INTELIGENCIA ARTIFICIAL (IA) PROPUESTA DE REGULACIÓN DE LA UNIÓN EUROPEA (UE)

Modificaciones necesarias para proteger a las personas consumidoras

Funded by the European Union

Esta publicación forma parte de una actividad que ha recibido financiación del Programa de la Unión Europea para los Consumidores (2020-2025) bajo una subvención de funcionamiento. El contenido de esta publicación representa únicamente las opiniones del autor bajo su exclusiva responsabilidad. La Comisión Europea no asume responsabilidad alguna por el uso que pueda hacerse de la información contenida en él.

cecu

RESUMEN DE CUESTIONES A MEJORAR

Una adecuada regulación de la IA es crucial para garantizar un alto nivel de protección a las personas consumidoras, así como un entorno justo, seguro y confiable en el que se asegure el desarrollo sostenible de nuestras sociedades.

CECU celebra la propuesta de Reglamento de la IA actualmente en debate a nivel europeo. Sin embargo, el proyecto de regulación requiere de importantes mejoras para garantizar que las personas consumidoras se encuentren adecuadamente protegidas y puedan confiar en que la IA respeta sus derechos y libertades. A tal fin, se entiende necesario que el futuro Reglamento de IA incluya las siguientes mejoras:

(i) debe ampliarse el ámbito de aplicación del Reglamento e imponerse una serie de principios y obligaciones horizontales (equidad, transparencia, rendición de cuentas, entre otros) que apliquen a todos los sistemas de IA;

(ii) la lista de prácticas prohibidas del art. 5 debe ser ampliada y reforzada para incluir prácticas dañinas que en la actual propuesta no se toman en cuenta, como por ejemplo, los sistemas de IA que manipulen causando un daño económico;

(iii) las personas consumidoras deben tener una serie de derechos reconocidos, tales como el derecho a acceder a la justicia y a la reparación, incluido el daño colectivo;

(iv) los procedimientos de evaluación de conformidad aplicables a los sistemas de alto riesgo deben ser reforzados, debiendo establecerse que las evaluaciones de terceros sean la regla para este tipo de sistemas;

(v) los estándares armonizados deben utilizarse únicamente para definir requerimientos técnicos, y no para definir o aplicar principios legales o relacionados con los derechos fundamentales;

(vi) el sistema de gobernanza y los mecanismos de aplicación por parte las autoridades nacionales debe ser clarificados y mejorados, por ejemplo, otorgando a la Comisión la competencia de iniciar procedimientos de evaluación de un sistema de IA bajo determinadas circunstancias.

¿Cuáles son las mejoras necesarias en la propuesta?[1]

1. Objetivos y brecha de protección al consumidor

La protección del consumidor no está presente en la propuesta. Entre los objetivos de esta no se hace referencia específica a la protección del consumidor frente a los posibles impactos adversos de la IA. Tampoco se establecen derechos horizontales para los consumidores y se los excluye de la definición de "usuario", que se define como un usuario institucional o comercial.

Se entiende necesario:

Mencionar entre los objetivos de la propuesta (art. 1) que se debe asegurar un mayor nivel de protección de los intereses públicos, como la salud y la seguridad en general, la protección del consumidor, del ambiente y de los derechos fundamentales.

2. Las implicancias y riesgos de la máxima armonización

Conforme al art. 3(1) se pretende un alto nivel de armonización, lo que deja poco lugar para que los Estados miembros establezcan mayores regulaciones y evita que se puedan establecer más restricciones y, por ende, normas protectoras a nivel nacional.

Se entiende necesario:

No introducir máxima armonización en tanto la propuesta abarca una lista de sistemas de "alto riesgo". El considerando 1 debería modificarse para aclarar que los Estados miembros pueden establecer limitaciones adicionales por razones de interés público y para la protección de las personas.

3. Principales definiciones y conceptos (art. 3)

3.1. Sistema de IA.

---

[1] Fuente: BEUC. 2021. Regulating AI to protect the consumer

La propuesta se abstiene de definir IA. Sin embargo, en el art. 3 (1) define "Sistema IA" como aquel que es capaz de generar resultados, como contenido, predicciones, recomendaciones o decisiones que influyen en los entornos con los que interactúa, a partir de un conjunto dado de objetivos definidos por personas, utilizando técnicas y enfoques definidos en el Anexo I como enfoques de aprendizaje automático, basados en la lógica, el conocimiento o estadísticas.

De esta manera, evita atarse a una definición que vincule el funcionamiento de la IA con la inteligencia humana, lo que reduciría significativamente su alcance. Ahora bien, en tanto la propuesta de Reglamento busca establecer un marco legal uniforme para toda la IA, es importante asegurar que no escape de establecer reglas básicas para todos los sistemas de IA.

Se entiende necesario:

El proyecto debería clarificar en el Considerando 2 que la referencia a "sistemas IA" también aplica a la IA como tal, según la definición del Grupo de Expertos de Alto Nivel [2](HLEG, por sus siglas en inglés) de la Comisión.

Para evitar malas interpretaciones, el considerando 6 debería clarificar el alcance de la definición de "sistema de IA", y brindar ejemplos de herramientas y sistemas, como las hojas de cálculo con fórmulas estadísticas, que normalmente no entrarían en la definición de "sistema de IA". En este sentido, el Anexo I no debería modificarse.

3.2. Usuario

La propuesta excluye a los individuos que utilizan la IA como "usuarios" a menos que se lo hagan en su capacidad profesional, así como aquellas personas que están sujetas al uso de un sistema de IA.

