III

*(Actos preparatorios)*

# COMITÉ DE LAS REGIONES

**INTERACTIO - REUNIÓN HÍBRIDA - 147.º PLENO DEL CDR, 1.12.2021 – 2.12.2021**

## Dictamen del Comité Europeo de las Regiones — Enfoque europeo de la inteligencia artificial — Ley de inteligencia artificial

**(Dictamen revisado)**

(2022/C 97/12)

| | |
|---|---|
| **Ponente**: | Guido RINK (NL/PSE), miembro de la Junta de Gobierno Local de Emmen |
| **Documentos de referencia**: | Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — Fomentar un planteamiento europeo en materia de inteligencia artificial<br>COM(2021) 205 final<br>Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión<br>COM(2021) 206 final |

I. **RECOMENDACIONES DE ENMIENDA**

**Enmienda 1**

Considerando 1

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interno mediante el establecimiento de un marco jurídico uniforme, en particular en lo que respecta al desarrollo, la comercialización y la utilización de la inteligencia artificial de conformidad con los valores de la Unión. El presente Reglamento persigue varios fines imperiosos de interés general, tales como asegurar un nivel elevado de protección de la salud, la seguridad y los derechos humanos, y garantiza la libre circulación transfronteriza de bienes y servicios basados en la IA, con lo que impide que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que el presente Reglamento lo autorice expresamente. | El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interno ***y garantizar los derechos fundamentales de la ciudadanía*** mediante el establecimiento de un marco jurídico uniforme, en particular en lo que respecta al desarrollo, la comercialización y la utilización de la inteligencia artificial de conformidad con los valores de la Unión. El presente Reglamento persigue varios fines imperiosos de interés general, tales como asegurar un nivel elevado de protección de la salud, la seguridad y los derechos humanos, y garantiza la libre circulación transfronteriza de bienes y servicios basados en la IA, con lo que impide que los Estados miembros impongan restricciones al desarrollo, la comercialización y la utilización de sistemas de IA, a menos que el presente Reglamento lo autorice expresamente. |

***Exposición de motivos***

Esta referencia a los derechos fundamentales tiene por objeto poner de relieve el vínculo con la Carta de los Derechos Fundamentales de la Unión Europea.

**Enmienda 2**

Nuevo considerando después del considerando 6

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| | ***La definición de los sistemas de IA es un proceso continuo que refleja el contexto en el que se inscribe la IA y sigue el ritmo de la evolución de la sociedad en este ámbito, sin perder de vista el vínculo entre el ecosistema de excelencia y el ecosistema de confianza.*** |

***Exposición de motivos***

La evolución en materia de IA y los avances tecnológicos requieren un enfoque adaptativo y evolutivo. Este considerando tiene por objeto aclarar que la definición de la IA debe evolucionar con el tiempo y en consonancia con los avances en los sistemas y aplicaciones de IA.

**Enmienda 3**

Considerando 20

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Para velar por que dichos sistemas se utilicen de manera responsable y proporcionada, también es importante establecer que, en esas tres situaciones enumeradas de manera limitativa y definidas con precisión, deben tenerse en cuenta determinados elementos, en particular en lo que se refiere a la naturaleza de la situación que dé lugar a la solicitud, a las consecuencias que su uso puede tener sobre los derechos y las libertades de todas las personas implicadas, y a las salvaguardias y condiciones que acompañen a su uso. Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley debe estar sujeto a límites temporales y espaciales ***adecuados*** que tengan en cuenta, en particular, las pruebas o indicios relativos a las amenazas, las víctimas o los autores. La base de datos de personas de referencia debe ser adecuada para cada caso de uso en cada una de las tres situaciones antes mencionadas. | Para velar por que dichos sistemas se utilicen de manera responsable y proporcionada, también es importante establecer que, en esas tres situaciones enumeradas de manera limitativa y definidas con precisión, deben tenerse en cuenta determinados elementos, en particular en lo que se refiere a la naturaleza de la situación que dé lugar a la solicitud, a las consecuencias que su uso puede tener sobre los derechos y las libertades de todas las personas implicadas, y a las salvaguardias y condiciones que acompañen a su uso. ***Se debería consultar a los entes locales y regionales afectados antes de recurrir excepcionalmente a estos sistemas.*** Además, el uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley debe estar sujeto a límites temporales y espaciales ***estrictos*** que tengan en cuenta, en particular, las pruebas o indicios relativos a las amenazas, las víctimas o los autores. La base de datos de personas de referencia debe ser adecuada para cada caso de uso en cada una de las tres situaciones antes mencionadas. |

***Exposición de motivos***

Los sistemas de identificación biométrica remota «en tiempo real» no deben utilizarse a la ligera.

**Enmienda 4**

Considerando 21

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley debe estar autorizado de manera expresa y específica por una autoridad judicial o por una autoridad administrativa independiente de un Estado miembro. ***En principio, dicha*** autorización debe obtenerse con anterioridad al uso, excepto en situaciones de urgencia debidamente justificadas, es decir, aquellas en las que la necesidad de utilizar los sistemas en cuestión sea tan imperiosa que imposibilite, de manera efectiva y objetiva, obtener una autorización antes de iniciar el uso. En ***tales situaciones de urgencia***, el uso debe limitarse al mínimo imprescindible y cumplir las salvaguardias y las condiciones oportunas, conforme a lo estipulado en el Derecho interno ***y según corresponda en cada caso concreto de uso urgente por parte de las fuerzas o cuerpos de seguridad***. Además, ***en esas situaciones*** las fuerzas o cuerpos de seguridad deben tratar de obtener una autorización ***lo antes posible e indicar los motivos por los que no han podido hacerlo antes***. | Todo uso de un sistema de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley debe estar autorizado de manera expresa y específica por una autoridad judicial o por una autoridad administrativa independiente de un Estado miembro. ***Dicha*** autorización debe obtenerse con anterioridad al uso, excepto en situaciones de urgencia debidamente justificadas, es decir, aquellas en las que la necesidad de utilizar los sistemas en cuestión sea tan imperiosa que imposibilite, de manera efectiva y objetiva, obtener una autorización antes de iniciar el uso. En ***cualquier caso***, el uso debe limitarse al mínimo imprescindible y cumplir las salvaguardias y las condiciones oportunas, conforme a lo estipulado en el Derecho interno. Además, las fuerzas o cuerpos de seguridad deben ***informar inmediatamente a los entes locales y regionales afectados y*** tratar de obtener una autorización ***de las autoridades competentes***. |

***Exposición de motivos***

La responsabilidad política y administrativa de la gestión y la vigilancia de los espacios públicos incumbe a los entes locales y regionales. Por consiguiente, hay que involucrarlos debidamente en el despliegue de dichos sistemas en los espacios públicos. En situaciones de emergencia en las que no quepa esperar razonablemente una consulta previa, deberá informarse inmediatamente al ente local o regional afectado del despliegue de sistemas biométricos en el espacio público.

