COMISIÓN
EUROPEA

Bruselas, 19.2.2020
COM(2020) 65 final

LIBRO BLANCO

sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza

Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza

La inteligencia artificial se está desarrollando rápido. Cambiará nuestras vidas, pues mejorará la atención sanitaria (por ejemplo, incrementando la precisión de los diagnósticos y permitiendo una mejor prevención de las enfermedades), aumentará la eficiencia de la agricultura, contribuirá a la mitigación del cambio climático y a la correspondiente adaptación, mejorará la eficiencia de los sistemas de producción a través de un mantenimiento predictivo, aumentará la seguridad de los europeos y nos aportará otros muchos cambios que de momento solo podemos intuir. Al mismo tiempo, la inteligencia artificial (IA) conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos.

En un contexto de feroz competencia mundial, se requiere un enfoque europeo sólido basado en la Estrategia Europea para la IA presentada en abril de 2018[1]. Para aprovechar las oportunidades que ofrece la inteligencia artificial y abordar los retos que presenta, la UE debe actuar conjuntamente y determinar de qué manera, a partir de los valores europeos, promoverá su desarrollo y adopción.

La Comisión se ha comprometido a facilitar el avance científico, preservar el liderazgo tecnológico de la UE y garantizar que las nuevas tecnologías estén al servicio de todos los europeos, de manera que mejoren sus vidas al mismo tiempo que respetan sus derechos.

La presidenta de la Comisión, Ursula von der Leyen, anunció en sus orientaciones políticas[2] un enfoque europeo coordinado en torno a las implicaciones éticas y humanas de la inteligencia artificial y un análisis sobre cómo mejorar la utilización de los macrodatos en la innovación.

Consecuentemente, la Comisión respalda un enfoque basado en la regulación y en la inversión, que tiene el doble objetivo de promover la adopción de la inteligencia artificial y de abordar los riesgos vinculados a determinados usos de esta nueva tecnología. La finalidad del presente Libro Blanco es formular alternativas políticas para alcanzar estos objetivos; no aborda ni el desarrollo ni el uso de la inteligencia artificial para fines militares. La Comisión invita a los Estados miembros, a otras instituciones europeas y a todas las partes interesadas, como la industria, los interlocutores sociales, las organizaciones de la sociedad civil, los investigadores, el público general y demás personas con interés en la materia, a que presenten sus opiniones con respecto de las opciones que se muestran a continuación y a que contribuyan a la futura toma de decisiones de la Comisión en este ámbito.

1. INTRODUCCIÓN

A medida que la tecnología digital adquiere un carácter cada vez más primordial en los distintos aspectos de la vida de las personas, es necesario que estas últimas puedan confiar en ella. Generar confianza es un requisito previo para su adopción, y ello supone una oportunidad para Europa, dada su estrecha vinculación con los valores y el Estado de Derecho y su capacidad demostrada de crear productos seguros, fiables y sofisticados en sectores que van desde la aeronáutica a la energía, pasando por la automoción y los equipos médicos.

El crecimiento económico sostenible y el bienestar social presentes y futuros de Europa se valen cada vez más de los valores creados por los datos. La inteligencia artificial es una de las partes más

[1] Inteligencia artificial para Europa [COM(2018) 237 final].
[2] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_es.pdf

importantes de la economía de los datos. Hoy en día, la mayor parte de los datos son relativos a los consumidores y se almacenan y tratan en infraestructuras ubicadas en nubes centralizadas. Frente a esto, una enorme proporción de los datos del futuro, que serán mucho más abundantes, procederá de la industria, las empresas y el sector público, y se almacenará en diversos sistemas, entre los que destacan los dispositivos informáticos que operan en el borde de la red. Este hecho ofrece nuevas oportunidades a Europa, que cuenta con una posición sólida en la industria digitalizada y las aplicaciones de comunicación empresarial, pero con una posición relativamente frágil en las plataformas de consumidores.