Se entiende necesario:

[2] Sistema IA: "sistemas de software (y posiblemente también de hardware) diseñados por humanos que, dado un objetivo complejo, actúan en la dimensión física o digital al percibir su entorno a través de adquisición de datos, interpretación de los datos estructurados o no estructurados recopilados, razonamiento sobre el conocimiento, o procesar la información derivada de estos datos y decidir la(s) mejor(es) acción(es) a tomar para lograr el objetivo dado meta. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar sus comportamientos mediante el análisis de cómo el medio ambiente se ve afectado por sus acciones anteriores. Como disciplina científica, la IA incluye varios enfoques y técnicas, como el aprendizaje automático (del cual el aprendizaje profundo y aprendizaje por refuerzo son ejemplos específicos), razonamiento automático (que incluye planificación, programación, representación y razonamiento del conocimiento, búsqueda y optimización) y robótica (que incluye control, percepción, sensores y actuadores, así como la integración de todas las demás técnicas en sistemas de ciberfísica."

Para asegurar un alto nivel de protección al consumidor, el proyecto debe incluir la definición de "consumidor".

3.3. Riesgo:

El proyecto presenta un enfoque "basado en el riesgo" a partir de una clasificación *ex ante* de sistemas de IA, siendo categoría de "alto riesgo" el principal objeto de regulación. La propuesta no define "riesgo" como tal. Sin embargo, ofrece indicios para poder identificarlos. Por ejemplo, el "riesgo de daño a la salud y seguridad, o riesgo de impactos adversos sobre derechos fundamentales" son criterios para actualizar la lista de "sistemas de IA de alto riesgo" que figura en el Anexo III.

Otros riesgos que plantea la IA para los individuos y la sociedad (por ejemplo, a la democracia o al Estado de Derecho) no se encuentran dentro del alcance del Reglamento. De esta manera, riesgos para la sociedad, como algoritmos de personalización que maximizan la atención en sistemas de recomendación, no se encuentran incluidos en el proyecto.

Se entiende necesario:

Incluir expresamente en la definición de "sistemas de IA que presentan riesgos" del art. 65(1), riesgos de que la IA tenga un impacto un impacto adverso en los consumidores, la autonomía de elección, el acceso a bienes y servicios, discriminación injusta y daño económico, a la privacidad y a la protección de datos, así como también los riesgos sociales.

3.4. Daños

El término es utilizado en la propuesta, pero no se define en la misma. En tal sentido, la aplicación de una definición de "sentido común" de "daño", podría acarrear dificultades en la aplicación práctica del Reglamento, particularmente si se tiene en cuenta la necesidad de establecer el uso y el alcance extremadamente limitado de las disposiciones sobre prácticas prohibidas.

Se entiende necesario:

Que los considerandos incluyan una guía detallada de daño, para aclarar: (i) cómo el "daño" debe ser entendido; (ii) la manera en que un daño es provocado: por un evento particular y a través de una exposición en el tiempo a prácticas algorítmicas dañinas; a través de una acción distribuida entre un número de actores donde la entidad que causa el daño no es necesariamente la que utilice la IA; el daño causado por usos distintos a los previstos, para evitar reducir el marco a los sistemas "destinados a

distorsionar el comportamiento", y basar el daño en una presunción de una "intención" que puede no existir, estar oculta o ser difícil de probar.

3.5. El propósito previsto y mal uso

El "propósito previsto" de un sistema de IA es un parámetro que pretende establecer el marco legal, que se define como "el uso previsto por el proveedor".

Por otro lado, el concepto de "uso indebido razonablemente previsible" es definido como el uso de un sistema de IA de una manera que no se encuentra en concordancia con su "propósito previsto", pero que podría resultar de un comportamiento humano razonablemente previsible o de la interacción con otros sistemas.

Tanto el concepto de "propósito previsto" como de "uso indebido" solo pueden ser aplicados a los sistemas clasificados como "alto riesgo".

Se entiende necesario:

Que se incluya un mecanismo para evaluar el propósito y el uso previsible, incluido el uso indebido, de todos los sistemas de IA, con el fin de permitir la evaluación de otros sistemas más allá de los actualmente etiquetados como de "alto riesgo".

El mecanismo de evaluación no debe limitarse a las nociones limitadas de "propósito previsto" y "uso indebido razonablemente previsible", sino que debería además permitir al órgano examinador el análisis de "usos potenciales" o "usos previsibles" de un sistema determinado.

3.6. Datos biométricos

La propuesta utiliza la siguiente definición de "datos biométricos": "datos personales que resultan de un procesamiento técnico específico relacionado con las características físicas, fisiológicas o de comportamiento de una persona natural, que permitan o confirmen la identificación única de esa persona natural".

Se ha destacado cierta preocupación respecto de tal definición. Las aplicaciones que utilizan el reconocimiento de emociones o la categorización biométrica pueden operar usando datos menos detallados.

Se entiende necesario:

Modificar las definiciones de sistema de reconocimiento de emociones (art. 3 (34)) y de sistema de categorización biométrica (art. 3 (35)) para evitar que se encuentren necesariamente atados a una identificación real (o confirmación

de una identificación) de un individuo. De esa manera, un sistema que realice interferencias invasivas -aunque anónimas- en el estado emocional o categoría social no quedarían fuera de los referidos artículos.

3.7. Sistemas de identificación biométrica remota

El art. 3 (36) define a un "sistema de identificación biométrica remota" como un sistema destinado a identificar a personas naturales a distancia, mediante la comparación de los datos biométricos de una persona con los contenidos en una base de datos, y sin previo conocimiento acerca de si la persona en cuestión estará presente y pueda ser identificada.

Se distinguen dos tipos de sistemas: (i) sistemas de identificación biométrica remota "en tiempo real", en los que la captura de los datos biométricos, su comparación y la identificación ocurren casi sin demoras; (ii) sistemas de identificación biométrica remota "posteriores".