**Enmienda 5**

Considerando 39

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Los sistemas de IA empleados en la gestión de la migración, el asilo y el control fronterizo afectan a personas que con frecuencia se encuentran en una situación especialmente vulnerable y dependen del resultado de las actuaciones de las autoridades públicas competentes. Por este motivo, es sumamente importante que los sistemas de IA que se utilizan en estos contextos sean precisos, no discriminatorios y transparentes, a fin de garantizar que se respeten los derechos fundamentales de las personas afectadas y, en particular, sus derechos a la libre circulación, la no discriminación, la intimidad personal y la protección de los datos personales, la protección internacional y la buena administración. Por lo tanto, ***procede*** considerar de alto riesgo a aquellos sistemas de IA destinados a que las autoridades públicas competentes que realizan tareas en el ámbito de la gestión de la migración, el asilo y el control fronterizo los utilicen como polígrafos y herramientas similares o para detectar el estado emocional de una persona física; para evaluar determinados riesgos que presenten personas físicas que entren en el territorio de un Estado miembro o soliciten un visado o asilo; para verificar la autenticidad de los documentos pertinentes de personas físicas; para ayudar a las autoridades públicas competentes a examinar las solicitudes de asilo, visado y permiso de residencia, así como las reclamaciones conexas en relación con el objetivo de determinar si las personas físicas solicitantes de un estatuto reúnen los requisitos necesarios para su obtención. Los sistemas de IA en el ámbito de la gestión de la migración, el asilo y el control fronterizo abarcados por el presente Reglamento deben cumplir los requisitos procedimentales pertinentes establecidos por la Directiva 2013/32/UE del Parlamento Europeo y del Consejo, el Reglamento (UE) n.º 810/2009 del Parlamento Europeo y el Consejo, y otra legislación en la materia. | Los sistemas de IA empleados en la gestión de la migración, el asilo y el control fronterizo afectan a personas que con frecuencia se encuentran en una situación especialmente vulnerable y dependen del resultado de las actuaciones de las autoridades públicas competentes. Por este motivo, es sumamente importante que los sistemas de IA que se utilizan en estos contextos sean precisos, no discriminatorios y transparentes, a fin de garantizar que se respeten los derechos fundamentales de las personas afectadas y, en particular, sus derechos a la libre circulación, la no discriminación, la intimidad personal y la protección de los datos personales, la protección internacional y la buena administración. Por lo tanto, ***se deben*** considerar de alto riesgo a aquellos sistemas de IA destinados a que las autoridades públicas competentes que realizan tareas en el ámbito de la gestión de la migración, el asilo y el control fronterizo los utilicen como polígrafos y herramientas similares o para detectar el estado emocional de una persona física; para evaluar determinados riesgos que presenten personas físicas que entren en el territorio de un Estado miembro o soliciten un visado o asilo; para verificar la autenticidad de los documentos pertinentes de personas físicas; para ayudar a las autoridades públicas competentes a examinar las solicitudes de asilo, visado y permiso de residencia, así como las reclamaciones conexas en relación con el objetivo de determinar si las personas físicas solicitantes de un estatuto reúnen los requisitos necesarios para su obtención. Los sistemas de IA en el ámbito de la gestión de la migración, el asilo y el control fronterizo abarcados por el presente Reglamento deben cumplir los requisitos procedimentales pertinentes establecidos por la Directiva 2013/32/UE del Parlamento Europeo y del Consejo, el Reglamento (UE) n.º 810/2009 del Parlamento Europeo y el Consejo, y otra legislación en la materia. |

***Exposición de motivos***

Esta enmienda tiene por objeto subrayar la necesidad de someter los sistemas de IA en cuestión al régimen reforzado previsto para los sistemas de IA de alto riesgo.

**Enmienda 6**

Considerando 43

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Deben aplicarse a los sistemas de IA de alto riesgo requisitos referentes a la calidad de los conjuntos de datos utilizados, la documentación técnica y el registro, la transparencia y la comunicación de información a los usuarios, la vigilancia humana, la solidez, la precisión y la ciberseguridad. Dichos requisitos son necesarios para mitigar de forma efectiva los riesgos para la salud, la seguridad y los derechos fundamentales, según corresponda en función de la finalidad ***prevista*** del sistema, y no se dispone razonablemente de otras medidas menos restrictivas del comercio, con lo que se evitan restricciones injustificadas de este. | Deben aplicarse a los sistemas de IA de alto riesgo requisitos referentes a la calidad de los conjuntos de datos utilizados, la documentación técnica y el registro, la transparencia y la comunicación de información a los usuarios, la vigilancia humana, la solidez, la precisión y la ciberseguridad. Dichos requisitos son necesarios para mitigar de forma efectiva los riesgos para la salud, la seguridad***, la seguridad de los datos, los derechos de los consumidores*** y los derechos fundamentales, según corresponda en función de la finalidad del sistema, y no se dispone razonablemente de otras medidas menos restrictivas del comercio, con lo que se evitan restricciones injustificadas de este. ***Las personas o grupos de personas físicas afectados por sistemas de IA de alto riesgo comercializados en la Unión o puestos en servicio de otro modo deben ser informados de manera adecuada, fácilmente accesible y comprensible y poder encontrar información pública de manera fácilmente accesible, adecuada y comprensible sobre el hecho de que están sometidos a dichos sistemas.*** |

***Exposición de motivos***

Los requisitos de transparencia e información para proveedores y usuarios deberían ampliarse a las personas o grupos de personas que puedan verse afectados por el uso de sistemas de IA de alto riesgo enumerados en el anexo III del Reglamento. El término «comprensible» significa, entre otras cosas, lenguaje comprensible y accesible para el usuario, lo que incluye tanto la lengua oral como la lengua de signos.

**Enmienda 7**

Nuevo considerando después del considerando 44

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| | ***Los proveedores de sistemas de IA se abstendrán de incluir en su sistema de gestión de la calidad medidas que fomenten la discriminación injustificada por motivos de sexo, origen, religión o convicciones, discapacidad, edad, orientación sexual o cualquier otra razón.*** |

***Exposición de motivos***

La discriminación ilegal deriva de la acción humana. Los proveedores de sistemas de IA deben abstenerse de incluir en su sistema de gestión de la calidad medidas que puedan fomentar la discriminación.

**Enmienda 8**

Considerando 47

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Por otro lado, debe exigirse ***cierto*** grado de transparencia respecto de los sistemas de IA de alto riesgo para subsanar la opacidad que puede hacer a algunos de ellos incomprensibles o demasiado complejos para las personas físicas. Los usuarios deben ser capaces de interpretar la información de salida del sistema y de usarla adecuadamente. En consecuencia, los sistemas de IA de alto riesgo deben ir acompañados de la documentación y las instrucciones de uso oportunas e incluir información clara y concisa, en particular sobre los posibles riesgos para los derechos fundamentales y de discriminación, cuando corresponda. | Por otro lado, debe exigirse ***un alto*** grado de transparencia respecto de los sistemas de IA de alto riesgo para subsanar la opacidad que puede hacer a algunos de ellos incomprensibles o demasiado complejos para las personas físicas ***o las autoridades públicas de todos los niveles de gobierno***. Los usuarios deben ser capaces de interpretar la información de salida del sistema y de usarla adecuadamente. En consecuencia, los sistemas de IA de alto riesgo deben ir acompañados de la documentación y las instrucciones de uso oportunas e incluir información clara y concisa, en particular sobre los posibles riesgos para los derechos fundamentales y de discriminación, cuando corresponda. |

***Exposición de motivos***

La responsabilidad de los diseñadores de sistemas de IA de alto riesgo se ve socavada por el empleo de la expresión «cierto grado de transparencia».

**Enmienda 9**

Considerando 48

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal modo que su funcionamiento pueda ser vigilado por personas físicas. A tal fin, el proveedor del sistema debe definir las medidas adecuadas de vigilancia humana antes de su introducción en el mercado o puesta en servicio. Cuando proceda, dichas medidas deben garantizar, en concreto, que el sistema presente limitaciones operativas incorporadas que el propio sistema no pueda desactivar, que responda al operador humano, y que las personas físicas a quienes se haya encomendado la vigilancia humana posean las competencias, la formación y la autoridad necesarias para desempeñar esa función. | Los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal modo que su funcionamiento pueda ser vigilado por personas físicas ***y las autoridades públicas de todos los niveles de gobierno***. A tal fin, el proveedor del sistema debe definir las medidas adecuadas de vigilancia humana antes de su introducción en el mercado o puesta en servicio. Cuando proceda, dichas medidas deben garantizar, en concreto, que el sistema presente limitaciones operativas incorporadas que el propio sistema no pueda desactivar, que responda al operador humano, y que las personas físicas a quienes se haya encomendado la vigilancia humana posean las competencias, la formación y la autoridad necesarias para desempeñar esa función. |

***Exposición de motivos***

Se considera innecesaria.

**Enmienda 10**

Considerando 67

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Los sistemas de IA de alto riesgo deben llevar el marcado CE para acreditar su conformidad con el presente Reglamento y así poder circular libremente por el mercado interno. Los Estados miembros no deben crear obstáculos ***injustificados*** a la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE. | Los sistemas de IA de alto riesgo deben llevar el marcado CE para acreditar su conformidad con el presente Reglamento y así poder circular libremente por el mercado interno. Los Estados miembros no deben crear obstáculos a la introducción en el mercado o la puesta en servicio de sistemas de IA de alto riesgo que cumplan los requisitos establecidos en el presente Reglamento y lleven el marcado CE. ***Los Estados miembros tienen la facultad de regular las prácticas y los sistemas de IA de alto riesgo únicamente por intereses de seguridad pública y nacional imperiosos y debidamente justificados.*** |

***Exposición de motivos***

Aunque los Estados miembros no deben obstaculizar la aplicación del Reglamento, deberían conservar el derecho a regular los sistemas de IA de alto riesgo si están en juego intereses de seguridad pública y nacional.