En otras palabras, la inteligencia artificial es una combinación de tecnologías que agrupa datos, algoritmos y capacidad informática. Los avances en computación y la creciente disponibilidad de datos son, por tanto, un motor fundamental en el pronunciado crecimiento actual de la inteligencia artificial. Europa puede aunar su potencial tecnológico e industrial con una infraestructura digital de gran calidad y un marco regulador basado en sus valores fundamentales para **convertirse en líder mundial de la innovación en la economía de los datos y sus aplicaciones**, tal como se establece en la Estrategia Europea de Datos[3]. Sobre estos cimientos, puede desarrollar un ecosistema de inteligencia artificial que acerque las ventajas de la tecnología a la sociedad y la economía europeas en su conjunto:

- a los **ciudadanos**, para que obtengan nuevos beneficios, como una mejor atención sanitaria, una menor cantidad de averías de los aparatos domésticos, unos sistemas de transporte más seguros y limpios, o mejores servicios públicos;
- al desarrollo **empresarial**, por ejemplo, mediante una nueva generación de productos y de servicios en áreas en las que Europa es particularmente fuerte (maquinaria, transporte, ciberseguridad, agricultura, economía verde y circular, atención sanitaria y sectores de gran valor añadido, como la moda y el turismo); y
- a los servicios de **interés público**, por ejemplo mediante una reducción de los costes de la prestación de servicios (transporte, educación, energía y gestión de los residuos), una mayor sostenibilidad de los productos[4], o proporcionando a los servicios y fuerzas de seguridad las herramientas adecuadas para que aseguren la protección de los ciudadanos[5], garantizando correctamente el respeto de sus derechos y libertades.

Teniendo en cuenta el enorme impacto que puede tener la inteligencia artificial en nuestra sociedad y la necesidad de que suscite confianza, resulta clave que la inteligencia artificial europea se asiente en nuestros valores y derechos fundamentales, como la dignidad humana y la protección de la privacidad.

Por otra parte, el impacto de los sistemas de IA debe considerarse no solo desde una perspectiva individual, sino también desde la perspectiva de la sociedad en su conjunto. El uso de sistemas de inteligencia artificial puede tener un papel importante en la consecución de los Objetivos de Desarrollo Sostenible y en el respaldo de los procesos democráticos y los derechos sociales. Con sus recientes propuestas sobre el Pacto Verde Europeo[6], Europa va a la vanguardia de la lucha contra el cambio

[3] COM(2020) 66 final.

[4] La inteligencia artificial y la digitalización en general son motores clave de las ambiciones contempladas en el Pacto Verde Europeo. No obstante, se estima que la huella medioambiental actual del sector de las TIC se sitúa por encima del 2 % del conjunto de emisiones mundiales. La Estrategia Digital Europea que acompaña al presente Libro Blanco propone medidas de transformación ecológica para el sector digital.

[5] Las herramientas de inteligencia artificial pueden ofrecer una oportunidad para proteger mejor a los ciudadanos de la UE de la delincuencia y los actos de terrorismo. Este tipo de herramientas podrían, por ejemplo, ayudar a detectar propaganda terrorista en línea, descubrir transacciones sospechosas en la venta de productos peligrosos, detectar objetos peligrosos ocultos o productos y sustancias ilícitos, ofrecer asistencia a los ciudadanos en situaciones de emergencia y servir de orientación al personal de primera intervención.

[6] COM(2019) 640 final.

climático y los retos medioambientales asociados. Las tecnologías digitales como la inteligencia artificial son motores clave para alcanzar los objetivos del Pacto Verde. Dada la importancia creciente de la inteligencia artificial, es necesario tomar en debida consideración las repercusiones medioambientales de sus sistemas a lo largo de su ciclo de vida y durante toda la cadena de suministro, por ejemplo, en lo que se refiere a la utilización de recursos para el entrenamiento de los algoritmos y el almacenamiento de datos.

A fin de alcanzar una envergadura suficiente y de evitar la fragmentación del mercado único, se necesita un enfoque europeo común en torno a la inteligencia artificial. Introducir iniciativas nacionales presenta el riesgo de hacer peligrar la seguridad jurídica, de reducir la confianza de los ciudadanos y de impedir el surgimiento de una industria europea dinámica.

El presente Libro Blanco ofrece alternativas políticas para facilitar un desarrollo de la inteligencia artificial seguro y fiable en Europa, que respete plenamente los valores y los derechos de los ciudadanos de la UE. Los pilares fundamentales del presente Libro Blanco son:

- El marco político por el que se establecen medidas para armonizar los esfuerzos a escala regional, nacional y europea. En colaboración con los sectores público y privado, los objetivos del marco son movilizar recursos para obtener un **«ecosistema de excelencia»** a lo largo de toda la cadena de valor, partiendo de la investigación y la innovación, así como crear los incentivos adecuados para acelerar la adopción de soluciones basadas en la inteligencia artificial, también por parte de las pequeñas y medianas empresas (pymes).