Se entiende necesario:

Para aclarar mejor qué constituye un sistema de "identificación remota", el significado de "distancia" debe ser clarificado en el art. 3(36).

En igual sentido, se debe aclarar bien qué constituye un sistema de reconocimiento en "tiempo real" o "posterior" conforme art. 3(37)-(38), con material "en vivo" o "casi en vivo" como menciona el Considerando 8.

4. Listado de prácticas prohibidas (art. 5)

El art. 5 establece un listado de prácticas prohibidas en la UE. Sin embargo, se entienden necesarias ciertas mejoras con el fin de tomar en consideración los intereses de los consumidores y asegurar una amplia y clara aplicación de las prohibiciones.

4.1. Técnicas subliminales que causan distorsión y daño del comportamiento – art. 5 (1) a)

Esta prohibición es limitada en la propuesta a la IA que cause daño físico o psicológico.

Por otra parte, parece que se prohíbe la IA cuyo "propósito" sea causar un daño físico o psicológico, quedando excluidos el "uso potencial" o "el uso indebido razonablemente previsible". Se rechaza expresamente el requisito de probar la intención. Esto no se requiere en la ley del consumidor de la UE, en caso de

prácticas comerciales desleales o responsabilidad del producto. **Esto sería un paso hacia atrás en el nivel de protección de los consumidores. Ello, sin mencionar que resulta muy difícil, o imposible, probar la intención maliciosa.**

Se entiende necesario:

Que el art. 5 (1) a) se expanda para incluir las prácticas de IA que manipulan de manera tal que puedan causar daños económicos;

Que el art. 5 (1) incluya la IA cuyo "propósito específico" o su "uso indebido razonablemente previsible" pueda manipular a una persona y provocar daños físicos, psicológicos o económicos. También debería incluir el "uso potencial" o el "uso previsible" y aplicarse independientemente de la clasificación de riesgo del sistema de IA;

El criterio "subliminal" del art. 5(1) a) debería ser eliminado, en tanto es vago e innecesario;

Establecer una amplia inversión de la carga de la prueba, de manera que la responsabilidad de demostrar el cumplimiento sea de la entidad que se encuentra detrás del sistema de IA. Esta recomendación se debe aplicar a todas las prácticas prohibidas;

El daño social causado por una práctica de IA debería incluirse (por ejemplo, los sistemas de IA pueden manipular a alguien de manera tal que tenga impacto en el funcionamiento de la democracia o el Estado de Derecho).

4.2. Grupos vulnerables - art. 5 (1) b)

La propuesta se focaliza en la IA que explote las vulnerabilidades de ciertos grupos, como los niños, las personas con diversidad funcional, con la intención específica de afectar su comportamiento material llevando a un daño físico o psicológico.

Se entiende necesario:

Que el art. 5(1)b) aplique también a la IA utilizada para explotar otras vulnerabilidades, además de las que se encuentran relacionadas con menores o personas con diversidad funcional (física o mental). Por ejemplo, debería proteger a los consumidores que se encuentran en posición de vulnerabilidad por el uso de perfiles de persuasión o prácticas de personalización (asimetría digital) o por vulnerabilidades temporales, como el duelo, la tristeza, la angustia emocional, etc.

Que el art. 5(1)b) incluya la IA cuyo "propósito específico" o su "uso indebido razonablemente previsible" pueda manipular a una persona y provocar daños físicos, psicológicos o económicos. También debería incluir el "uso potencial" o el "uso previsible" y aplicarse independientemente de la clasificación de riesgo del sistema de IA.

4.3. *Especial consideración a menores y jóvenes*

Consideramos necesario realizar una especial mención a la situación de los menores y jóvenes, en atención al impacto que tienen sobre ellos los sistemas de IA. Tanto generación *Z* como la *Alpha* han nacido ya con la IA como una de las herramientas que se encuentra presente en su día a día. Si bien la IA puede tener muchos beneficios para ellos, también conlleva la existencia de numerosos riesgos. Por ejemplo, la IA puede cambiar el modo en que los jóvenes se comunican o se relacionan entre sí.

Al respecto, se ha puesto de resalto cómo el diseño persuasivo y las estrategias desplegadas para maximizar la colección de datos personales, impactan en la vida social, mental y en el desarrollo físico de los niños. Tales impactos incluyen la ansiedad personal, la agresión social, las relaciones despojadas, la privación del sueño, así como también influyen en la educación, la salud y el bienestar[3]. Por ello, se considera que, por ejemplo, es necesario educar a los menores y jóvenes para que resguarden sus datos personales, a fin de evitar que en un futuro se les dificulte el acceso al trabajo, a un nivel alto de educación o, incluso, a un crédito.

En ese sentido, se recuerda que los menores poseen derechos específicos establecidos en el artículo 24 de la Carta de la UE y en la Convención sobre los Derechos del Niño de las Naciones Unidas. De los mismos se desprende la necesidad de atender a la situación de vulnerabilidad de los menores, y de brindarles especial protección y asistencia para su bienestar.

De esta manera, consideramos que resulta insuficiente únicamente prohibir aquellos sistemas de IA "destinados" a alterar la conducta humana, como aquellas prácticas que se aprovechan de las vulnerabilidades de grupos vulnerables concretos, como los menores, para alterar de manera sustancial su comportamiento de un modo que es probable que les provoque perjuicios físicos o psicológicos a ellos o a otras personas.

Se observa de la propuesta de Reglamento (considerando 16) que se hace referencia a la "intención" de alterar sustancialmente el comportamiento de una

[3] 5Rights. 2018. *Disrupted Childhood: The cost of Persuasive design*

persona y de un modo que perjudique o es probable que perjudique a esa misma persona o a otra, lo cual termina por reducir el ámbito de protección de los menores.