**Enmienda 11**

Considerando 70

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Determinados sistemas de IA destinados a interactuar con personas físicas o a generar contenidos pueden conllevar riesgos específicos de suplantación o falsificación, con independencia de si son clasificados como de alto riesgo o no. Por consiguiente, el uso de estos sistemas debe estar sujeto***, en determinadas circunstancias,*** a obligaciones de transparencia específicas, sin perjuicio de los requisitos y las obligaciones aplicables a los sistemas de IA de alto riesgo. En particular, debe informarse a las personas físicas de que interactúan con un sistema de IA***, a menos que ello sea evidente debido a las circunstancias y al contexto de uso***. Además, debe informarse a las personas físicas de que están expuestas a un sistema de reconocimiento emocional o a un sistema de categorización biométrica. Esta información y estas notificaciones deben facilitarse en formatos accesibles para las personas con discapacidad. Además, los usuarios que utilicen un sistema de IA para generar o manipular imágenes, archivos de audio o vídeos que se asemejen notablemente a personas, lugares o sucesos reales y puedan inducir erróneamente a una persona a pensar que son auténticos, deben comunicar que estos han sido creados o manipulados de manera artificial etiquetando el contenido generado por la inteligencia artificial como corresponda e indicando su origen artificial. | Determinados sistemas de IA destinados a interactuar con personas físicas o a generar contenidos pueden conllevar riesgos específicos de suplantación o falsificación, con independencia de si son clasificados como de alto riesgo o no. Por consiguiente, el uso de estos sistemas debe estar sujeto a obligaciones de transparencia específicas, sin perjuicio de los requisitos y las obligaciones aplicables a los sistemas de IA de alto riesgo. En particular, debe informarse ***sistemáticamente*** a las personas físicas de que interactúan con un sistema de IA. Además, debe informarse a las personas físicas de que están expuestas a un sistema de reconocimiento emocional o a un sistema de categorización biométrica. Esta información y estas notificaciones deben facilitarse en formatos accesibles para las personas con discapacidad. Además, los usuarios que utilicen un sistema de IA para generar o manipular imágenes, archivos de audio o vídeos que se asemejen notablemente a personas, lugares o sucesos reales y puedan inducir erróneamente a una persona a pensar que son auténticos, deben comunicar que estos han sido creados o manipulados de manera artificial etiquetando el contenido generado por la inteligencia artificial como corresponda e indicando su origen artificial. |

***Exposición de motivos***

No debe hacerse ninguna excepción a la obligación de transparencia e información cuando las personas físicas interactúen con sistemas de IA.

**Enmienda 12**

Considerando 76

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Debe establecerse un Comité Europeo de Inteligencia Artificial que facilite la aplicación fluida, efectiva y armonizada del presente Reglamento. Dicho Comité deberá encargarse de diversas tareas de asesoramiento. Entre otras cosas, deberá emitir dictámenes, recomendaciones, informes de asesoramiento u orientaciones sobre asuntos relacionados con la aplicación de este Reglamento, en particular en lo que respecta a las especificaciones técnicas o las normas existentes en relación con los requisitos previstos en el presente Reglamento, y asesorar y apoyar a la Comisión en cuestiones específicas vinculadas a la inteligencia artificial. | Debe establecerse un Comité Europeo de Inteligencia Artificial que facilite la aplicación fluida, efectiva y armonizada del presente Reglamento. Dicho Comité deberá encargarse de diversas tareas de asesoramiento. Entre otras cosas, deberá emitir dictámenes, recomendaciones, informes de asesoramiento u orientaciones sobre asuntos relacionados con la aplicación de este Reglamento, en particular en lo que respecta a las especificaciones técnicas o las normas existentes en relación con los requisitos previstos en el presente Reglamento, y asesorar y apoyar a la Comisión en cuestiones específicas vinculadas a la inteligencia artificial. ***La composición del referido Comité Europeo de Inteligencia Artificial debe reflejar los intereses de la sociedad europea y respetar el equilibrio de género.*** |

***Exposición de motivos***

El Comité Europeo de Inteligencia Artificial debe reflejar adecuadamente los intereses principales de la sociedad europea. Entre ellos figuran sus intereses en materia de derechos humanos, el clima y la eficiencia energética de los sistemas de IA, la seguridad, la inclusión social, la salud, etc. El equilibrio entre hombres y mujeres es una condición *sine qua non* para garantizar la diversidad en las actividades de asesoramiento, elaboración de orientaciones, etc.

**Enmienda 13**

Considerando 77

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Los Estados miembros desempeñan un papel clave en la aplicación y ejecución de este Reglamento. En este sentido, cada Estado miembro debe designar a una o varias autoridades nacionales competentes que se encarguen de supervisar su aplicación y ejecución. Con el fin de incrementar la eficiencia en términos de organización en los Estados miembros y establecer un punto de contacto oficial con el público y otros homólogos en los Estados miembros y la Unión, una autoridad nacional de cada Estado miembro debe ser designada autoridad nacional de supervisión. | Los Estados miembros desempeñan un papel clave en la aplicación y ejecución de este Reglamento. En este sentido, cada Estado miembro debe designar a una o varias autoridades nacionales competentes que se encarguen de supervisar su aplicación y ejecución. Con el fin de incrementar la eficiencia en términos de organización en los Estados miembros y establecer un punto de contacto oficial con el público y otros homólogos en los Estados miembros y la Unión, una autoridad nacional de cada Estado miembro debe ser designada autoridad nacional de supervisión. ***Se encomendarán a los entes locales y regionales tareas de supervisión o ejecución cuando un Estado miembro lo considere oportuno.*** |

***Exposición de motivos***

A efectos de la aplicabilidad del Reglamento y sus disposiciones de supervisión y ejecución, debe facultarse a los Estados miembros a encomendar tareas de supervisión o ejecución a los entes locales y regionales cuando sea necesario y en la medida de lo posible.

**Enmienda 14**

Considerando 79

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Con el objetivo de garantizar el cumplimiento adecuado y efectivo de los requisitos y obligaciones previstos en el presente Reglamento, que constituye legislación armonizada de la Unión, debe aplicarse en su totalidad el sistema relativo a la vigilancia del mercado y la conformidad de los productos establecido por el Reglamento (UE) 2019/1020. Cuando sea necesario para el cumplimiento de su mandato, las autoridades o los organismos públicos nacionales que supervisen la aplicación del Derecho de la Unión que protege los derechos fundamentales, incluidos los organismos de igualdad, también deben tener acceso a la documentación que se cree en virtud del presente Reglamento. | Con el objetivo de garantizar el cumplimiento adecuado y efectivo de los requisitos y obligaciones previstos en el presente Reglamento, que constituye legislación armonizada de la Unión, debe aplicarse en su totalidad el sistema relativo a la vigilancia del mercado y la conformidad de los productos establecido por el Reglamento (UE) 2019/1020. Cuando sea necesario para el cumplimiento de su mandato, las autoridades o los organismos públicos nacionales que supervisen la aplicación del Derecho de la Unión que protege los derechos fundamentales, incluidos los organismos de igualdad ***y, en su caso, los entes locales y regionales***, también deben tener acceso a la documentación que se cree en virtud del presente Reglamento. |

***Exposición de motivos***

Esta enmienda tiene por objeto tener en cuenta las distintas estructuras de gobierno de los Estados miembros de la UE.

**Enmienda 15**

Considerando 83

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Todas las partes implicadas en la aplicación del presente Reglamento deben respetar la confidencialidad de la información y los datos que obtengan en el ejercicio de sus funciones, con vistas a garantizar la cooperación fiable y constructiva de las autoridades competentes en la Unión y a escala nacional. | Todas las partes implicadas en la aplicación del presente Reglamento deben respetar la confidencialidad de la información y los datos que obtengan en el ejercicio de sus funciones, con vistas a garantizar la cooperación fiable y constructiva de las autoridades competentes en la Unión y a escala nacional***, regional y local***. |

***Exposición de motivos***

Esta enmienda tiene por objeto tener en cuenta las distintas estructuras de gobierno de los Estados miembros de la UE.

**Enmienda 16**

Título I, artículo 3 — Definiciones, punto 1

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| «Sistema de inteligencia artificial (sistema de IA)»: el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa. | «Sistema de inteligencia artificial (sistema de IA)»: el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran ***enumeradas con carácter no exhaustivo*** en el anexo I***, relativo a las prácticas sociales, a la identidad y a la cultura,*** y que puede, para un conjunto determinado de objetivos definidos por seres humanos, ***a partir de la observación de su entorno mediante la recopilación de datos, la interpretación de los datos recopilados —ya sean estructurados o no—, la gestión del conocimiento o el tratamiento de la información derivada de dichos datos,*** generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa. |

***Exposición de motivos***

Un sistema de IA consiste en una combinación de elementos técnicos que vinculan datos, algoritmos y potencia de cálculo con determinadas prácticas sociales, la sociedad, la identidad y la cultura. La definición de este conjunto sociotécnico dinámico deberá, por tanto, estar preparada para el futuro y actualizarse periódicamente para reflejar de manera adecuada el impacto social cada vez mayor de la IA, al tiempo que se ponen de relieve con rapidez los retos y oportunidades asociados a la IA, incluido el vínculo entre la gestión del conocimiento y la IA. Los algoritmos desarrollados por otros algoritmos también deben estar sujetos al presente Reglamento.

