda en cada supuesto concreto de uso urgente por parte de la propia autoridad garante del cumplimiento del Derecho».

10.2.2.1. Solicitud previa y motivada de conformidad con las normas procesales nacionales

a) ¿Quién presenta la solicitud?

384) Aunque no se especifica, cabe suponer que será normalmente el responsable del despliegue, es decir, **la autoridad (de garantía del cumplimiento del Derecho) competente**, quien presentará la solicitud. Según la definición de «autoridad garante del cumplimiento del Derecho» que figura en el artículo 3, punto 45, letra b), del Reglamento de Inteligencia Artificial, «cualquier otro organismo o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de delitos o ejecución de sanciones penales, incluidas la protección frente a amenazas para la seguridad pública y la prevención de dichas amenazas» se considera una autoridad garante del cumplimiento del Derecho y también podría ser la «autoridad competente» encargada de presentar la solicitud de autorización previa.

385) El uso de un sistema de identificación biométrica remota en tiempo real para actividades que no entren en el ámbito de aplicación del Reglamento de Inteligencia Artificial no necesita una autorización con arreglo al artículo 5, apartado 3, de dicho Reglamento. Si, posteriormente, dicho sistema se utiliza con fines de garantía del cumplimiento del Derecho, su uso entraría en el ámbito de aplicación del Reglamento de Inteligencia Artificial y se necesitaría una autorización si se cumplen los requisitos a que se refiere su artículo 5, apartado 1, letra h).

b) ¿Para qué uso se presenta la solicitud?

386) Se necesita una autorización previa para el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público **con fines de garantía del cumplimiento del Derecho**, aunque sean otras partes, como clubes deportivos o centros comerciales, quienes utilicen los sistemas en nombre de las autoridades garantes del cumplimiento del Derecho**.**

> Por ejemplo:
>
> - Una organización a la que se confían recursos para buscar menores desaparecidos decide utilizar un sistema de identificación biométrica remota en tiempo real. Carece de mandato para ejercer la autoridad pública y las competencias públicas y no está facultado para prevenir delitos ni realizar tareas de prevención de amenazas para la seguridad pública. Este uso no entra en el ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia

[219] Considerando 35 del Reglamento de Inteligencia Artificial.

Artificial, ya que no tiene fines de garantía del cumplimiento del Derecho. Sin embargo, este sistema se clasificará como de «alto riesgo» [punto 1, letra a), del anexo III] y puede que sea necesaria una obligación de consulta previa a la autoridad de control de protección de datos de conformidad con el artículo 36 del RGPD. En función del Derecho nacional aplicable y de si se aplica una de las excepciones a lo dispuesto en el artículo 9, apartado 1, del RGPD, este tratamiento también puede estar sujeto a una autorización previa. En cambio, si las autoridades garantes del cumplimiento del Derecho solicitaran a la misma organización que actuara en su nombre para buscar a menores desaparecidos en un contexto de garantía del cumplimiento del Derecho y bajo la supervisión y las instrucciones de las autoridades garantes del cumplimiento del Derecho competentes, sería necesaria una autorización previa de conformidad con el artículo 5, apartado 3, del Reglamento de Inteligencia Artificial.

- Una organización privada encargada de proporcionar recursos para ayudar a las personas que corren el riesgo de ser víctimas de una catástrofe natural[220] decide utilizar a tal efecto un sistema de identificación biométrica remota en tiempo real. Este uso no entra en el ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial, ya que no tiene fines de garantía del cumplimiento del Derecho. Sin embargo, este sistema se clasificará como de «alto riesgo» [punto 1, letra a), del anexo III] y puede que sea necesaria una obligación de consulta previa a la autoridad de control de protección de datos de conformidad con el artículo 36 del RGPD. En función del Derecho nacional aplicable y de si se aplica una de las excepciones a lo dispuesto en el artículo 9, apartado 1, del RGPD, este tratamiento también puede estar sujeto a una autorización previa.

c) ¿Cuándo? «Todo uso»

387) De conformidad con el artículo 5, apartado 3, del Reglamento de Inteligencia Artificial, es necesaria una autorización previa para «todo uso». Así pues, dicha autorización no debe obtenerse antes de la instalación de un sistema de identificación biométrica remota en tiempo real, sino antes de cada uso concreto.

Por ejemplo:

- La policía instala cámaras de circuitos cerrados de televisión que permiten la identificación biométrica en la estación ferroviaria principal de una ciudad. No es necesaria una autorización conforme al Reglamento de Inteligencia Artificial, pero el sistema biométrico debe cumplir los requisitos aplicables a los sistemas de alto riesgo, debe prepararse una evaluación de impacto relativa a los derechos fundamentales antes de su primer uso y es necesario que una autoridad judicial o una autoridad administrativa independiente conceda una autorización antes de cada uso del sistema.

La policía tiene indicios concretos de que un terrorista llegará en tren a la ciudad (se necesita una autorización previa para la identificación en tiempo real).

220 Las inundaciones fluviales o los incendios naturales son ejemplos de catástrofes naturales.

d) Solicitud motivada

388) El artículo 5, apartado 3, del Reglamento de Inteligencia Artificial exige que cada solicitud de uso de la identificación biométrica remota en tiempo real esté «motivada» y, por tanto, esté justificada y fundamentada.

389) En algunos Estados miembros, es posible presentar dichas solicitudes en línea[221]. De conformidad con el artículo 5, apartado 5, del Reglamento de Inteligencia Artificial, la legislación nacional debe establecer requisitos relativos al contenido exacto de la solicitud, teniendo plenamente en cuenta los requisitos expuestos anteriormente, incluidas pruebas suficientes para determinar la estricta necesidad y proporcionalidad del uso de la identificación biométrica remota en tiempo real y otros aspectos pertinentes para reflejar el carácter excepcional de la autorización de dicho uso.