Se entiende necesario que:

Se mejore la protección de los menores y jóvenes, ampliando las prácticas prohibidas para que se incluya una visión preventiva que abarque a aquellas que intenten llevar a los niños a conductas adictivas o peligrosas, más allá de la probabilidad de daño. En su caso, que el daño considerado abarque usos distintos a los "previstos", de manera tal que se evite la necesidad de basar el daño en la presunción de una "intención" que puede no existir, estar oculta o ser difícil de probar. Es decir, debe considerarse el "uso indebido razonablemente previsible", el "uso potencial" y el "uso previsible".

4.4. Calificación social - art. 5(1)c)

Se prohíbe la calificación social por parte de las autoridades públicas. Sin embargo, tal prohibición por parte de entidades privadas no está expresamente regulada.

Se entiende necesario:

Incluir una prohibición general de IA utilizada por parte de entidades públicas y privadas para evaluar la confiabilidad de una persona con base en su comportamiento social u otros atributos personales, como preferencias, emociones, salud o inteligencia. La calificación social debería prohibirse con independencia del contexto en que se recopilaron los datos,

El comportamiento discriminatorio a través de la calificación social debería ser siempre ilícito, incluso cuando el trato perjudicial o desfavorable es proporcionado al comportamiento social del individuo.

4.5 Identificación biométrica remota en tiempo real (art. 5(1)d)

Las compañías están utilizando cada vez más datos biométricos para diferentes propósitos. En todo el mundo, el reconocimiento facial es usado para "etiquetar" a una persona en las plataformas de redes sociales, para desbloquear teléfonos inteligentes o autenticar o identificar consumidores en el contexto de los servicios financieros.

Los datos biométricos son particularmente sensibles, por lo que su procesamiento ilegítimo puede conllevar serias consecuencias para los consumidores y la sociedad.

Así, el art. 5 (1)d) prohíbe el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con el fin de hacer cumplir la ley (por ejemplo, en la calle). Sin embargo, esta prohibición no es absoluta. En la propuesta actual, en ciertas situaciones (por ejemplo, búsqueda de niños perdidos) y en ciertas condiciones (por ejemplo, autorización judicial previa), el uso de tales sistemas en espacios públicos está permitido. Por su parte, el uso de estos por parte de entidades privadas está permitido.

Si se tiene en cuenta el riesgo que representa para los derechos fundamentales, la base de los principios democráticos y los valores de la UE, su uso en espacios públicos por parte de entidades privadas debería estar prohibido sin excepciones.

Se entiende necesario que:

El uso de la identificación biométrica remota en tiempo real por parte de entidades públicas y privadas sea totalmente prohibido, sin excepciones.

4.6. Reconocimiento de emociones

El uso de IA para reconocer emociones es una cuestión preocupante para los consumidores, y puede llevar a serias violaciones a su privacidad y a su manipulación. En la propuesta actual, el uso de IA para el reconocimiento de emociones no es considerado como "alto riesgo" y se encuentra simplemente sujeto a obligaciones de transparencia.

Se entiende necesario que **el art. 5 también prohíba el uso de IA para el reconocimiento de emociones, excepto en circunstancias específicas relacionadas con la salud o la investigación, en línea con las recomendaciones del CEPD y SEPD.**

4.7. Sistemas de IA no probados científicamente

Se entiende necesario que:

Se prohíba la utilización de IA cuya validez científica no está acreditada o cuyos supuestos beneficios han sido desacreditados por la ciencia.

5. Alcance restringido y evaluación de riesgos

5.1. Alcance restringido

5.1.1. Sistemas de Alto Riesgo

Una de las principales deficiencias de la propuesta es el limitado ámbito de aplicación de sus obligaciones y requisitos. Estos se refieren casi exclusivamente a los "sistemas de IA de alto riesgo", dejando una gran mayoría de los sistemas de IA existentes sin regular.

Para cualquier otro tipo de sistema de IA, la Comisión Europea confía en el concepto de voluntarismo. La propuesta sugiere que los requisitos para los "sistemas de alto riesgo" podrían ser aplicables de manera voluntaria a través de códigos de conducta, y que su elaboración debería ser fomentada por la Comisión y los Estados Miembros (art. 69).

Un sistema de IA es considerado de "alto riesgo" si se especifica como tal en el art. 6 de la propuesta, esto es, si constituye un producto o un componente de seguridad de un producto contemplados por la legislación de armonización de la UE prevista en el Anexo II y exige una evaluación de conformidad de terceros; o si se encuentra expresamente en el Anexo III.

Este enfoque conlleva grandes implicaciones. En primer lugar, deja fuera del alcance del Reglamento una gran mayoría de sistemas de IA que afectan diariamente a ciudadanos y consumidores, como son los algoritmos de perfilado y personalización en línea, los sistemas de recomendación que seleccionan lo que la gente ve en sus redes sociales. En segundo lugar, este enfoque no resulta flexible para poder abordar otros riesgos que puedan manifestarse después de la implementación de un sistema de IA. Por ello, la propuesta de Reglamento corre el riesgo de quedarse desactualizada de manera rápida. En tercer lugar, la categoría misma de "alto riesgo" en sí misma se encuentra definida de modo limitado, excluyendo de su alcance a aplicaciones de IA que pueden causar serios daños en caso de ser mal utilizadas.