**Enmienda 17**

Artículo 5, apartado 1

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Estarán prohibidas las siguientes prácticas de inteligencia artificial: | Estarán prohibidas las siguientes prácticas de inteligencia artificial: |
| 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 para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra. | 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 para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra***, vulnere o sea probable que vulnere los derechos fundamentales de otra persona o de un grupo de personas, en particular su salud e integridad física o psicológica, tenga o sea probable que tenga un efecto perjudicial para los consumidores, como pérdidas o discriminación económicas, o socave o sea probable que socave la democracia y el Estado de derecho***. |
| b) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra. | b) La introducción en el mercado, la puesta en servicio o la utilización de un sistema de IA que aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra. |

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| c) La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA por parte de las autoridades públicas o en su representación con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas***, de forma que la clasificación social resultante provoque una o varias de las situaciones siguientes:***<br>***i) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente;***<br>***ii) un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este.*** | c) La introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA por parte de las autoridades públicas o en su representación con el fin de evaluar o clasificar la fiabilidad de personas ***o de grupos de personas*** físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas***, que lleven a una calificación social con fines generales;*** |
| d) El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:<br>i) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos;<br>ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista;<br>iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI ([62]) del Consejo, para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro. | d) ***La introducción en el mercado, la puesta en servicio o la utilización, por parte de las autoridades públicas o en su representación, de sistemas de IA que hagan un uso de sistemas de calificación social sin control humano para fines específicos, es decir, en contextos sociales que guarden relación con los contextos donde se generaron o recabaron los datos originalmente, con el fin de evaluar o clasificar la fiabilidad de personas o de grupos de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas, de forma que la clasificación social resultante provoque un trato perjudicial o desfavorable hacia determinadas personas físicas o colectivos enteros que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este;*** |

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

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| | ***e)*** El uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley, salvo y en la medida en que dicho uso sea estrictamente necesario para alcanzar uno o varios de los objetivos siguientes:<br>i) la búsqueda selectiva de posibles víctimas concretas de un delito, incluidos menores desaparecidos;<br>ii) la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas o de un atentado terrorista;<br>iii) la detección, la localización, la identificación o el enjuiciamiento de la persona que ha cometido o se sospecha que ha cometido alguno de los delitos mencionados en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI ([62]) del Consejo, para el que la normativa en vigor en el Estado miembro implicado imponga una pena o una medida de seguridad privativas de libertad cuya duración máxima sea al menos de tres años, según determine el Derecho de dicho Estado miembro.<br>([62]) Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros (DO L 190 de 18.7.2002, p. 1). |

***Exposición de motivos***

En general, las técnicas subliminales pueden socavar la libertad, los derechos humanos y, por ende, el funcionamiento del Estado de Derecho democrático. Al mismo tiempo, la inteligencia artificial puede socavar los derechos de los consumidores. El objetivo de las adiciones propuestas es aclarar este aspecto.

Por lo que se refiere a la calificación social por las autoridades públicas o por encargo de estas, debe prohibirse si se lleva a cabo con fines generales, habida cuenta de los peligros derivados de tales prácticas, tal y como se explica en el considerando 17. La generación o recopilación de datos para fines específicos solo debe permitirse con supervisión humana y siempre que no viole el derecho a la dignidad y a la no discriminación ni los valores de igualdad y justicia.

**Enmienda 18**

Artículo 5, apartado 4

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| 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 aplicación de la ley dentro de los límites y en las condiciones que se indican en el apartado 1, letra d), y los apartados 2 y 3. A tal fin, tendrán que establecer en sus respectivos Derechos internos 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 de estas. Dichas normas especificarán también para cuáles de los objetivos enumerados en el apartado 1, letra d), y en su caso en relación con cuáles de los delitos indicados en su inciso iii), se podrá autorizar que las autoridades competentes utilicen esos sistemas con fines de aplicación de la ley. | 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 aplicación de la ley dentro de los límites y en las condiciones que se indican en el apartado 1, letra d), y los apartados 2 y 3. A tal fin, tendrán que establecer en sus respectivos Derechos internos 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 de estas. Dichas normas especificarán también para cuáles de los objetivos enumerados en el apartado 1, letra d), y en su caso en relación con cuáles de los delitos indicados en su inciso iii), se podrá autorizar que las autoridades competentes utilicen esos sistemas con fines de aplicación de la ley. ***Tales normas establecen, además, las modalidades de información y consulta de los entes locales y regionales afectados. Deberá efectuarse esta consulta antes de recurrir de manera excepcional a estos sistemas en los espacios públicos. En situaciones de emergencia en las que no quepa esperar razonablemente una consulta previa, el ente local o regional afectado deberá ser informado inmediatamente del despliegue de la aplicación de IA de que se trate.*** |

***Exposición de motivos***

La responsabilidad política y administrativa de la gestión y la vigilancia de los espacios públicos incumbe a los entes locales y regionales. Por lo tanto, deben tener voz antes del despliegue de tales aplicaciones de IA y estar debidamente informados sobre el recurso excepcional a sistemas de IA con fines coercitivos.

En situaciones de emergencia en las que no quepa esperar razonablemente una consulta previa, el ente local o regional afectado deberá ser informado inmediatamente.

**Enmienda n.º 19**

Artículo 13

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Artículo ***13*** — Transparencia y comunicación de información a los usuarios | Artículo ***13a*** — Transparencia y comunicación de información a los usuarios |
| 1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida. Se garantizará un tipo y un nivel de transparencia ***adecuados*** para que el usuario y el proveedor cumplan las obligaciones oportunas previstas en el capítulo 3 del presente título. | 1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida. Se garantizará un tipo y un nivel ***adecuados*** de transparencia ***y de explicación comprensible*** para que el usuario y el proveedor cumplan las obligaciones oportunas previstas en el capítulo 3 del presente título. ***Esta explicación se facilitará al menos en la lengua del país en el que se despliegue el sistema de IA.*** |

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| 2. Los sistemas de IA de alto riesgo irán acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado***, las cuales*** incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios. | 2. Los sistemas de IA de alto riesgo irán acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado***. Las instrucciones serán públicas, comprensibles y accesibles para todos e*** incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios. |
| 3. La información a que se refiere el apartado 2 especificará: | 3. La información a que se refiere el apartado 2 especificará: |
| a) la identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado; | a) la identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado; |
| b) las características, capacidades y limitaciones del funcionamiento del sistema de IA de alto riesgo, y en particular: | b) las características, capacidades y limitaciones del funcionamiento del sistema de IA de alto riesgo, y en particular: |
| i) su finalidad prevista; | i) su finalidad prevista; |
| ii) el nivel de precisión, solidez y ciberseguridad mencionado en el artículo 15 con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y que puede esperarse de este, así como las circunstancias conocidas o previsibles que podrían afectar al nivel de precisión, solidez y ciberseguridad esperado; | ii) el nivel de precisión ***(expresada mediante parámetros adecuados para la evaluación de modelos)***, solidez y ciberseguridad mencionado en el artículo 15 con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y que puede esperarse de este, así como las circunstancias conocidas o previsibles que podrían afectar al nivel de precisión, solidez y ciberseguridad esperado; |
| iii) cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales; | iii) cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales; |
| iv) su funcionamiento en relación con las personas o los grupos de personas en relación con los que se pretenda utilizar el sistema; | iv) su funcionamiento en relación con las personas o los grupos de personas en relación con los que se pretenda utilizar el sistema; |
| v) cuando proceda, especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA; | v) cuando proceda, especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA; |
| | ***vi) los parámetros utilizados para generar el modelo y las medidas adoptadas para evitar sobreajuste o un ajuste insuficiente;*** |

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| c) los cambios en el sistema de IA de alto riesgo y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso; | c) los cambios en el sistema de IA de alto riesgo y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso; |
| d) las medidas de vigilancia humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de la información de salida de los sistemas de IA por parte de los usuarios; | d) las medidas de vigilancia humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de la información de salida de los sistemas de IA por parte de los usuarios; |
| e) la vida útil prevista del sistema de IA de alto riesgo, así como las medidas de mantenimiento y cuidado necesarias para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a la actualización del software. | e) la vida útil prevista del sistema de IA de alto riesgo, así como las medidas de mantenimiento y cuidado necesarias para garantizar el correcto funcionamiento de dicho sistema, también en lo que respecta a la actualización del software. |
| | ***Artículo 13b — Transparencia e información de las personas afectadas*** |
| | ***Las personas o grupos de personas que puedan verse afectados por un sistema de IA de alto riesgo serán informados de manera adecuada, fácilmente accesible y comprensible, y deben poder encontrar información pública de manera fácilmente accesible, adecuada y comprensible sobre el hecho de que están sometidos a dichos sistemas.*** |

***Exposición de motivos***

Con el fin de reforzar el ecosistema de confianza, deben ponerse a disposición del público instrucciones para el uso de sistemas de IA de alto riesgo. Estas instrucciones deben redactarse de manera comprensible, en la lengua del país en el que se implante el sistema de IA.