10.2.2.2. Autorización por parte de una autoridad judicial o una autoridad administrativa independiente

390) Solo podrá conceder la autorización una autoridad judicial o una autoridad administrativa independiente cuya decisión sea vinculante.

a) Autoridad independiente

391) El TJUE ha interpretado el concepto de «independencia» en diferentes contextos. En el asunto HK/Prokuratuur, por ejemplo, el TJUE explicó que la independencia significa que la autoridad mantiene una «posición neutral»[222]. El TJUE precisó que una autoridad implicada en investigaciones anteriores, en ese caso el fiscal, no goza de tal independencia. Pueden aplicarse consideraciones similares en lo que respecta a la independencia exigida por el artículo 5, apartado 3, del Reglamento de Inteligencia Artificial, lo que implica que la autoridad que concede la autorización debe ser independiente de la autoridad que utiliza el sistema de identificación biométrica remota. Esto se aplicaría no solo a la policía, sino también a los jueces de instrucción o fiscales que supervisan el trabajo de la policía y el uso de la identificación biométrica remota para el que se solicita la autorización.

392) En el asunto Comisión/Polonia, en el que se trataba la cuestión de cuándo puede considerarse que un organismo es independiente en el contexto de la seguridad ferroviaria, el TJUE declaró que, «en lo que se refiere a los órganos públicos, la independencia designa normalmente un estatuto que asegure al órgano de que se trate la posibilidad de actuar con total libertad con respecto a los organismos frente a los cuales debe garantizarse su independencia, al abrigo de cualquier instrucción o presión»[223]. Pueden aplicarse indicaciones similares en el contexto del artículo 5, apartado 3, del Reglamento de Inteligencia Artificial.

393) En general, en una sociedad democrática, las autoridades judiciales son también autoridades independientes. El poder judicial desempeña un importante papel cuando es independiente del Gobierno o Gobiernos ejecutivos y del legislador; es el responsable

221 Véanse, por ejemplo, las solicitudes de autorización a la CNIL, la autoridad francesa de protección de datos.
222 Sentencia del Tribunal de Justicia de 2 de marzo de 2021, Prokuratuur, C-746/18, ECLI:EU:C:2021:152, apartado 54.
223 Sentencia del Tribunal de Justicia de 13 de junio de 2018, Comisión/Polonia, C-530/16, ECLI:EU:C:2018:430, apartado 67.

de aplicar la legislación y los derechos y libertades fundamentales, así como de revisar dicha aplicación, de manera autónoma e independiente. La independencia judicial es uno de los aspectos fundamentales del Estado de Derecho y está garantizada por el artículo 47 de la Carta y el artículo 6, apartado 1, del Convenio Europeo de Derechos Humanos (CEDH)[224].

b) Autoridad del lugar en el que se utilizará el sistema

394) La autorización debe dirigirse a la autoridad competente de acuerdo con el Derecho nacional[225].

c) Autorización cuando sea necesario y proporcionado para alcanzar alguno de los objetivos especificados en las excepciones

395) Toda autorización para utilizar la identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho requiere una evaluación para determinar si se han cumplido los requisitos establecidos en el artículo 5, apartado 3, del Reglamento de Inteligencia Artificial.

Muy intrusivo

396) En el contexto de la protección de datos, el Comité Europeo de Protección de Datos (CEPD), en sus Directrices 5/2022, y el Supervisor Europeo de Protección de Datos (SEPD) han considerado que el uso de datos biométricos, en particular de la tecnología de reconocimiento facial, afecta a varios derechos y libertades fundamentales. La Agencia de los Derechos Fundamentales de la Unión Europea y el Consejo de Europa comparten esa postura[226]. Tanto el TJUE[227] como el TEDH[228] han confirmado el carácter sensible del tratamiento de datos biométricos.

397) Toda injerencia **en los derechos y libertades fundamentales debe respetar siempre el contenido esencial de dichos derechos y libertades**. Así se desprende del artículo 52, apartado 1, de la Carta.

398) El concepto de «contenido esencial» de los derechos y libertades fundamentales se ha desarrollado en la jurisprudencia del TJUE y constituye un valor independiente en el ordenamiento jurídico de la Unión. No respetar el contenido esencial de un derecho o libertad fundamental significa que una medida afecta indebidamente a un derecho o libertad, de modo que no se permitirá ninguna injerencia de antemano.

---

224 Véase Manko, R. *Judicial independence in the case law of the European Court of Human Rights* [«La independencia judicial en la jurisprudencia del Tribunal Europeo de Derechos Humanos», documento no disponible en español], Documento informativo del Servicio de Estudios del Parlamento Europeo (EPRS), 2022, p. 12; X, *ECJ case law on judicial independence. A Chronological overview*[«Jurisprudencia del Tribunal de Justicia de la Unión Europea sobre la independencia judicial: una presentación cronológica», documento no disponible en español], Documento informativo del Servicio de Estudios del Parlamento Europeo (EPRS), 2023, p.12.

225 Véase la sentencia del Tribunal de Justicia de 6 de octubre de 2015, Schrems, C-362/14,https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62014CJ0362, ECLI:EU:C:2015:650, apartado 44.

226 Comité Consultivo del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (ETS 108), *Guidelines on Facial Recognition* [«Directrices sobre el reconocimiento facial», documento no disponible en español] 2021.

227 Sentencia del Tribunal de Justicia de 26 de enero de 2023, Ministerstvo na vatreshnite raboti, C-205/21, ECLI:EU:C:2023:49, apartados 60 a 76 y 116 a 134.

228 Sentencia del Tribunal Europeo de Derechos Humanos de 4 de julio de 2023, Glukhin/Rusia, solicitud n.º 11519/20, ECLI:CE:ECHR:2023:0704JUD001151920, apartados 88 y 90 (en lo sucesivo, «la sentencia Glukhin/Rusia»).