5.1.2. Actualización de listado de sistemas de riesgo

La Comisión pretende evaluar anualmente si la lista de aplicaciones de alto riesgo que figura en el Anexo III necesita ser actualizada. Sin embargo, tal actualización se encuentra sujeta a condiciones estrictas que harán demasiado dificultoso ampliar el alcance del Anexo. En primer lugar, la propuesta limita la posibilidad de expandir el alcance a las áreas que ya se encuentran en el Anexo III (art. 7 (1) a)), lo cual resulta irrazonable dada la complejidad y los desafíos que representa la tecnología IA. En segundo lugar, la IA solo puede ser agregada al Anexo III si posee

un riesgo de daño a la salud, seguridad o tiene impacto en derechos fundamentales. Esto no toma en consideración, como se ha indicado, el daño económico o los impactos sociales negativos.

5.1.3. Sistemas distintos a los de alto riesgo

CECU, siguiendo a BEUC, apoya el "enfoque de riesgo" pero uno en el que todos los sistemas de IA (incluido los que no son de alto riesgo) se encuentran adecuadamente regulados.

Se entiende necesario:

Que el alcance del Reglamento sea ampliado para regular adecuadamente sistemas de IA distintos de los calificados como de "alto riesgo", como serían los contadores inteligentes, los juguetes conectados con IA, los asistentes virtuales o la IA que organiza lo que las personas ven las redes sociales;

Todos los sistemas de IA empleados en la UE, incluyendo los de riesgo medio y bajo, deberían respetar un conjunto de principios comunes establecidos en el Reglamento (por ejemplo, transparencia, equidad, no discriminación);

La lista existente de aplicaciones de "alto riesgo" que figura en el Anexo III debería ser ampliada para incluir otras aplicaciones de IA, como por ejemplo, las que se utilizan para evaluar primas de seguro, servicios de pago y cobro de débitos. También la Directiva de Baja Tensión debería incluirse en el Anexo II, en tanto los dispositivos alimentados por IA que adquieran consumidores caen bajo su alcance.

5.2. Metodología de evaluación

El Reglamento no prevé una prueba de evaluación de riesgos u otros medios para clasificar un sistema de IA, que complemente la clasificación de "alto riesgo". Es necesario incluir un proceso que determine el nivel de riesgo (alto, medio, bajo) y posibles incumplimientos del art. 5.

Se entiende necesario:

Ampliar el marco de riesgos para incluir otras categorías, como bajo y medio, que deberían ser asignados en base a un sistema de clasificación;

Tal sistema debe incluir una cláusula general que permitiría la clasificación de los sistemas de IA para asignarles una categoría de riesgo adecuada, desde alto a bajo;

Debería ser obligatoria una autoevaluación preliminar para todos los proveedores de sistemas de IA con el fin de determinar la categoría de riesgo y descartar el incumplimiento de cualquier prohibición expresa del art. 5, de manera previa a que el sistema sea puesto en uso en intervalos regulares luego de su despliegue;

El sistema de clasificación de riesgos debería incluir daños a la salud, seguridad, derechos fundamentales, protección de los consumidores, daños económicos, daños sociales y ambientales;

Los niveles riesgo diferentes de "alto" deben ser sujetos a requerimientos apropiados, como por ejemplo, cumplir con principios horizontales que el Reglamento debería establecer (como transparencia y equidad). A su vez, para los sistemas de riesgo medio debe establecerse el mantenimiento del registro de auditorías y obligaciones de reporte para asegurar un nivel adecuado y verificable de transparencia.

6. Principios y derechos horizontales de IA para las personas consumidoras

El art. 69 de la propuesta alienta a los Estados Miembro a redactar códigos de conducta para fomentar la aplicación voluntaria de los requisitos establecidos en el título III, Capítulo I, de los sistemas de IA que no son considerados de "alto riesgo". Además del art. 52 sobre transparencia y el art. 5 sobre prácticas prohibidas, solo estos compromisos voluntarios serían aplicables a los sistemas de IA que no son de alto riesgo.

Si se toma en cuenta el riesgo y el potencial que tienen los sistemas de IA para causar daños a los individuos y a la sociedad, **resulta inaceptable atribuir la protección de los consumidores a un conjunto de reglas no exigibles.**

Los principios horizontales deben traducirse en derecho exigibles para las personas y obligaciones para los usuarios comerciales y proveedores de sistemas de IA.

6.1. Transparencia, explicación y objeción

El Reglamento establece ciertas obligaciones de transparencia para los "sistemas de IA de alto riesgo", incluyendo la transparencia hacia los usuarios de los sistemas (por ejemplo, aquellos que los emplean, que no son consumidores), autoridades de control y requisitos de documentación. El art. 52 también establece reglas limitadas de transparencia para cierta IA.

Sin embargo, no hay regla que obligue a los proveedores o usuarios comerciales de IA a brindar una explicación individual de las razones específicas por las que se toma una decisión que los afecta. Las reglas de transparencia deberían aplicarse a toda la IA.

Se entiende necesario que:

El Reglamento incluya un principio general que requiera que todos los sistemas de IA sean utilizados de forma transparente en relación con sus ciudadanos y consumidores;

El Reglamento debería permitir a los consumidores tener el derecho a recibir una explicación acerca de los procesos de toma de decisiones que utilizan IA, que puedan afectarlos individualmente;

El Reglamento debería otorgar a los consumidores el derecho a impugnar las decisiones algorítmicas y solicitar la intervención de una persona humana, siempre que una decisión pueda tener un impacto significativo sobre ellos.

6.2. Rendición de cuentas y control

Todos los sistemas de IA deben contar con ciertas medidas técnicas y organizativas para garantizar el cumplimiento de las normas y la supervisión regulatoria. El art. 14 establece un sistema basado en la supervisión humana, pero como sucede con la mayoría de los requerimientos de la propuesta, solo aplica a los sistemas de IA de alto riesgo.