- Los elementos clave de un futuro marco normativo para la inteligencia artificial en Europa que generen un **«ecosistema de confianza»** exclusivo. Para hacerlo, este marco debe velar por el cumplimiento de las normas de la UE, especialmente las normas de protección de los derechos fundamentales y los derechos de los consumidores, y en concreto con relación a los sistemas de inteligencia artificial que operan en la UE y presentan un riesgo elevado[7]. Generar un ecosistema de confianza constituye un objetivo político en sí mismo, y debe ofrecer seguridad a los ciudadanos para que adopten las aplicaciones de la inteligencia artificial y seguridad jurídica a las empresas y organismos públicos para que innoven usando esta última. La Comisión respalda firmemente un enfoque antropocéntrico que se base en la Comunicación *Generar confianza en la inteligencia artificial centrada en el ser humano*[8], y tendrá en cuenta también los resultados obtenidos durante la fase de prueba de las directrices éticas elaboradas por el grupo de expertos de alto nivel sobre la IA.

La Estrategia Europea de Datos, que acompaña al presente Libro Blanco, tiene por objeto ayudar a Europa a convertirse en la economía con agilidad en el manejo de los datos más atractiva, segura y dinámica del mundo, lo que fortalecerá a Europa con información para reforzar sus decisiones y mejorar las vidas de todos sus ciudadanos. La Estrategia establece varias medidas políticas, como la movilización de inversiones públicas y privadas, necesarias para alcanzar este objetivo. Finalmente, en el informe de la Comisión adjunto al presente Libro Blanco, se analizan las repercusiones de la inteligencia artificial, el internet de las cosas y otras tecnologías digitales en la legislación en materia de seguridad y responsabilidad civil.

[7] Aunque puede que se requieran medidas adicionales para evitar y combatir el uso abusivo de la inteligencia artificial con fines delictivos, se trata de una cuestión independiente del ámbito del presente Libro Blanco.
[8] COM(2019) 168.

2. APROVECHAR LOS PUNTOS FUERTES DE LOS MERCADOS INDUSTRIALES Y PROFESIONALES

Europa se encuentra en buena posición para beneficiarse del potencial de la inteligencia artificial, no solo como usuaria sino también como creadora y productora de esta tecnología. Cuenta con excelentes centros de investigación y con empresas emergentes innovadoras, es líder mundial en los sectores de la robótica, la fabricación y los servicios competitivos, desde la automoción hasta la atención sanitaria, pasando por la energía, los servicios financieros y la agricultura. Europa ha desarrollado una infraestructura informática sólida (mediante, por ejemplo, ordenadores de elevado rendimiento), lo que resulta fundamental para el funcionamiento de la inteligencia artificial. Además, posee un gran volumen de datos públicos y de la industria, cuyo potencial está infrautilizado actualmente. Cuenta con una capacidad industrial reconocida en sistemas digitales seguros y protegidos de bajo consumo de energía que son fundamentales para continuar desarrollando la IA.

Aprovechar la capacidad de la UE para invertir en tecnologías e infraestructuras de la siguiente generación, así como en competencias digitales como la alfabetización sobre datos, reforzará la soberanía tecnológica de Europa en el sector de las tecnologías y las infraestructuras clave para dinamizar la economía de los datos. Las infraestructuras deben respaldar la creación de repositorios de datos que permitan materializar una inteligencia artificial fiable, es decir, una inteligencia artificial basada en los valores y las normas europeos.

Europa debe aprovechar sus puntos fuertes para ampliar su posición en los ecosistemas y en toda la cadena de valor, desde determinados sectores de fabricación de equipos informáticos al despliegue de los programas informáticos durante todo su recorrido hasta los servicios. En cierta medida, esto ya es realidad. Europa produce más de un cuarto de todos los robots de servicios industriales y profesionales (por ejemplo, para la agricultura de precisión, la seguridad, la sanidad, la logística, etc.), y desempeña un papel importante en el desarrollo y el uso de las aplicaciones informáticas para empresas y organizaciones (aplicaciones interempresariales como los programas informáticos de planificación de recursos, de diseño y de ingeniería), así como de aplicaciones para el fomento de la administración digital y las «empresas inteligentes».