Únicamente si es «necesario y proporcionado»

399) Toda injerencia en los derechos y libertades fundamentales requiere una «norma» que, en principio, debe respetar la necesidad y la proporcionalidad de conformidad con el artículo 52 de la Carta (véase más adelante la sección sobre el artículo 5, apartado 5, del Reglamento de Inteligencia Artificial). El artículo 5, apartado 3, del Reglamento de Inteligencia Artificial exige que la legislación nacional que permita el uso de la identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho establezca que la autorización para dicho uso solo se permita «cuando [la autoridad] tenga constancia [...] de que el uso [...] es necesario y proporcionado para alcanzar alguno de los objetivos especificados» en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial. Las autoridades nacionales deben verificar si la identificación biométrica es estrictamente necesaria[229]. Esta evaluación debe basarse en la evaluación de impacto relativa a los derechos fundamentales, en la que ya debería haberse llevado a cabo una evaluación de la necesidad y la proporcionalidad de manera general antes de solicitar una autorización para cada uso con las circunstancias específicas.

10.2.2.3. La excepción al requisito de autorización previa: presentación de la solicitud en un plazo de veinticuatro horas y consecuencias en caso de rechazo

400) En situaciones de urgencia, un usuario puede presentar una solicitud de autorización en un plazo de veinticuatro horas a partir del momento en que se empiece a utilizar el sistema de identificación biométrica remota en tiempo real. En la práctica, este es, por lo general, el momento en que las cámaras que permiten el reconocimiento biométrico están «encendidas» y desplegadas y en que se realiza la primera comparación biométrica con el sistema. El registro de las actividades de tratamiento debe ponerse a disposición de la autoridad para justificar el cumplimiento de los plazos de la solicitud[230].

401) En tal caso, en la solicitud deben exponerse los motivos por los que no se presentó ninguna solicitud previa antes de empezar a utilizar el sistema.

10.2.2.4. Interrupción inmediata en caso de rechazo de la solicitud de autorización y supresión de los datos

402) Además, el artículo 5, apartado 3, del Reglamento de Inteligencia Artificial establece que, si se rechaza una solicitud de autorización en caso de urgencia, el uso del sistema de identificación biométrica remota en tiempo real debe interrumpirse con efecto inmediato. En estos casos, todos los datos, incluidos los resultados y la información de salida generados por dicho uso, deben desecharse y suprimirse inmediatamente[231]. El

---

229 Véase también para la recogida de datos: Sentencia del Tribunal de Justicia de 28 de noviembre de 2024, Ministerstvo na vatreshnite raboti, C-80/23, ECLI:EU:C:2024:991.

230 Los registros de datos generados automáticamente deben conservarse durante al menos seis meses en el caso de los sistemas de IA de alto riesgo e incluirán, en el caso de los sistemas de alto riesgo mencionados en el punto 1, letra a), del anexo III, la fecha y hora del inicio y finalización de cada uso. Véanse el artículo 12, apartado 3, letra a), y el artículo 19 del Reglamento de Inteligencia Artificial.

231 Las autoridades de control también deben tener competencias para llevar a cabo esta comprobación y control posteriores. Véase el artículo 5, apartado 5, del Reglamento de Inteligencia Artificial.

artículo 5, apartado 3, del Reglamento de Inteligencia Artificial es explícito a este respecto, sin excepción. El responsable del despliegue tendrá:

a) una base de datos de referencia que contenga la información biométrica (por ejemplo, imágenes faciales, extractos de voz, etc.) y la información de identificación relacionada, si procede, con la que

b) la información biométrica recogida sobre las personas presentes en el espacio de acceso público se compara para señalar y distinguir a dichas personas;

c) este proceso dará lugar al resultado de la comparación.

403) La obligación de desechar y suprimir los datos recogidos y tratados también significa que la base o las bases de datos de referencia utilizadas para la identificación biométrica no autorizada deben eliminarse y suprimirse si se han creado específicamente para la búsqueda impugnada. La base de datos solo puede conservarse si las autoridades garantes del cumplimiento del Derecho han creado y tienen previsto mantener actualizada la base de datos utilizada para la identificación *lícita* y con fines legítimos *distintos* del uso no autorizado de la identificación biométrica remota en tiempo real.

404) Además de la supresión de cualquier base de datos (ilícita) que contenga información biométrica, también deben suprimirse todas las imágenes y otros datos personales recogidos, en particular los metadatos, los datos técnicos de tratamiento, incluidas las plantillas y otros datos personales, y otros datos de comparación y resultados de salida obtenidos durante el uso ilícito del sistema de identificación biométrica remota en tiempo real.

405) Cuando la autoridad garante del cumplimiento del Derecho impugne el rechazo, un administrador puede conservar los datos hasta que se adopte una decisión definitiva sobre la solicitud. Durante ese período, esos datos no deberían ponerse en principio a disposición de la autoridad garante del cumplimiento del Derecho [310].

10.2.2.5. Ninguna decisión adoptada únicamente sobre la base de los resultados de salida del sistema de identificación biométrica remota en tiempo real

406) De conformidad con el artículo 5, apartado 3, del Reglamento de Inteligencia Artificial, incluso cuando el responsable del despliegue de un sistema de identificación biométrica remota en tiempo real obtiene una autorización, no puede adoptarse ninguna decisión que produzca efectos jurídicos adversos para una persona exclusivamente sobre la base de los resultados de salida del sistema de identificación biométrica remota «en tiempo real».

Por ejemplo:

- Una persona es detenida y encarcelada por un delito grave únicamente sobre la base de una identificación realizada por un sistema de reconocimiento facial, sin ningún control adicional. Esto se suma al requisito de supervisión humana establecido en el artículo 14 del Reglamento de Inteligencia Artificial. Los controles podrían consistir, por ejemplo, en comprobar si una persona determinada se encontraba en un lugar

diferente o si existen otros motivos por los que esa persona no pueda ser la persona buscada.