Se entiende necesario que:

El Reglamento incluya una obligación para todos los proveedores de IA de controlar regularmente el funcionamiento de su sistema de IA, y evaluar si respeta las obligaciones y derechos establecidos en la propia regulación. Tal control debería involucrar siempre a personas humanas ;

El Reglamento incluya un principio general de rendición de cuentas que establezca claramente que las entidades que desarrollan y utilizan sistemas de IA son responsables, y deben poder demostrar el cumplimiento de las normas.

6.3 Equidad

Los sistemas de IA deben ser desarrollados y utilizados de forma justa y responsable. Por ejemplo, los procesos de toma de decisiones deben ser justos, desde el punto de vista de los datos procesados, los medios utilizados para el proceso de decisión y el propósito que se encuentra detrás del resultado.

Este último aspecto no se encuentra totalmente abordado en las normas de protección de datos de la UE, que se focaliza más que nada en el tratamiento de datos personales, pero no en las consecuencias que resultan de las interferencias y el análisis predictivo.

Se entiende necesario que:

El Reglamento incluya un principio general de que todos los sistemas y prácticas de IA deben ser justos para los individuos y para la sociedad.

6.4. No discriminación

Los consumidores deberían ser protegidos de la discriminación ilegal y de las distinciones injustas que se llevan a cabo a mediante el uso de sistemas de IA. Mediante el uso de conjuntos de datos y algoritmos sesgados, un proceso de creación de perfiles puede realizar inferencias erróneas y producir predicciones incorrectas, clasificando a los individuos, al asumir ciertas características. Tales errores podrían dañar desproporcionadamente a ciertos grupos.

Se entiende que:

El Reglamento debería imponer a todos los proveedores de IA y usuarios comerciales una obligación general de no discriminación. Esto debería incluir una prohibición de los sistemas de IA que puedan llevar a una discriminación, sobre la base de las características enumeradas en el art. 21 de la Carta de Derechos Fundamentales de la UE, datos biométricos u otros, así como también a una discriminación injusta sobre la base de factores económicos.

6.5. Seguridad y protección

Todos los productos y servicios impulsados por la IA deben ser seguros a lo largo de su ciclo de vida.

Se entiende necesario que:

El Reglamento incluya un principio general que requiera que todos los productos y servicios alimentados por IA sean seguros a lo largo de todo su ciclo de vida (seguridad por diseño y por defecto).

6.6. Acceso a la justicia y derecho a reparación, incluida la reparación colectiva

La propuesta falla por completo en abordar este punto. No incluye ningún mecanismo que permita a los consumidores utilizar herramientas privadas de aplicación cuando un sistema de IA o una práctica infringe sus derechos o les causa daño.

En igual sentido, la propuesta no permite a las organizaciones de la sociedad civil, incluidas las organizaciones de consumidores, representar a los consumidores dañados en el ejercicio de sus derechos. Falta un artículo similar al art. 80 del RGPD (representación de los interesados)[4].

Se entiende necesario que:

La propuesta incluya el derecho de los consumidores a presentar una reclamación ante autoridades nacionales o entablar acciones legales en la justicia cuando un sistema o una práctica de IA que los afecta;

Se incluya una obligación para las compañías de establecer un mecanismo de reclamaciones para los consumidores. Además, deben estar obligadas a reaccionar ante esas reclamaciones en un plazo corto;

Se incluya un artículo que permita a las organizaciones de consumidores u organizaciones de la sociedad civil representar a consumidores individuales en el ejercicio de sus derechos bajo esta regulación. Además, deberían poder actuar en nombre del "interés general" (por ejemplo, presentar reclamaciones sin mandato de individuo cuando un sistema o práctica de IA se encuentre incumplimiendo el Reglamento);

Se incluya una previsión que agregue al Reglamento en el Anexo de la Directiva sobre acciones de representación colectiva (RAD, por sus siglas en inglés), para que se puedan iniciar acciones colectivas de resarcimiento o solicitud de medidas cautelares en caso de un sistema de IA que se encuentre en incumplimiento.

6.7. Fiabilidad y resistencia

Todos los productos alimentados por IA deben ser técnicamente fiables y resistentes desde el diseño. Cuanto más autónomas se vuelven las máquinas, más importante es que los usuarios confíen en el sistema respecto a su rendimiento, precisión y resistencia a lo largo de su ciclo vital.

Se entiende necesario que:

El Reglamento incluya un principio general relativo a que el funcionamiento de los sistemas de IA sea confiable, preciso y resistente durante todo el ciclo de vida del producto.

[4] El art. 80 del RGPD permite a los consumidores encargar a un organismo sin ánimo de lucro que presente reclamaciones en su nombre.

7. Procedimiento de evaluación de conformidad (art. 43)

La propuesta descansa demasiado en la autoevaluación del cumplimiento de la industria. La evaluación de terceros solo es llevada a cabo en pocos casos, por lo que este enfoque es inadecuado y no toma en consideración la complejidad de los riesgos derivados de la IA.

Se entiende necesario que:

La evaluación de terceros sea la regla para evaluar la conformidad de los sistemas de IA de alto riesgo. La autoevaluación solo debe permitirse cuando los sistemas de IA no están considerados de alto riesgo;

En los supuestos de sistemas de IA de alto riesgo, los resultados de los procesos de evaluación de conformidad y toda la documentación relevante, deben ser notificados a la autoridad de vigilancia del mercado pertinente, antes de que el producto sea puesto en el mercado y publicado en una base de datos de acceso público;

En los casos de otros sistemas de IA, los resultados del proceso de evaluación de riesgos y toda la documentación relevante, deberían ser notificados solamente a las autoridades públicas cuando así lo requieran.