Europa se sitúa a la vanguardia de la utilización de la inteligencia artificial en la fabricación. Más de la mitad de los mayores fabricantes aplican al menos un elemento de IA en sus operaciones de fabricación[9].

Una razón de la sólida posición de Europa en lo que se refiere a la investigación es el programa de financiación de la UE, que ha demostrado ser fundamental en las actividades de recopilación, así como a la hora de evitar duplicaciones y de movilizar inversiones públicas y privadas en los Estados miembros. A lo largo de los últimos tres años, la financiación de la UE para investigación e innovación en inteligencia artificial ha aumentado a 1 500 millones EUR, es decir, un incremento del 70 % en comparación con el período anterior.

No obstante, la inversión en investigación e innovación de Europa se sigue representando una proporción menor que la de las inversiones públicas y privadas en otras regiones del mundo. En 2016, se invirtieron unos 3 200 millones EUR en inteligencia artificial en Europa, frente a los cerca de 12 100 millones EUR en América del Norte y 6 500 millones EUR en Asia[10]. Ante este hecho, Europa debe aumentar significativamente sus niveles de inversión. El Plan coordinado sobre inteligencia artificial[11] desarrollado con los Estados miembros está demostrando ser un buen punto de partida para

[9] Por delante de Japón (30 %) y los EE. UU. (28 %). Fuente: CapGemini (2019).
[10] «10 imperatives for Europe in the age of AI and automation», McKinsey, 2017.
[11] COM(2018) 795.

estrechar la cooperación en materia de inteligencia artificial en Europa y crear sinergias que optimicen la inversión en la cadena de valor correspondiente.

3. APROVECHAR LAS PRÓXIMAS OPORTUNIDADES: LA SIGUIENTE OLEADA DE DATOS

Aunque Europa todavía se encuentra en una posición más menos consolidada con relación a las aplicaciones de consumidores y las plataformas en línea (lo que se traduce en una desventaja competitiva en el acceso a los datos), se están experimentando cambios importantes en el valor y la reutilización de los datos en los distintos sectores. El volumen de datos producido en el mundo va en aumento rápidamente, de 33 zetabytes en 2018 a una previsión de 175 zetabytes en 2025[12]. Cada nueva oleada de datos ofrece la oportunidad a Europa de posicionarse en la economía ágil en el manejo de los datos y convertirse en líder mundial en este ámbito. Además, la manera en que se almacenan y tratan los datos cambiará drásticamente a lo largo de los próximos cinco años. A día de hoy, el 80 % del tratamiento y el análisis de datos que se produce en la nube tiene lugar en centros de datos e instalaciones informáticas centralizadas, y el 20 % en aparatos inteligentes conectados, como automóviles, utensilios domésticos o robots de fabricación, e instalaciones informáticas cercanas al usuario («computación en el borde»). Está previsto que, de aquí a 2025, estos porcentajes cambien de manera notable[13].

Europa es líder mundial en electrónica de bajo consumo, lo que resulta fundamental para la siguiente generación de procesadores especializados en relación con la inteligencia artificial. Actualmente, este mercado está dominado por terceros de fuera de la UE. Este hecho podría cambiar con ayuda de iniciativas como la Iniciativa Europea en materia de Procesadores, centrada en desarrollar sistemas informáticos de bajo consumo de energía tanto de computación en el borde como de computación de alto rendimiento de la siguiente generación, y del trabajo de la empresa común de tecnología digital clave, cuyo inicio se ha propuesto para 2021. Europa también es líder en soluciones neuromórficas[14] que están perfectamente adaptadas para automatizar los procesos industriales (industria 4.0) y los modos de transporte. Estas soluciones pueden mejorar la eficiencia energética mediante varios órdenes de magnitud.

Los avances recientes en computación cuántica generarán aumentos exponenciales en la capacidad de tratamiento[15]. Europa puede situarse a la vanguardia de esta tecnología gracias a su fortaleza académica en computación cuántica, así como a la sólida posición de la industria europea en materia de simuladores cuánticos y entornos de programación para la computación cuántica. Las iniciativas europeas que tienen por objeto incrementar la disponibilidad de pruebas y de instalaciones de ensayo cuánticos contribuirán a aplicar estas nuevas soluciones cuánticas en varios sectores industriales y académicos.