Requisitos del artículo 14 del Reglamento de Inteligencia Artificial relativos a la supervisión humana

407) El uso de la identificación biométrica remota en tiempo real que esté permitido porque persigue uno de los objetivos enumerados en el artículo 5, apartado 1, letra h), y cumple lo dispuesto en el artículo 5, apartados 2 a 6, del Reglamento de Inteligencia Artificial sigue estando sujeto a las normas aplicables a los sistemas de alto riesgo. Según el artículo 14 del Reglamento de Inteligencia Artificial, los sistemas de IA de alto riesgo «se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas». De conformidad con el artículo 14, apartado 5, del Reglamento de Inteligencia Artificial, el responsable del despliegue no puede adoptar ninguna medida o decisión basándose en la identificación generada por el sistema, «salvo si al menos dos personas físicas con la competencia, formación y autoridad necesarias han verificado y confirmado por separado dicha identificación» o a menos que «el Derecho nacional o de la Unión considere que la aplicación de este requisito es desproporcionada». El artículo 4 del Reglamento de Inteligencia Artificial establece medidas de alfabetización en materia de IA para los proveedores y usuarios de sistemas de IA con el fin de garantizar que «su personal y demás personas que se encarguen en su nombre del funcionamiento y la utilización de sistemas de IA tengan un nivel suficiente de alfabetización en materia de IA», teniendo en cuenta las personas con las que se prevé utilizar los sistemas.

408) Como afirma el CEPD en el contexto de la protección de datos, para que la supervisión humana sea eficaz, es fundamental «capacitar a dicha persona para que comprenda el sistema de [en ese caso, reconocimiento facial] y sus limitaciones y para que interprete correctamente sus resultados. También es necesario establecer un puesto de trabajo y una organización que contrarresten los efectos del sesgo de la automatización y eviten fomentar la aceptación no crítica de los resultados, por ejemplo, a causa de la presión del tiempo, procedimientos gravosos, posibles efectos perjudiciales para la carrera profesional, etc.[232]». Pueden aplicarse consideraciones similares en el contexto del Reglamento de Inteligencia Artificial.

10.3. Notificación a las autoridades de cada uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho

Según el artículo 5, apartado 4, del Reglamento de Inteligencia Artificial:

Sin perjuicio de lo dispuesto en el apartado 3, todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho se notificará a la autoridad de vigilancia del mercado

[232] CEPD, «Directrices 5/2022, sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley», v. 2.0, 26 de abril de 2023, p. 22.

pertinente y a la autoridad nacional de protección de datos de conformidad con las normas nacionales a que se refiere el apartado 5. La notificación contendrá, como mínimo, la información especificada en el apartado 6 y no incluirá datos operativos sensibles.

409) Todo uso de un sistema de identificación biométrica remota que persiga uno de los objetivos enumerados en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial debe notificarse a la autoridad de vigilancia del mercado pertinente y a la autoridad nacional de protección de datos. La notificación debe efectuarse después de cada uso, de modo que pueda comunicarse el número de autorizaciones y sus resultados. No es necesario que en la notificación se incluyan datos operativos sensibles. Según el artículo 3, punto 38, del Reglamento de Inteligencia Artificial, se entiende por «datos operativos sensibles» los datos operativos relacionados con actividades de garantía del cumplimiento del Derecho (prevención, detección, investigación o enjuiciamiento de delitos), cuya divulgación podría poner en peligro la integridad de las causas penales.

410) Para más información sobre la obligación de notificación, véase la sección 10.6.

10.4. Necesidad de normas nacionales dentro de los límites de las excepciones contempladas en el Reglamento de Inteligencia Artificial

10.4.1. Principio: se necesita una norma nacional para proporcionar la base jurídica de la autorización para todas o algunas de las excepciones

411) Se necesitan normas nacionales para hacer operativo el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho. Al mismo tiempo, el artículo 5, apartado 5, del Reglamento de Inteligencia Artificial establece que los Estados miembros siguen siendo libres de decidir si adoptan o no dichas legislaciones nacionales. Si se adopta una norma nacional que autorice el uso de la identificación biométrica remota en tiempo real, el Reglamento de Inteligencia Artificial especifica los elementos sustantivos que debe contener dicha legislación para cumplir los requisitos establecidos en el Reglamento de Inteligencia Artificial.

Artículo 5, apartado 5, del Reglamento de Inteligencia Artificial

Los Estados miembros podrán decidir contemplar la posibilidad de autorizar, ya sea total o parcialmente, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho dentro de los límites y en las condiciones que se indican en el apartado 1, párrafo primero, letra h), y los apartados 2 y 3. Los Estados miembros de que se trate deberán establecer en sus respectivos Derechos nacionales las normas detalladas necesarias aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones a que se refiere el apartado 3, así como a la supervisión y la presentación de informes relacionadas con estas. Dichas normas especificarán también para qué objetivos de los enumerados en el apartado 1, párrafo primero, letra h), y en su caso en relación con qué delitos de los indicados en la letra h), inciso iii), se podrá autorizar a las autoridades competentes para

que utilicen esos sistemas con fines de garantía del cumplimiento del Derecho. Los Estados miembros notificarán dichas normas a la Comisión a más tardar treinta días después de su adopción. Los Estados miembros podrán adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas sobre el uso de sistemas de identificación biométrica remota.

10.4.2. El Derecho nacional respetará los límites y las condiciones del artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial

412) Dado que el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho se considera una injerencia en los derechos fundamentales, el artículo 5, apartado 5, del Reglamento de Inteligencia Artificial dispone que el Derecho nacional de los Estados miembros debe establecer dicho uso. Estas normas nacionales constituyen la base jurídica para la utilización de tales sistemas.

413) Las normas nacionales deberán respetar los límites establecidos en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial y todas las demás condiciones conexas establecidas en dicho Reglamento. Esto implica que los Estados miembros no pueden añadir otros objetivos a la lista de objetivos para los que puede utilizarse la identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho que figura en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial[233].

414) Los Estados miembros notificarán sus normas a la Comisión a más tardar treinta días después de su adopción. Dicha notificación no confiere presunción de conformidad del Derecho de los Estados miembros con el Reglamento de Inteligencia Artificial. Una vez recibida la notificación, la Oficina de IA enviará un acuse de recibo. Antes de que adopten una ley nacional (o regional), se recomienda a los Estados miembros que envíen una versión preliminar de dicha propuesta de ley a la Oficina de IA. En cualquier caso, la falta de notificación a la Oficina de IA en el plazo legal de treinta días tras la adopción establecida en el artículo 5, apartado 5, puede suponer que la legislación nacional no se pueda invocar en procedimientos judiciales, como se ha declarado en diferentes contextos[234]. La Comisión publicará la legislación de los Estados miembros en un sitio web público.