En pro de la transparencia y la comprensión de los algoritmos, debe ser posible explicar qué parámetros se han utilizado para generar el modelo y qué medidas se han adoptado para evitar un sobreajuste o un ajuste insuficiente.

El artículo 13b regula la obligación de transparencia e información que incumbe a las personas que interactúan con sistemas de IA o que podrían verse afectadas por un sistema de IA.

**Enmienda 20**

Artículo 14, apartado 4

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Las medidas mencionadas en el apartado 3 permitirán que las personas a quienes se encomiende la vigilancia humana puedan, en función de las circunstancias: | Las medidas mencionadas en el apartado 3 permitirán que las personas a quienes se encomiende la vigilancia humana puedan, en función de las circunstancias: |
| a) entender por completo las capacidades y limitaciones del sistema de IA de alto riesgo y controlar debidamente su funcionamiento, de modo que puedan detectar indicios de anomalías, problemas de funcionamiento y comportamientos inesperados y ponerles solución lo antes posible; | a) entender por completo las capacidades y limitaciones del sistema de IA de alto riesgo y controlar debidamente su funcionamiento, de modo que puedan detectar indicios de anomalías, problemas de funcionamiento y comportamientos inesperados y ponerles solución lo antes posible; |

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en la información de salida generada por un sistema de IA de alto riesgo («sesgo de automatización»), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión; | b) ser conscientes de la posible tendencia a confiar automáticamente o en exceso en la información de salida generada por un sistema de IA de alto riesgo («sesgo de automatización») ***o de cualquier otro tipo de sesgo***, en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión; |
| c) interpretar correctamente la información de salida del sistema de IA de alto riesgo, teniendo en cuenta en particular las características del sistema y las herramientas y los métodos de interpretación disponibles; | c) interpretar correctamente la información de salida del sistema de IA de alto riesgo, teniendo en cuenta en particular las características del sistema y las herramientas y los métodos de interpretación disponibles; |
| d) decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o desestimar, invalidar o revertir la información de salida que este genere; | d) decidir, en cualquier situación concreta, no utilizar el sistema de IA de alto riesgo o desestimar, invalidar o revertir la información de salida que este genere; |
| e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema accionando un botón específicamente destinado a tal fin o mediante un procedimiento similar. | e) intervenir en el funcionamiento del sistema de IA de alto riesgo o interrumpir el sistema accionando un botón específicamente destinado a tal fin o mediante un procedimiento similar. |

***Exposición de motivos***

Existen varios tipos de sesgo que pueden resultar problemáticos. Cabe citar como ejemplo el sesgo del diseñador o del propio usuario («sesgo social»), el sesgo en cuanto a si el sistema de IA implantado es una solución adecuada al problema («sesgo tecnológico») y los diferentes tipos de sesgos estadísticos.

**Enmienda 21**

Artículo 14, nuevo apartado tras el apartado 5

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| | ***Toda decisión adoptada por los sistemas de IA a que se refiere el anexo III, punto 5, letras a) y b), estará sujeta a intervención humana y se basará en un proceso de toma de decisiones riguroso. Debe garantizarse un contacto humano con estas decisiones.*** |

***Exposición de motivos***

El artículo 14 se refiere únicamente al control de los sistemas de IA de alto riesgo por parte de los seres humanos. Por lo que se refiere a las decisiones adoptadas por las autoridades públicas, es importante subrayar que deben garantizarse la intervención humana y el contacto y el respeto de los procedimientos.

**Enmienda 22**

Artículo 17, apartado 1 — añádanse dos letras después de la letra m)

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Los proveedores de sistemas de IA de alto riesgo establecerán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento. Dicho sistema se documentará de manera sistemática y ordenada mediante políticas, procedimientos e instrucciones escritas e incluirá, al menos, los siguientes aspectos: | Los proveedores de sistemas de IA de alto riesgo establecerán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento. Dicho sistema se documentará de manera sistemática y ordenada mediante políticas, procedimientos e instrucciones escritas e incluirá, al menos, los siguientes aspectos: |
| a) una estrategia para el cumplimiento reglamentario, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y de los procedimientos de gestión de las modificaciones de los sistemas de IA de alto riesgo; | a) una estrategia para el cumplimiento reglamentario, incluido el cumplimiento de los procedimientos de evaluación de la conformidad y de los procedimientos de gestión de las modificaciones de los sistemas de IA de alto riesgo; |
| b) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el diseño y el control y la verificación del diseño del sistema de IA de alto riesgo; | b) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el diseño y el control y la verificación del diseño del sistema de IA de alto riesgo; |
| c) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el desarrollo y el control y el aseguramiento de la calidad del sistema de IA de alto riesgo; | c) las técnicas, los procedimientos y las actuaciones sistemáticas que se utilizarán en el desarrollo y el control y el aseguramiento de la calidad del sistema de IA de alto riesgo; |
| d) los procedimientos de examen, prueba y validación que se llevarán a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, así como la frecuencia con que tendrán lugar; | d) los procedimientos de examen, prueba y validación que se llevarán a cabo antes, durante y después del desarrollo del sistema de IA de alto riesgo, así como la frecuencia con que tendrán lugar; |
| e) las especificaciones técnicas, incluidas las normas, que se aplicarán y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad, los medios que se utilizarán para velar por que el sistema de IA de alto riesgo cumpla los requisitos establecidos en el capítulo 2 del presente título; | e) las especificaciones técnicas, incluidas las normas, que se aplicarán y, cuando las normas armonizadas pertinentes no se apliquen en su totalidad, los medios que se utilizarán para velar por que el sistema de IA de alto riesgo cumpla los requisitos establecidos en el capítulo 2 del presente título; |
| f) los sistemas y procedimientos de gestión de datos, lo que incluye su recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con ese fin; | f) los sistemas y procedimientos de gestión de datos, lo que incluye su recopilación, análisis, etiquetado, almacenamiento, filtrado, prospección, agregación, conservación y cualquier otra operación relacionada con los datos que se lleve a cabo antes de la introducción en el mercado o puesta en servicio de sistemas de IA de alto riesgo y con ese fin; |
| g) el sistema de gestión de riesgos que se menciona en el artículo 9; | g) el sistema de gestión de riesgos que se menciona en el artículo 9; |
| h) el establecimiento, la implantación y el mantenimiento de un sistema de seguimiento posterior a la comercialización con arreglo al artículo 61; | h) el establecimiento, la implantación y el mantenimiento de un sistema de seguimiento posterior a la comercialización con arreglo al artículo 61; |

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| i) los procedimientos asociados a la notificación de incidentes graves y defectos de funcionamiento con arreglo al artículo 62; | i) los procedimientos asociados a la notificación de incidentes graves y defectos de funcionamiento con arreglo al artículo 62; |
| j) la gestión de la comunicación con las autoridades nacionales competentes; las autoridades competentes, incluidas las sectoriales, que permiten acceder a datos o facilitan el acceso a ellos; los organismos notificados; otros operadores; | j) la gestión de la comunicación con las autoridades nacionales competentes; las autoridades competentes, incluidas las sectoriales, que permiten acceder a datos o facilitan el acceso a ellos; los organismos notificados; otros operadores; |
| k) los sistemas y procedimientos destinados a llevar un registro de toda la documentación e información pertinente; | k) los sistemas y procedimientos destinados a llevar un registro de toda la documentación e información pertinente; |
| l) la gestión de los recursos, incluida la seguridad de las medidas relacionadas con el suministro; | l) la gestión de los recursos, incluida la seguridad de las medidas relacionadas con el suministro; |
| m) un marco de rendición de cuentas que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado. | m) un marco de rendición de cuentas que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado; |
| | ***n) medidas destinadas a evitar cualquier discriminación injustificada por motivos de sexo, origen étnico, religión o convicciones, discapacidad, edad, orientación sexual o cualquier otra razón;*** |
| | ***o) una explicación de cómo se han tenido en cuenta determinados valores éticos específicos a la hora de diseñar el sistema de IA de alto riesgo.*** |

***Exposición de motivos***

Esta adición subraya que la inclusión y la lucha contra las discriminaciones injustificadas deben ser elementos destacados del sistema de gestión de la calidad.