8. Estándares

De acuerdo con el concepto propuesto en el Reglamento, su aplicación exitosa dependerá más que nada del desarrollo y aplicación de estándares armonizados de los fabricantes de los sistemas de IA.

El art. 40 establece un incentivo importante para la aplicación de estándares por parte de los fabricantes: los sistemas de IA de alto riesgo que se encuentran conformes a los estándares armonizados se presumen de conformidad con los requerimientos del Reglamento, y se invierte la carga de la prueba acerca del cumplimiento de los requisitos legales. Otro incentivo está previsto en el art. 43, en virtud del cual los proveedores de servicios de un sistema de IA que apliquen tales estándares podrán llevar a cabo autoevaluaciones.

El uso de la estandarización, como se encuentra en la propuesta, es inaceptable en un campo tan sensible e importante para nuestra sociedad y para los derechos fundamentales, como lo es la IA, particularmente si se tienen en cuenta los objetivos de la UE para la transición digital.

Se entiende necesario que:

Los estándares armonizados no sean utilizados para definir o aplicar derechos fundamentales, principios legales o éticos. Su uso debería estar limitado a implementar aspectos técnicos. Al respecto, un estándar, por ejemplo, no debería ser utilizado para determinar qué tipo de sesgos se encuentran prohibidos bajo el art. 10(2)f);

El Reglamento incluya reglas más detalladas acerca de los requerimientos aplicables a la IA de alto riesgo, incluyendo reglas sobre discriminación;

Como los estándares tendrán un papel importante en detallar los requisitos esenciales establecidos en el Reglamento, el sistema de gobernanza del proceso de estandarización debe ser modificado. En efecto, las organizaciones de consumidores deben ser involucradas en la estandarización. Las autoridades públicas también deben proveer los marcos políticos y financieros para permitir la participación de las partes interesadas;

Dado que las autoridades públicas también se han retirado de muchas actividades de estandarización en detrimento del interés público, es necesario hacer un llamado a las autoridades a estar más comprometidos con ello y apoyar la participación de los consumidores.

9. Aplicación del Reglamento

9.1 Notificación (únicamente) de incidentes graves y de mal funcionamiento de sistemas de alto riesgo (artículo 62)

Bajo el art. 62, los proveedores de sistemas de IA de alto riesgo que se encuentren en el mercado de la UE deben notificar a las autoridades de vigilancia de mercado "un incidente serio o el mal funcionamiento de tale sistemas que constituya un incumplimiento de las obligaciones de la legislación europea destinada a la protección de los derechos fundamentales".

Se entiende necesario:

Clarificar en el considerando que bajo el art. 62 se incluye la obligación de notificar un incidente serio que viole los derechos de los consumidores;

El art. 62 debe asegurar que los consumidores que se encuentren afectados por un incidente o mal funcionamiento de la IA sean inmediatamente informados de ello.

9.2. Estructura de gobernanza y mecanismos de aplicación del Reglamento (art. 63)

La estructura de gobernanza propuesta descansa mayormente a nivel nacional con la autoridad de vigilancia del mercado.

Se entiende necesario que:

La aplicación a nivel nacional sea reforzada técnicamente con la creación de un cuerpo especializado de expertos designados por la Comisión, que debería asistir a esta última y a las autoridades nacionales en los aspectos técnicos de sus investigaciones, y tener competencia para emitir opiniones no vinculantes acerca de los casos planteados por tales autoridades;

El procedimiento previsto en el art. 66 (salvaguardia de la Unión) no se encuentre limitado al inicio de acciones por parte de las autoridades de los Estados Miembros. La Comisión Europea debería poder iniciar un procedimiento de evaluación acerca de un sistema de IA cuando: (a) existan razones suficientes para creer que el sistema presenta un riesgo; (b) ninguna autoridad de vigilancia del mercado haya iniciado una investigación bajo el art. 65 (2) (Procedimiento aplicable a los sistemas de IA que presenten un riesgo a nivel nacional), y (c) el sistema de IA afecte a los consumidores de más de un Estado Miembro;

El Reglamento clarifique que las autoridades de vigilancia del mercado llevan a cabo sus actividades no solo en base a la proporcionalidad, sino también desde un enfoque precautorio.

9.3. Acceso a datos y documentación (art. 64)

Se entiende necesario que:

El art. 64 garantice a las organizaciones de consumidores el derecho a acceder a documentación importante creada, en el contexto del Reglamento, por un proveedor y a requerir que la autoridad lleve a cabo auditorías *ad-hoc* de un sistema particular.

9.4. Procedimiento aplicable a los sistemas de IA que presenten un riesgo a nivel nacional (art. 65)

En lo relativo a los sistemas que no son de alto riesgo, la aplicación del art. 65 es poco clara. Aparentemente, el art. 65 (1) establece un marco para evaluar riesgos a nivel nacional, haciendo referencia al art. 3(19) del Reglamento UE 2019/1020 de vigilancia del mercado, pero en lo que respecta “a los riesgos para la salud, la seguridad o la protección de los derechos fundamentales”.

Por su parte, de acuerdo con el art. 65 (2), cuando una autoridad de vigilancia del mercado tiene "motivos suficientes" para creer que cualquier IA presenta un riesgo para la salud, seguridad o la protección de los derechos fundamentales, de conformidad con el art. 65 (1), debe llevar a cabo una evaluación de la IA con respecto al cumplimiento de todos los requisitos y obligaciones del Reglamento. Sin embargo, esta última remisión es confusa, en tanto se establecen muy pocas obligaciones para los sistemas de IA que no son de alto riesgo. El único área donde tales sistemas podrían ser incluidos por esta previsión sería el incumplimiento de la "lista negra" del art. 5 o las obligaciones de transparencia del art. 52. En el resto de los casos, el art. 65(2) solo permite a la autoridad nacional iniciar una investigación en los sistemas de IA de alto riesgo.