415) Los Estados miembros pueden adoptar, de conformidad con el Derecho de la Unión, leyes más restrictivas, es decir, leyes con unos requisitos más estrictos que los establecidos en el artículo 5, apartado 1, letra h), y apartados 2 a 7 del Reglamento de Inteligencia Artificial.

10.4.3. Normas detalladas del Derecho nacional aplicables a la solicitud, la concesión y el ejercicio de las autorizaciones

233 Véase la sentencia del Tribunal de Justicia de 5 de abril de 2022, Commissioner of An Garda Síochána, C-140/20, ECLI:EU:C:2022:258, apartado 54: «Para cumplir el requisito de proporcionalidad, una normativa debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas».

234 Véase, por analogía, la sentencia del Tribunal de Justicia de 19 de diciembre de 2019, Airbnb Ireland, C-390/18, EU:C:2019:1112, apartados 96 a 97.

416) Las normas detalladas aplicables a la solicitud, la concesión y el ejercicio de la autorización, estas deben determinarse en el Derecho nacional. Todo Estado miembro que desee permitir el uso de los sistemas en cuestión debe especificar en su Derecho nacional dichas normas, que tienen por objeto proporcionar a la autoridad que concede la autorización información pertinente y completa sobre el uso de los sistemas de identificación biométrica remota en tiempo real, de modo que esta pueda decidir sobre la estricta necesidad y proporcionalidad de dicho uso.

A continuación se enumeran algunos aspectos que puede regular la legislación nacional que permite el uso de sistemas de identificación biométrica remota en tiempo real:

- cuáles son las autoridades competentes sujetas al artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial y las autoridades independientes del Estado miembro competentes para conceder (o rechazar) una autorización;
- el ámbito de aplicación detallado de los objetivos para los que la identificación biométrica remota en tiempo real en espacios de acceso público puede utilizarse con fines de garantía del cumplimiento del Derecho [sin ir más allá de los objetivos enumerados en el artículo 5, apartado 1, letra h), incisos i) a iii), sino con la posibilidad de restringirlos aún más];
- disposiciones que establezcan que las solicitudes se presenten por escrito y exijan una explicación detallada del uso específico y de la finalidad prevista del uso para un delito o situación particular que justifique su uso;
- el requisito de motivación y la presentación de pruebas justificativas (y, si procede, la necesidad de una traducción) para justificar el uso del sistema que persigue los objetivos enumerados en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial, en particular en relación con el lugar, la duración y el ámbito personal, así como la estricta necesidad y proporcionalidad, incluidas la pertinencia, la suficiencia y la eficacia del uso del sistema y la ausencia de medios menos intrusivos;
- la descripción de la tecnología que se utilizará y los puntos de localización de la recogida de datos;
- la fiabilidad mínima, los umbrales utilizados y los índices de precisión de los sistemas utilizados;
- la posibilidad de que la autoridad que concede la autorización controle la información presentada, incluidos los detalles técnicos y los criterios de precisión, en cualquier momento *ex ante* y *ex post*;
- las bases de datos de referencia utilizadas;
- el período de conservación de los datos recogidos y de todos los demás datos personales relacionados que se han utilizado;
- las medidas de seguridad, en particular contra el acceso ilícito a los datos;
- otras garantías (cuando proceda);

- la descripción de toda cooperación con autoridades públicas o privadas, incluso en otros países, y de las transferencias e intercambios de datos;

- la trazabilidad del proceso;

- los nombres de las personas responsables del despliegue con las que deben ponerse en contacto;

Para la emisión *de otros elementos formales*

- la posibilidad de un procedimiento escrito complementado con una vista;

- los motivos del rechazo;

- los derechos de las personas que son objeto de una búsqueda, los derechos de las personas cuyos datos se recogen y los posibles derechos de terceros[235];

- los plazos en los que las autoridades deberán tomar su decisión;

- la posible necesidad de notificaciones oficiales al conceder o rechazar la autorización;

- sanciones por incumplimiento de los requisitos (formales y sustanciales);

- el derecho a interponer un recurso en caso de que la autorización haya sido denegada;

Para el ejercicio

- el registro del uso de sistemas de identificación biométrica remota en tiempo real en un registro central que contenga un resumen de los elementos sustantivos;

- posibles obligaciones adicionales de presentación de informes;

- el procedimiento de prórroga o modificación de la autorización.

10.4.4. Normas detalladas del Derecho nacional aplicables a la supervisión y la presentación de informes relacionadas con la autorización

417) El artículo 70 del Reglamento de Inteligencia Artificial exige a los Estados miembros que establezca «al menos una autoridad notificante y al menos una autoridad de vigilancia del mercado». En el artículo 74, apartado 8, del Reglamento de Inteligencia Artificial se dispone que «los Estados miembros designarán como autoridades de vigilancia del mercado a efectos del presente Reglamento bien a las autoridades de control encargadas de la protección de datos competentes con arreglo al Reglamento (UE) 2016/679 o a la Directiva (UE) 2016/680, bien a cualquier otra autoridad designada con arreglo a las mismas condiciones establecidas en los artículos 41 a 44 de la Directiva (UE) 2016/680».

418) Este requisito se suma a la designación de la autoridad que concede la autorización, que el Estado miembro debe establecer antes de que pueda autorizar el uso de sistemas de identificación biométrica remota en tiempo real para cualquiera de los objetivos enumerados en el artículo 5, apartado 1, letra h), incisos i) a iii), del Reglamento de Inteligencia Artificial.

[235] Véase, por ejemplo, CEPD, «Directrices 5/2022, sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley», versión 2.0, 26 de abril de 2023, p. 24 y ss.