El sistema debe respetar los valores éticos que un usuario del sistema de IA aspira a asociar a este o cuyo proveedor puede razonablemente aspirar a que se asocien a un sistema de IA de alto riesgo. El proveedor debe poder explicar cómo ha tenido en cuenta dichos valores.

**Enmienda 23**

Artículo 19, apartado 1

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Los proveedores de sistemas de IA de alto riesgo se asegurarán de que sus sistemas sean sometidos al procedimiento de evaluación de la conformidad oportuno, de conformidad con el artículo 43, antes de su introducción en el mercado o puesta en servicio. Cuando dicha evaluación de la conformidad demuestre que los sistemas de IA cumplen los requisitos establecidos en el capítulo 2 del presente título, sus proveedores elaborarán una declaración UE de conformidad con arreglo al artículo 48 y colocarán el marcado CE de conformidad con arreglo al artículo 49. | Los proveedores de sistemas de IA de alto riesgo se asegurarán de que sus sistemas sean sometidos al procedimiento de evaluación de la conformidad oportuno, de conformidad con el artículo 43, antes de su introducción en el mercado o puesta en servicio. Cuando dicha evaluación de la conformidad demuestre que los sistemas de IA cumplen los requisitos establecidos en el capítulo 2 del presente título, sus proveedores elaborarán una declaración UE de conformidad con arreglo al artículo 48 y colocarán el marcado CE de conformidad con arreglo al artículo 49. ***Los proveedores de sistemas de IA de alto riesgo publicarán en un lugar de acceso público la declaración UE de conformidad y un resumen de la evaluación de la conformidad.*** |

***Exposición de motivos***

Con el fin de reforzar el ecosistema de confianza en los sistemas de IA, los proveedores de sistemas de IA de alto riesgo deben hacer gala de transparencia. Por consiguiente, el público debe poder comprobar que la evaluación de la conformidad se ha realizado correctamente con arreglo a lo dispuesto en el Reglamento.

**Enmienda 24**

Artículo 29, nuevo apartado tras el apartado 6

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| | ***Los usuarios de sistemas de IA de alto riesgo deberán llevar a cabo una evaluación ética antes de poner en funcionamiento el sistema. Deberán ser capaces de explicar el posible impacto del despliegue de la tecnología para los particulares y la sociedad. Especificarán la finalidad para la que se despliega el sistema de IA, los valores fundamentales que entraña y la manera en que se han determinado. También especificarán si esos valores se han tenido o no en cuenta en el sistema. Evaluarán el impacto real del sistema en las personas y la sociedad a lo largo de todo el ciclo de vida del sistema de IA.*** |

***Exposición de motivos***

La ética es un concepto amplio. Existen muchas maneras de poner en práctica la ética en el ámbito de la tecnología, tanto en términos de justificaciones teóricas como de metodologías, herramientas y valores de diseño concretos. Los valores son elementos considerados importantes por determinadas personas o grupos de personas; pueden ser más bien concretos o más conceptuales. Es importante preservar la gama de valores morales que pueden aplicarse y evaluar continuamente el ciclo de vida del sistema de IA.

**Enmienda 25**

Artículo 52, apartado 1

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Los proveedores garantizarán que los sistemas de IA destinados a interactuar con personas físicas estén diseñados y desarrollados de forma que dichas personas estén informadas de que están interactuando con un sistema de IA***, excepto en las situaciones en las que esto resulte evidente debido a las circunstancias y al contexto de utilización***. Esta obligación no se aplicará a los sistemas de IA autorizados por la ley para fines de detección, prevención, investigación o enjuiciamiento de infracciones penales, salvo que estos sistemas estén a disposición del público para denunciar una infracción penal. | Los proveedores garantizarán que los sistemas de IA destinados a interactuar con personas físicas estén diseñados y desarrollados de forma que dichas personas estén informadas de que están interactuando con un sistema de IA. Esta obligación no se aplicará a los sistemas de IA autorizados por la ley para fines de detección, prevención, investigación o enjuiciamiento de infracciones penales, salvo que estos sistemas estén a disposición del público para denunciar una infracción penal. ***El abanico de opciones y el estatuto jurídico de las personas físicas que interactúan con sistemas de IA no deben verse limitados por esta interacción.*** |

***Exposición de motivos***

Cuando se utilicen artefactos tecnológicos como medio de interacción con personas físicas, puede existir el riesgo de que las decisiones tomadas por las personas físicas que interactúan con dichos artefactos sean limitadas. Las personas físicas deben ser debidamente informadas siempre que estén expuestas a sistemas de IA, sin que ello pueda estar sujeto a la interpretación de una situación concreta. Sus derechos deben garantizarse en todo momento en las interacciones con los sistemas de IA.

**Enmienda 26**

Artículo 57, apartado 1

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| El Comité estará compuesto por las autoridades nacionales de supervisión, que estarán representadas por el jefe de dicha autoridad o un funcionario de alto nivel equivalente, y el Supervisor Europeo de Protección de Datos. Se podrá invitar a otras autoridades nacionales a las reuniones, cuando los temas tratados sean de relevancia para ellas. | El Comité estará compuesto por las autoridades nacionales de supervisión, que estarán representadas por el jefe de dicha autoridad o un funcionario de alto nivel equivalente, y el Supervisor Europeo de Protección de Datos. Se podrá invitar a otras autoridades nacionales***, regionales y locales*** a las reuniones, cuando los temas tratados sean de relevancia para ellas. |

***Exposición de motivos***

Los entes locales y regionales deberían poder participar en el seguimiento de los sistemas basados en la IA y rendir cuentas de su implantación sobre el terreno.

**Enmienda 27**

Artículo 58

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Cuando preste asesoramiento y asistencia a la Comisión en el contexto del artículo 56, apartado 2, el Comité, en particular: | Cuando preste asesoramiento y asistencia a la Comisión en el contexto del artículo 56, apartado 2, el Comité, en particular: |
| a) recopilará y compartirá conocimientos técnicos y buenas prácticas entre los Estados miembros; | a) recopilará y compartirá conocimientos técnicos y buenas prácticas entre los Estados miembros ***y los entes regionales o locales***; |
| b) contribuirá a uniformizar las prácticas administrativas en los Estados miembros, incluidas las relativas al funcionamiento de los espacios controlados de pruebas a que se refiere el artículo 53; | b) contribuirá a uniformizar las prácticas administrativas en los Estados miembros, incluidas las relativas al funcionamiento de los espacios controlados de pruebas a que se refiere el artículo 53; |
| c) emitirá dictámenes, recomendaciones o contribuciones por escrito sobre cuestiones relacionadas con la aplicación del presente Reglamento, en particular: | c) emitirá dictámenes, recomendaciones o contribuciones por escrito sobre cuestiones relacionadas con la aplicación del presente Reglamento, en particular: |
| i) sobre especificaciones técnicas o normas existentes relativas a los requisitos establecidos en el título III, capítulo 2; | i) sobre especificaciones técnicas o normas existentes relativas a los requisitos establecidos en el título III, capítulo 2; |
| ii) sobre el uso de normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41; | ii) sobre el uso de normas armonizadas o especificaciones comunes a que se refieren los artículos 40 y 41; |
| iii) sobre la preparación de documentos de orientación, incluidas las directrices relativas a la fijación de multas administrativas a que se refiere el artículo 71. | iii) sobre la preparación de documentos de orientación, incluidas las directrices relativas a la fijación de multas administrativas a que se refiere el artículo 71. |

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|

***Exposición de motivos***

Los entes locales y regionales son los más cercanos a las ciudadanos y las economías locales y deben ocupar explícitamente un lugar destacado a la hora de compartir conocimientos.