Se entiende necesario que:

Las organizaciones de la sociedad civil tengan el derecho a requerir la evaluación de sistemas de IA, notificando a los organismos cuando haya indicios suficientes de que un sistema de IA causa daños significativos;

La frase "motivos suficientes para considerar" prevista en el art. 65(2) debería ser clarificada para evitar malas interpretaciones y una aplicación desigual a nivel nacional. En cualquier caso, una reclamación de consumidores debería ser considerada como "motivos suficientes" para iniciar una investigación por parte de las autoridades del mercado bajo el art. 65(2);

Para asegurar una aplicación coherente y consistente del Reglamento, el mismo debe especificar en el art. 65(2) que las autoridades que inician una investigación deben informar a sus pares de otros Estados miembros dentro del Comité de IA;

Los requisitos previstos en el art. 6 para sistemas de alto riesgo deben ser complementados con un marco común de reglas y obligaciones aplicable a todos los sistemas de IA que presenten riesgos medios o bajos, junto con un sistema flexible que permita a las autoridades y reguladores asignar las categorías de riesgos a los sistemas de IA. Si ello se hace, el art. 65(2) será más claro y permitirá verdaderas evaluaciones de riesgo;

Los riesgos mencionados en el art. 65(1), y como en todo el resto del Reglamento, no deben limitarse a la salud, seguridad y derechos fundamentales, sino que deben incluir también los daños económicos e impactos sociales;

El art. 65(1) debe despejar todo tipo duda respecto de qué partes del art. 3(19) del Reglamento UE 2019/1020 sobre vigilancia del mercado se encuentran incluidas en la referencia.

9.5. Procedimiento de salvaguardia de la Unión (art. 66)

Bajo el art. 66, cuando un Estado Miembro formula objeciones contra medidas adoptadas por otro Estado Miembro o cuando la Comisión considera que ciertas medidas son contrarias a las normas de la UE, esta última entablará consultas con el Estado Miembro pertinente e iniciará una evaluación. Sin embargo, la Comisión solo tiene el poder de aceptar o rechazar la medida tomada por el Estado Miembro.

Se entiende necesario que:

La Comisión pueda proponer medidas alternativas a las tomadas por la autoridad del Estado Miembro que inició el procedimiento bajo el art. 65, luego de solicitar el asesoramiento del Comité IA.

10. Comité IA (art. 56-58)

La propuesta establece un Comité Europeo de Inteligencia Artificial ("el Comité IA") compuesto por representantes de los Estados Miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea. El Comité contribuye a efectivizar la cooperación entre autoridades nacionales.

Se entiende necesario que:

Las tareas del Comité incluyan asegurarse de que las autoridades nacionales de vigilancia del mercado cooperen activamente en la aplicación del Reglamento, en particular respecto de los arts. 65 y 66, explicados precedentemente.

11. Interacción con otras áreas de las normas de la UE

11.1. Reglamento General de Protección de Datos (RGPD)

El Reglamento debe explícitamente establecer que el RGPD aplica a cualquier tratamiento de datos personales que caiga dentro del alcance del Reglamento IA, y que sus disposiciones se aplican sin perjuicio de los derechos y obligaciones establecidos bajo el RGPD.

Sin embargo, lo cierto es que el RGPD no provee suficiente protección en el contexto de la IA. Derechos esenciales para los consumidores, como el derecho a impugnar una decisión algorítmica, no deberían depender del tratamiento de datos personales, como es el caso de las reglas europeas de protección de datos.

11.2. Directiva de Responsabilidad de los Productos (PLD, por sus siglas en inglés)

En paralelo y como complemento del Reglamento de IA, la Comisión Europea está considerando actualizar las reglas de responsabilidad civil para adaptarlas para hacer frente a los desafíos planteados por la IA, que incluyen la previsibilidad, el comportamiento autónomo, la adaptación continua, la complejidad y la opacidad, lo que dificulta que se reclame una indemnización en caso de daños.

Todavía hay incertidumbre acerca del instrumento que va a proponer la Comisión. Se espera que la propuesta sea publicada el tercer trimestre del 2022.

Para combatir la asimetría en la información que previene a los consumidores de formular sus reclamos de compensaciones, debería establecerse una inversión de la carga probatoria.

11.3. IA y legislación de los consumidores - Abordar la asimetría digital

Existe una nueva posición de vulnerabilidad para los consumidores, que es a la vez estructural (debido a la estructura de los mercados digitales que impide que los consumidores interactúen con los agentes del mercado en pie de igualdad) y arquitectónica (debido a la forma en que se diseñan y operan las interfaces). Este desequilibrio de poder y la vulnerabilidad consecuente se conocen en el debate académico actual como “asimetría digital” y debe abordarse mediante una revisión del acervo en materia de derecho de los consumidores de la UE.

Una revisión debe introducir nuevas medidas como la modernización de los conceptos de “equidad” y “vulnerabilidad”, la expansión de las “listas negras” para incluir prácticas digitales y la introducción de la inversión de la carga de prueba, colocando la responsabilidad de probar el cumplimiento normativo en cabeza del comerciante.

11.4. IA y sostenibilidad

La propuesta no prevé ningún marco de evaluación que permita a las autoridades evaluar el impacto de un sistema de IA en los derechos fundamentales, incluido el derecho a un alto nivel de protección del medio ambiente.

En este sentido, es necesario realizar un replanteo general de estrategias políticas para garantizar la coherencia entre la sostenibilidad y los objetivos de la política digital.