10.5. Informes anuales de las autoridades nacionales de vigilancia del mercado y de las autoridades nacionales de protección de datos de los Estados miembros

Según el artículo 5, apartado 6, del Reglamento de Inteligencia Artificial:

Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos de los Estados miembros a las que se haya notificado el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho con arreglo al apartado 4 presentarán a la Comisión informes anuales sobre dicho uso. A tal fin, la Comisión facilitará a los Estados miembros y a las autoridades nacionales de vigilancia del mercado y de protección de datos un modelo que incluya información sobre el número de decisiones adoptadas por las autoridades judiciales competentes o una autoridad administrativa independiente cuya decisión sea vinculante en relación con las solicitudes de autorización de conformidad con el apartado 3, así como su resultado.

419) Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos de los Estados miembros a las que los responsables del despliegue hayan notificado el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho (véase el artículo 5, apartado 4) deben presentar a la Comisión informes anuales sobre dicho uso. Estos informes se elaborarán sobre la base de un modelo facilitado por la Comisión. Esta plantilla se elaborará a su debido tiempo.

420) Cuando el responsable del despliegue es una institución, órgano u organismo de la UE, el SEPD está obligado a informar anualmente a la Comisión sobre los sistemas de identificación biométrica remota en tiempo real utilizados en espacios de acceso público con fines de garantía del cumplimiento del Derecho.

421) Únicamente el informe de la autoridad nacional de protección de datos abarcará el período comprendido entre el 2 de febrero de 2025 y el 2 de agosto de 2025, ya que el Reglamento de Inteligencia Artificial no exige a los Estados miembros que designen una autoridad nacional de vigilancia del mercado antes de esta última fecha.

422) Las autoridades nacionales de vigilancia del mercado y las autoridades nacionales de protección de datos tienen libertad para decidir si desean presentar informes separados o un informe conjunto por Estado miembro.

10.6. Informes anuales de la Comisión

Según el artículo 5, apartado 7, del Reglamento de Inteligencia Artificial:

La Comisión publicará informes anuales sobre el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de garantía del cumplimiento del Derecho elaborados basados en datos agregados relativos a los Estados miembros sobre la base de los informes anuales a que se refiere el apartado 6. Dichos informes anuales no incluirán datos operativos sensibles de las actividades de garantía del cumplimiento del Derecho conexas.

423) El Reglamento de Inteligencia Artificial exige a la Comisión que publique informes anuales sobre el uso de los sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho en los Estados miembros y por las instituciones, órganos y organismos de la Unión, sobre la base de datos agregados. Estos informes se basarán en la información notificada por las autoridades nacionales de conformidad con el artículo 5, apartado 6, del Reglamento de Inteligencia Artificial.

424) El informe anual de la Comisión no contendrá datos operativos sensibles. Por «datos operativos sensibles» se entienden «los datos operativos relacionados con actividades de prevención, detección, investigación o enjuiciamiento de delitos cuya divulgación podría poner en peligro la integridad de las causas penales»[236]. Esto podría significar que no se deben publicar detalles específicos que revelen información sobre investigaciones en curso o pasadas, como, por ejemplo, ubicaciones o cámaras utilizadas.

10.7. Fuera del ámbito de aplicación

425) Todos los demás usos de los sistemas de identificación biométrica remota que no estén contemplados en la prohibición del artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial entran en la categoría de sistemas de IA de alto riesgo, tal como se definen en el artículo 6 y se enumeran en el anexo III, punto 1, letra a), de dicho Reglamento, siempre que entren en su ámbito de aplicación.

426) Entre los sistemas de identificación biométrica remota que quedan fuera del ámbito de aplicación de la prohibición establecida en el artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial se encuentran los sistemas de verificación o autenticación biométrica y los sistemas de identificación biométrica remota (en diferido) en espacios de acceso público con fines de garantía del cumplimiento del Derecho utilizados de forma retroactiva. Por ejemplo, el Derecho nacional podría autorizar a las autoridades policiales a realizar un reconocimiento facial retroactivo para comparar imágenes de sospechosos de delitos con imágenes faciales registradas en una base de datos delictivos[237]. Otro uso que queda fuera del ámbito de aplicación de la prohibición es el uso de sistemas de identificación biométrica remota en tiempo real con fines de garantía del cumplimiento del Derecho en un espacio privado (como en el domicilio de una persona) o en un espacio virtual (como el uso de una sala para chatear o un juego en línea para identificar a un sospechoso de difundir material de abuso sexual de menores). Por último, el uso de sistemas de identificación biométrica remota por agentes privados, tanto en tiempo real como retrospectivo (como un supermercado que utiliza tecnología de reconocimiento facial en tiempo real para identificar a los ladrones conocidos, un centro deportivo que utiliza tecnología de reconocimiento facial en tiempo real para identificar a personas a quienes se prohibió la entrada o las escuelas que utilizan tecnología de reconocimiento facial en tiempo real en escuelas para

236 Artículo 3, punto 38, del Reglamento de Inteligencia Artificial.

237 Por ejemplo, la base de datos *Traitement des Antécédents Judiciaires* [Tratamiento de los antecedentes penales] en Francia, creada por el *Décret n.º 2012-652 du 4 mai 2012 relatif au Traitement des antécédents Judiciaires* [Decreto 2012-652 de 4 de mayo de 2012 relativo al tratamiento de los antecedentes penales].

garantizar la seguridad y controlar la asistencia) quedan fuera del ámbito de aplicación de la prohibición.

427) Además de las normas que se aplican a los sistemas de IA de alto riesgo en general, el **uso retroactivo de los sistemas de identificación biométrica remota** con fines de garantía del cumplimiento del Derecho está sujeto a condiciones y garantías adicionales de conformidad con el artículo 26, apartado 10, del Reglamento de Inteligencia Artificial (aplicable a partir del 2 de agosto de 2026)[238].

428) Los usos con **fines distintos de la garantía del cumplimiento del Derecho** deben, en cualquier caso, cumplir las normas en materia de protección de datos. Los casos que figuran a continuación ilustran la interpretación del artículo 9, apartado 2, del RGPD en los casos de este tipo de uso y las excepciones al tratamiento de datos biométricos.