**Enmienda 28**

Artículo 59, apartado 1

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Cada Estado miembro establecerá o designará autoridades nacionales competentes con el fin de garantizar la aplicación y ejecución del presente Reglamento. Las autoridades nacionales competentes se organizarán de manera que se preserve la objetividad e imparcialidad de sus actividades y funciones. | Cada Estado miembro establecerá o designará autoridades nacionales competentes con el fin de garantizar la aplicación y ejecución del presente Reglamento. Las autoridades nacionales competentes se organizarán de manera que se preserve la objetividad e imparcialidad de sus actividades y funciones. ***Se facultará a los entes locales y regionales para llevar a cabo tareas de supervisión o ejecución cuando un Estado miembro lo considere oportuno.*** |

***Exposición de motivos***

A efectos de la aplicabilidad del Reglamento y sus disposiciones de supervisión y ejecución, los Estados miembros deberán poder encomendar tareas de supervisión o ejecución a los entes locales y regionales cuando sea necesario y en la medida de lo posible. En este contexto, los entes locales y regionales deben recibir apoyo y formación a fin de estar plenamente facultados para llevar a cabo tareas de supervisión o ejecución.

**Enmienda 29**

Artículo 69, apartado 3

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Los códigos de conducta podrán ser elaborados por proveedores individuales de sistemas de IA, por organizaciones que los representen o por ambos, también con la participación de usuarios y de cualquier parte interesada y sus organizaciones representativas. Los códigos de conducta podrán abarcar uno o varios sistemas de IA, teniendo en cuenta la similitud de la finalidad prevista de los sistemas pertinentes. | Los códigos de conducta podrán ser elaborados ***por autoridades nacionales, regionales o locales,*** por proveedores individuales de sistemas de IA, por organizaciones que los representen o por ambos, también con la participación de usuarios y de cualquier parte interesada y sus organizaciones representativas. Los códigos de conducta podrán abarcar uno o varios sistemas de IA, teniendo en cuenta la similitud de la finalidad prevista de los sistemas pertinentes. |

***Exposición de motivos***

Las autoridades nacionales, locales y regionales deben estar facultadas legalmente para elaborar códigos de conducta sobre los sistemas de IA que desarrollen o utilicen.

**Enmienda 30**

Anexo I — Técnicas y estrategias de inteligencia artificial mencionadas en el artículo 3, punto 1

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| | ***Habida cuenta del estado actual de la ciencia, la IA abarca las técnicas y estrategias siguientes:*** |
| a) Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo. | a) Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo. |
| b) Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico). | b) Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico). |
| c) Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización. | c) Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización. |

***Exposición de motivos***

La definición y la lista de técnicas de IA deben estar preparadas para el futuro. La lista de técnicas y estrategias específicas utilizadas para el desarrollo de sistemas de IA no debe ser exhaustiva y debe quedar claro que se basa en el estado actual de la ciencia.

**Enmienda 31**

Anexo III, puntos 1 a 5

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| Los sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 2, son los sistemas de IA mencionados en cualquiera de los ámbitos siguientes: | Los sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 2, son los sistemas de IA mencionados en cualquiera de los ámbitos siguientes: |
| 1. Identificación biométrica y categorización de personas físicas: | 1. Identificación biométrica y categorización de personas físicas: |
| a) sistemas de IA destinados a utilizarse en la identificación biométrica remota «en tiempo real» o «en diferido» de personas físicas. | a) sistemas de IA destinados a utilizarse en la identificación biométrica remota «en tiempo real» o «en diferido» de personas físicas. |
| 2. Gestión y funcionamiento de infraestructuras esenciales: | 2. Gestión y funcionamiento de infraestructuras esenciales: |
| a) sistemas de IA destinados a utilizarse como componentes de seguridad en la gestión y funcionamiento del tráfico rodado y el suministro de agua, gas, calefacción y electricidad. | a) sistemas de IA destinados a utilizarse como componentes de seguridad en la gestión y funcionamiento del tráfico rodado y el suministro de agua, gas, calefacción y electricidad***, así como en las infraestructuras de telecomunicaciones, de distribución de agua y de internet***. |

| Texto de la Comisión Europea | Enmienda del CDR |
|---|---|
| 3. Educación y formación profesional: | 3. Educación y formación profesional: |
| a) sistemas de IA destinados a utilizarse para determinar el acceso o la asignación de personas físicas a los centros de educación y formación profesional; | a) sistemas de IA destinados a utilizarse para determinar el acceso o la asignación de personas físicas a los centros de educación y formación profesional; |
| b) sistemas de IA destinados a utilizarse para evaluar a los estudiantes de centros de educación y formación profesional y para evaluar a los participantes en pruebas generalmente necesarias para acceder a centros de educación. | b) sistemas de IA destinados a utilizarse para evaluar a los estudiantes de centros de educación y formación profesional y para evaluar a los participantes en pruebas generalmente necesarias para acceder a centros de educación. |
| 4. Empleo, gestión de los trabajadores y acceso al autoempleo: | 4. Empleo, gestión de los trabajadores y acceso al autoempleo: |
| a) sistemas de IA destinados a utilizarse para la contratación o selección de personas físicas, especialmente para anunciar puestos vacantes, clasificar y filtrar solicitudes o evaluar a candidatos en el transcurso de entrevistas o pruebas; | a) sistemas de IA destinados a utilizarse para la contratación o selección de personas físicas, especialmente para anunciar puestos vacantes, clasificar y filtrar solicitudes o evaluar a candidatos en el transcurso de entrevistas o pruebas; |
| b) IA destinada a utilizarse para tomar decisiones relativas a la promoción y resolución de relaciones contractuales de índole laboral, a la asignación de tareas y al seguimiento y evaluación del rendimiento y la conducta de las personas en el marco de dichas relaciones. | b) IA destinada a utilizarse para tomar decisiones relativas a la promoción y resolución de relaciones contractuales de índole laboral, a la asignación de tareas y al seguimiento y evaluación del rendimiento y la conducta de las personas en el marco de dichas relaciones. |
| 5. Acceso y disfrute de servicios públicos y privados esenciales y sus beneficios: | 5. Acceso y disfrute de servicios públicos y privados esenciales y sus beneficios: |
| a) sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para ***evaluar*** la admisibilidad de las personas físicas para acceder a prestaciones y servicios de asistencia pública, así como para conceder, reducir, retirar o recuperar dichas prestaciones y servicios; | a) sistemas de IA destinados a ser utilizados por las autoridades públicas o en su nombre para ***evaluar y decidir sobre*** la admisibilidad de las personas físicas para acceder a prestaciones y servicios de asistencia pública, así como para conceder, reducir, retirar o recuperar dichas prestaciones y servicios; |
| b) sistemas de IA destinados a utilizarse para ***evaluar*** la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA puestos en servicio por parte de proveedores a pequeña escala para su uso propio; | b) sistemas de IA destinados a utilizarse para ***determinar*** la solvencia de personas físicas o establecer su calificación crediticia, salvo los sistemas de IA puestos en servicio por parte de proveedores a pequeña escala para su uso propio; |
| c) sistemas de IA destinados a utilizarse para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, por ejemplo bomberos y servicios de asistencia médica. | c) sistemas de IA destinados a utilizarse para el envío o el establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia, por ejemplo bomberos y servicios de asistencia médica. |

***Exposición de motivos***

Las infraestructuras de telecomunicaciones, agua e internet figuran entre las infraestructuras críticas.

La clasificación de un sistema de IA como sistema de alto riesgo equivale a decidir si tal sistema puede suponer un riesgo real para los ciudadanos. La mera evaluación analítica y teórica de la admisibilidad de las personas físicas para acceder a prestaciones y servicios públicos no entraña en sí misma un alto riesgo. Complementar el verbo «evaluar» con «decidir sobre» subraya que este riesgo aparece efectivamente al adoptar la decisión, en particular para las personas afectadas.