Por ejemplo:

- En Francia, un tribunal administrativo consideró que probar una tecnología de reconocimiento facial en directo en dos centros educativos públicos para controlar el acceso y con fines de seguridad no era necesario ni proporcionado (de conformidad con las normas de protección de datos). Habría sido posible recurrir a soluciones alternativas menos intrusivas para los estudiantes, como, por ejemplo, utilizar tarjetas de acceso. Además, no se cumplían las condiciones para el consentimiento expreso. Por lo tanto, el consentimiento no podía utilizarse como base jurídica válida para probar la tecnología de reconocimiento facial en centros de educación secundaria[239].
- En los Países Bajos, un supermercado no estaba autorizado a utilizar tecnología de reconocimiento facial en tiempo real para evitar los robos. Sin el consentimiento explícito del cliente o sin ninguna base jurídica que permita el tratamiento por motivos de interés público esencial (como, por ejemplo, fines de seguridad), el supermercado no podría tratar datos biométricos ni, por tanto, desplegar tecnologías de reconocimiento facial[240].
- En Francia[241], se prohibió el uso de un dispositivo con tecnología de reconocimiento facial en directo por parte de un club de fútbol para identificar a los aficionados; en España, se prohibió el uso del mismo tipo de dispositivo para garantizar la seguridad de los espectadores[242].

10.8. Ejemplos de uso

Durante un partido de la Eurocopa, la policía instala cámaras móviles de circuitos cerrados de televisión con tecnologías de reconocimiento facial basadas en IA en una furgoneta policial estacionada cerca de la entrada principal de un estadio de fútbol para proteger la zona e identificar a las personas cuyas caras están registradas en una

238 Artículo 26, apartado 10, y considerando 94 del Reglamento de Inteligencia Artificial.
239 TA Marseille (Tribunal administrativo de Marsella), 27 de febrero de 2020, n.º 1901249.
240 https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-issues-formal-warning-to-supermarket-for-use-of-facial-recognition-technology.
241 https://www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnil-adresse-un-avertissement-un-club
242 https://www.biometricupdate.com/202401/spanish-data-authority-opposes-facial-recognition-for-football-stadium-access

base de datos *ad hoc* que contiene una lista de vigilancia de personas buscadas. En esta lista de vigilancia figuran personas sospechosas de haber cometido un delito (desde delitos graves hasta fraudes y robos), personas que pueden resultar de interés con fines de inteligencia y personas vulnerables con problemas mentales. El uso por parte de la policía de tecnologías de reconocimiento facial en directo no está vinculado a la información relativa a la presencia de una persona concreta en el evento. Aunque es probable que haya personas en la lista de vigilancia para cuya búsqueda se permitiría el uso de la identificación biométrica remota en tiempo real, esta lista no es suficientemente precisa y no está relacionada con el evento en cuestión, en este caso, el partido de fútbol. Por lo tanto, dicho uso estaría prohibido.

Un sistema de identificación biométrica (no remota) verifica si las personas tienen acceso a una central de energía nuclear. Cuando las personas se presentan delante de la cámara (claramente visible) y el sistema deniega el acceso, el sistema intenta comprobar si la persona figura en una lista de vigilancia de terroristas. El sistema no es remoto. Las personas participaban activamente en el ejercicio de verificación para acceder a la central. El caso de uso no entra en el ámbito de aplicación de la prohibición del artículo 5 del Reglamento de Inteligencia Artificial.

Las autoridades policiales de una concurrida ciudad despliegan cámaras de circuitos cerrados de televisión basadas en la IA, que pueden llevar a cabo tecnologías de reconocimiento facial en tiempo real. Además del reconocimiento facial, es posible que se añadan otras funciones, como la detección de objetos y el movimiento de multitudes.

Colocan estas cámaras en diferentes lugares, como lugares de culto, sitios frecuentados por la comunidad LGBT +, consultas médicas, farmacias y varios restaurantes y bares. El Reglamento de Inteligencia Artificial no prohíbe la instalación de cámaras que permiten el reconocimiento biométrico como tal. No obstante, se prohíben determinados usos, como la identificación generalizada e indiscriminada de personas físicas.

Durante las vacaciones de verano se produjeron varios robos en un barrio residencial. La policía obtiene una descripción del sospechoso de testigos oculares, que lo vieron en el barrio en varias ocasiones antes de los robos. Para identificar y detener al sospechoso, la policía utiliza la tecnología de reconocimiento facial en directo en diferentes lugares del barrio durante un fin de semana. Sobre la base de las indicaciones de testigos oculares, la policía creó un retrato robot del sospechoso y extrajo de una base de datos de detenciones varias imágenes de personas que se asemejaban a dicho retrato.
Aunque la policía utiliza la tecnología de reconocimiento facial en tiempo real con un sospechoso que constituye el objetivo específico y ha definido un perímetro y un período de uso, no se permite su despliegue para este tipo de infracción que no figura en el anexo II del Reglamento de Inteligencia Artificial.

La policía utiliza un sistema de reconocimiento biométrico para analizar las emociones de los aficionados en un estadio de fútbol. El sistema detecta un posible comportamiento agresivo y despliega inmediatamente en esa parte del estadio la identificación biométrica remota en tiempo real para identificar a los hinchas violentos que actuaron con violencia en el pasado.
La identificación de emociones en el estadio no está prohibida por el Reglamento de Inteligencia Artificial, aunque sigue entrando en la categoría de alto riesgo de dicho Reglamento. Sin embargo, la aplicación de la identificación biométrica remota en tiempo real estaría prohibida por el Reglamento de Inteligencia Artificial, en particular cuando el sistema biométrico es el que decide sobre la necesidad de identificar a las personas a efectos de la garantía del cumplimiento del Derecho.

La policía se sirve de una red de circuitos cerrados de televisión instalada en la ciudad y en el metro para identificar a un manifestante político que organizó una protesta colectiva en las calles. En el Estado miembro de que se trate, los organizadores de protestas colectivas en la vía pública y en zonas públicas, como las calles, deben informar a las autoridades municipales con tres días de antelación sobre la protesta prevista, a fin de evitar perturbaciones del orden público y la violencia. La ausencia de notificación es un delito punible con una pena de prisión de hasta seis meses y una multa de hasta 8 000 EUR. Para identificar al manifestante, la policía extrae las transmisiones de vídeo de las cámaras de circuitos cerrados de televisión instaladas en las calles y realiza un reconocimiento facial retroactivo comparando las imágenes extraídas con fotografías publicadas en las redes sociales.