II. **RECOMENDACIONES POLÍTICAS**

EL COMITÉ EUROPEO DE LAS REGIONES

**Un ecosistema de excelencia**

1. subraya que la ambición de la Comisión de convertir la UE en líder mundial del desarrollo responsable, centrado en el ser humano, de la inteligencia artificial (IA) solo puede lograrse si los entes locales y regionales ocupan una posición sólida en el proceso. Estos son los mejor situados para contribuir a la creación de un entorno que favorezca el aumento de la inversión en la IA durante los próximos años y extender la confianza en esta tecnología;

2. destaca que, además de impulsar la participación de los entes locales y regionales, es importante proporcionar apoyo y formación para mejorar sus capacidades en este ámbito, especialmente porque pueden encomendárseles funciones de supervisión y ejecución;

3. observa que habrá disponibles fondos de la Unión para el desarrollo de la inteligencia artificial, pero llama la atención sobre la fragmentación del enfoque debido a la diversidad de programas, lo que aumenta el riesgo de dispersión y solapamiento;

4. por lo tanto, pide a la Comisión que desarrolle y conecte espacios de datos comunes sólidos y polifacéticos que permitan resolver el tratamiento de casos de uso social mediante datos públicos y privados. Esto requiere, en particular, la armonización con las iniciativas legislativas de la Estrategia Europea de Datos;

**Un ecosistema de confianza**

5. lamenta que la propuesta de Reglamento no evoque los entes locales y regionales, aunque el marco jurídico se aplique a los agentes tanto públicos como privados;

6. señala en ese sentido que los sistemas de IA pueden desempeñar un papel importante para los entes locales y regionales en la interacción con la ciudadanía y la prestación de servicios. Además, los sistemas de IA ofrecen la posibilidad, entre otras, de mejorar la eficiencia del sector público y ayudar a los entes locales y regionales a realizar las adaptaciones necesarias a nivel local y regional en el contexto de las transiciones ecológica y digital. Por ello es importante que la experiencia de los entes locales y regionales se aproveche activamente en la revisión en curso del Reglamento;

7. pide una definición más precisa de «proveedor» y «usuario», especialmente en situaciones en las que las empresas, los institutos de investigación, las autoridades públicas y la ciudadanía desarrollan y prueban conjuntamente sistemas de IA en «laboratorios vivientes». También debe prestarse la debida atención a los ciudadanos o consumidores afectados por decisiones basadas en IA de los sistemas empleados por usuarios profesionales;

8. subraya la necesidad de consultar previamente a los entes locales y regionales afectados cuando se recurra a sistemas de inteligencia artificial para la identificación biométrica de las personas físicas en tiempo real y a distancia, con fines coercitivos, en zonas accesibles al público;

9. acoge con satisfacción la consulta pública de la Comisión Europea sobre la adaptación de las normas de responsabilidad civil a los retos específicos de la era digital y la inteligencia artificial ([1]) y confía que esto se traduzca en un marco actualizado que permita garantizar la reparación de los daños causados por las aplicaciones de IA a los consumidores;

10. se pregunta por qué los sistemas de IA utilizados en procesos democráticos, como las elecciones, no están incluidos en la lista de sistemas de IA de alto riesgo;

11. insta a que los sistemas de IA de alto riesgo estén sujetos a los mismos requisitos de transparencia e información para las personas físicas que los que se aplican actualmente a los usuarios;

12. observa que recurrir a calificaciones sociales conlleva importantes riesgos y repercusiones en materia de derechos humanos;

13. en este contexto, expresa gran escepticismo en relación con las dos situaciones descritas en el Reglamento ([2]) para determinar cuándo una calificación social hace que se dispense un trato perjudicial o desfavorable de personas o grupos de personas, ya que es extremadamente difícil comprobar la existencia de tales situaciones. En este contexto, el Comité insta a que se formulen claramente salvaguardias sólidas para garantizar que no se eluda la prohibición de las prácticas de clasificación social;

([1]) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation_es.

([2]) Artículo 5, apartado 1, letra c).

14. acoge con satisfacción que los considerandos del Reglamento aborden en detalle los riesgos a los que están expuestas las personas físicas como resultado de su interacción con sistemas de IA de alto riesgo, en particular en el contexto de la enseñanza, la formación, el empleo, la gestión de los recursos humanos, el acceso al trabajo por cuenta propia o el acceso y el derecho a determinados servicios públicos y privados esenciales;

15. pide a la Comisión que examine más detenidamente la clasificación de alto riesgo de los sistemas de IA destinados a ser utilizados por las autoridades públicas ([3]);

16. aspira a que una autoridad se pronuncie *ex ante* de manera sustancial sobre la interpretación de las disposiciones del Reglamento, en particular en relación con el Reglamento General de Protección de Datos, lo que reforzará la seguridad jurídica y reducirá los costes de diseño y puesta en práctica de sistemas de IA;

17. subraya a tal efecto la importancia de la claridad en la formulación del Reglamento, que es fundamental para crear un ecosistema de confianza y despejar la inseguridad jurídica en torno al desarrollo y la utilización de sistemas de IA. De este modo se evitarían interpretaciones erróneas de los requisitos propuestos y se reducirían al mínimo los riesgos de una posterior mala gestión de las aplicaciones de IA, maximizando así la eficacia del Reglamento y la credibilidad de las sanciones. Al mismo tiempo, y en consonancia con el programa de mejora de la legislación de la Comisión Europea, es de suma importancia detectar precozmente posibles solapamientos o conflictos con la normativa existente y eliminarlos;

18. constata que numerosos entes locales y regionales utilizan los mismos sistemas de IA para realizar tareas similares. En la gran mayoría de los casos, estos sistemas son diseñados por empresas privadas;

19. señala que la propuesta de Reglamento no es un elemento aislado en lo que respecta a la garantía de los derechos de los ciudadanos, sino que debe considerarse en relación con la legislación vigente. Por consiguiente, se invita a los Estados miembros a garantizar de forma continuada las medidas administrativas necesarias para responder a las oportunidades y los riesgos asociados al uso de la IA en el sector público;

20. de ello se desprende que son las empresas y los organismos notificados los que interpretan las normas europeas y nacionales en el contexto de la evaluación de la conformidad y que, por lo tanto, esta interpretación se refleja en la práctica de los entes locales y regionales que utilizan estos sistemas de IA. Por ello, no está claro en qué medida estos sistemas de IA pueden tener en cuenta la política local. El Comité hace hincapié en las necesidades específicas de los entes locales y regionales y señala que aplicar el mismo enfoque en todos los casos puede socavar la eficacia de los sistemas de IA a la hora de responder a esas necesidades. Sugiere también que se faculte a los Estados miembros para regular los sistemas de IA de alto riesgo por motivos imperiosos y justificados de interés público;

21. a este respecto, pide que las evaluaciones de la conformidad sean transparentes y estén a disposición del público. Por otra parte, los entes locales y regionales deberían también poder participar en la supervisión de los sistemas basados en la IA, rendir cuentas de su implantación sobre el terreno y contribuir formalmente a la evaluación, por parte de la Comisión Europea, de la aplicación del Reglamento;

22. subraya que deben crearse las condiciones jurídicas, metodológicas y éticas adecuadas para la puesta en práctica de un entorno controlado de pruebas que permita el desarrollo de la tecnología, la elaboración de la legislación y su evaluación. Además, deben establecerse criterios claros para que las empresas puedan hacer uso del referido entorno controlado de pruebas; Para garantizar que las organizaciones de consumidores puedan hacer cumplir las disposiciones de la Ley de Inteligencia Artificial, esta última debe añadirse en el anexo I de la Directiva (UE) 2020/1828 relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores;

**Campañas de información**

23. destaca la importancia de las campañas públicas, de modo que el público en general esté informado y familiarizado con la existencia y utilidad de los sistemas de IA, así como con los posibles riesgos. Subraya además la importancia fundamental de una información exhaustiva para los consumidores en el ámbito de la inteligencia artificial y la toma de decisiones impulsada por máquinas. Pide, a tal efecto, a la Comisión Europea que asigne recursos financieros para estas campañas;

([3]) Anexo III, punto 5, letra a).

**Carga administrativa**

24. expresa su preocupación por la posible carga administrativa que puede conllevar la propuesta de Reglamento. La carga administrativa puede impedir que las pequeñas y medianas empresas y los entes locales y regionales promuevan la innovación e implanten sistemas de IA ([4]);

**Proporcionalidad y subsidiariedad**

25. considera que el proyecto de Reglamento se ajusta a los principios de proporcionalidad y subsidiariedad. El valor añadido de la actuación de la UE en este ámbito y los fundamentos jurídicos pertinentes que ha elegido la Comisión son claros y coherentes. La evaluación de impacto incluyó una sección específica sobre subsidiariedad. Además, ningún Parlamento nacional ha emitido dictámenes motivados sobre el incumplimiento del principio de subsidiariedad durante el plazo estipulado, que expiró el 2 de septiembre de 2021.

Bruselas, 2 de diciembre de 2021.

*El Presidente*
*del Comité Europeo de las Regiones*

Apostolos TZITZIKOSTAS

([4]) En un estudio encargado recientemente por la Comisión Europea *(Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, p. 12)* se considera que, sobre la base de hipótesis razonables, el coste medio de la obtención de la certificación de un sistema de IA podría oscilar entre 16 800 y 23 000 EUR, es decir, entre un 10 % y un 14 % de sus costes de desarrollo.