El **uso retrospectivo de la tecnología de reconocimiento facial** no está prohibido por el Reglamento de Inteligencia Artificial. Es un uso considerado de alto riesgo y debe cumplir los requisitos del Reglamento de Inteligencia Artificial para dichos sistemas[243].
Estos son otros ejemplos de prácticas que NO están prohibidas:

- Hoteles que utilizan la identificación biométrica remota en tiempo real para reconocer a los invitados VIP. Esto no es garantía del cumplimiento del Derecho.
- Centros comerciales que utilizan la identificación biométrica remota en tiempo real para encontrar a ladrones en comercios. Esto no es garantía del cumplimiento del Derecho.

Prácticas prohibidas:

[243] El tratamiento de datos biométricos con fines de garantía del cumplimiento del Derecho sigue sujeto a lo dispuesto en el artículo 10 de la Directiva sobre protección de datos en el ámbito penal, que debe aplicarse a escala nacional. El tratamiento de estos datos para llevar a cabo el uso retroactivo de la tecnología de reconocimiento facial solo debe permitirse si es estrictamente necesario, y debe estar sujeto a las garantías adecuadas. Que el uso retroactivo de la tecnología de reconocimiento facial sea estrictamente necesario para identificar al manifestante es cuestionable. En la sentencia Glukhin/Rusia, que sirve de base para este escenario, el TEDH dictaminó que, si bien la detección de delitos puede ser un objetivo legítimo, el uso de la tecnología de reconocimiento facial, tanto con carácter retroactivo como en tiempo real, era desproporcionado, ya que no existían riesgos para el orden público o la seguridad del transporte. El Tribunal de Justicia destacó el carácter «particularmente intrusivo» de las tecnologías de reconocimiento facial. En dicho asunto, el Tribunal de Justicia concluyó que el uso de las tecnologías de reconocimiento facial no respondía a una necesidad social apremiante ni era necesario en una sociedad democrática.

A petición de la policía, un centro comercial usa la identificación biométrica remota en tiempo real para encontrar a ladrones que roban en comercios. El sistema se despliega con fines de garantía del cumplimiento del Derecho, en un espacio de acceso público. Este uso está prohibido porque la búsqueda de ladrones que roban en los comercios no forma parte de ninguna de las excepciones del artículo 5, apartado 1, letra h), del Reglamento de Inteligencia Artificial.

11. FECHA DE COMIENZO DE APLICACIÓN

429) De conformidad con el artículo 113 del Reglamento de Inteligencia Artificial, el artículo 5 del Reglamento de Inteligencia Artificial se aplica a partir del 2 de febrero de 2025. Las prohibiciones establecidas en dicha disposición se aplican, en principio, a todos los sistemas de IA, independientemente de que hayan sido introducidos en el mercado o puestos en servicio antes o después de esa fecha[244].

430) Los capítulos sobre gobernanza y sanciones serán aplicables el 2 de agosto de 2025. Por consiguiente, las disposiciones relativas a las sanciones por incumplimiento de las prohibiciones establecidas en el artículo 5 del Reglamento de Inteligencia Artificial no se aplicarán antes del 2 de agosto de 2025. Durante este período transitorio, tampoco habrá autoridades de vigilancia del mercado que supervisen si las prohibiciones se cumplen de forma adecuada.

431) No obstante, incluso durante este período transitorio, las prohibiciones son plenamente aplicables y obligatorias para los proveedores y responsables del despliegue de sistemas de IA. Así pues, dichos operadores deben adoptar las medidas necesarias para garantizar que no introducen en el mercado, ponen en servicio o utilizan sistemas de IA que puedan constituir prácticas prohibidas en virtud del artículo 5 del Reglamento de Inteligencia Artificial. Aunque las disposiciones relativas a la supervisión y las multas no se apliquen hasta una fecha posterior, las propias prohibiciones tienen efecto directo y, por tanto, permiten a las partes afectadas exigir que se respeten ante los órganos jurisdiccionales nacionales y solicitar medidas cautelares contra las prácticas prohibidas.

12. REVISIÓN Y ACTUALIZACIÓN DE LAS DIRECTRICES DE LA COMISIÓN

432) Las presentes directrices constituyen una primera interpretación con ejemplos prácticos de las prohibiciones establecidas en el artículo 5 del Reglamento de Inteligencia Artificial. La Comisión prestará apoyo adicional a los operadores y a las autoridades para comprender las prohibiciones y recopilará de forma continua nuevos casos prácticos con las aportaciones de los proveedores y los responsables del despliegue de sistemas de IA, el Consejo de IA y otras partes interesadas pertinentes.

433) La Comisión revisará las presentes directrices tan pronto como sea necesario teniendo en cuenta la experiencia práctica adquirida gracias a la aplicación de las prohibiciones

[244] Véase el artículo 111, apartados 1 y 2, del Reglamento de Inteligencia Artificial, que especifica que la cláusula de anterioridad se entiende sin perjuicio de la aplicación del artículo 5 de dicho Reglamento a que se refiere su artículo 113, apartado 3, letra a).

y el ritmo de la evolución tecnológica, social y reglamentaria en este ámbito. Esto también incluye cualquier experiencia pertinente obtenida a partir de la aplicación de medidas de garantía del cumplimiento en materia de vigilancia del mercado y de las interpretaciones del TJUE sobre las prohibiciones y otras disposiciones del Reglamento de Inteligencia Artificial examinadas en las presentes directrices. Durante dicha revisión, la Comisión podrá decidir retirar o modificar las presentes directrices. La Comisión anima a los proveedores y a los responsables del despliegue de sistemas de IA, a las autoridades nacionales de vigilancia del mercado a través del Consejo de IA, el foro consultivo sobre IA, la comunidad investigadora y las organizaciones de la sociedad civil a que contribuyan a este proceso respondiendo a futuras consultas públicas.