Paralelamente, Europa seguirá liderando el progreso de los fundamentos algorítmicos de la inteligencia artificial a partir de su propia excelencia científica. Existe la necesidad de tender puentes entre disciplinas que actualmente trabajan de manera independiente, tales como el aprendizaje automático y el aprendizaje profundo (caracterizados por su naturaleza interpretable limitada y por la necesidad de un gran volumen de datos para entrenar a los modelos y aprender mediante correlaciones) y los enfoques simbólicos (en los que las normas se crean mediante intervención humana). La combinación de

[12] IDC (2019).
[13] Gartner (2017).
[14] Por soluciones neuromórficas se entiende todo sistema de muy gran escala compuesto por circuitos integrados que imitan la arquitectura neuronal biológica del sistema nervioso.
[15] Los ordenadores cuánticos tendrán la capacidad de procesar en fracciones de segundos conjuntos de datos mucho más amplios y numerosos que los ordenadores de mayor rendimiento de la actualidad, lo que permitirá el desarrollo de nuevas aplicaciones de IA en los distintos sectores.

razonamiento simbólico con redes neurales profundas puede ayudarnos a mejorar la capacidad de explicar los resultados de la inteligencia artificial.

4. UN ECOSISTEMA DE EXCELENCIA

Para crear un ecosistema de excelencia que pueda respaldar el desarrollo y la adopción de la inteligencia artificial en el conjunto de la economía y la administración pública de la UE, es necesario redoblar las acciones en varios niveles.

A. COLABORACIÓN CON LOS ESTADOS MIEMBROS

En cumplimiento de su Estrategia sobre la Inteligencia Artificial adoptada en abril de 2018[16], en diciembre del mismo año la Comisión presentó un Plan coordinado, preparado con los Estados miembros, para fomentar el desarrollo y la utilización de la inteligencia artificial en Europa[17].

Este Plan propone cerca de 70 acciones conjuntas para hacer que la cooperación entre los Estados miembros y la Comisión en áreas clave como la investigación, la inversión, la introducción en el mercado, las capacidades y el talento, los datos y la cooperación internacional, sea más estrecha y eficiente. Está programado que el Plan esté operativo hasta 2027, y se prevé hacer un seguimiento y revisarlo de manera regular.

El objetivo es optimizar las repercusiones de la inversión en la investigación, la innovación y la utilización de la inteligencia artificial, evaluar las estrategias nacionales sobre esta tecnología y aprovechar y ampliar el Plan coordinado sobre la inteligencia artificial junto con los Estados miembros:

- *Acción 1: Teniendo en cuenta los resultados de la consulta pública sobre el Libro Blanco, la Comisión propondrá a los Estados miembros una revisión del Plan coordinado que debe adoptarse a finales de 2020.*

La financiación en inteligencia artificial a escala de la UE debe atraer y poner en común inversiones en sectores en los que se requieren acciones que van más allá de lo que un Estado miembro puede conseguir por sí solo. El objetivo es atraer más de 20 000 millones EUR[18] de inversión total anual en inteligencia artificial en la UE a lo largo de la próxima década. A fin de estimular la inversión pública y privada, la UE facilitará recursos del programa Europa Digital, de Horizonte Europa y de los Fondos Estructurales y de Inversión Europeos para abordar las necesidades de las regiones menos desarrolladas y de las zonas rurales.

El Plan coordinado también puede ayudar a integrar el bienestar social y medioambiental como principios clave de la inteligencia artificial. Los sistemas de IA prometen ayudar a combatir las preocupaciones más acuciantes, como el cambio climático y la degradación medioambiental. Además, es importante que todo ello tenga lugar de una manera respetuosa con el medio ambiente. La IA puede y debe analizar por sí misma de manera crítica el uso de los recursos y el consumo de energía y ser entrenada para optar por alternativas que resulten positivas para el medio ambiente. La Comisión valorará opciones para fomentar y promover las soluciones de inteligencia artificial que se encarguen de ello junto con los Estados miembros.

B. CENTRAR LOS ESFUERZOS DE LA COMUNIDAD DE INVESTIGACIÓN E INNOVACIÓN

[16] Inteligencia artificial para Europa [COM(2018) 237].
[17] Plan coordinado sobre la inteligencia artificial [COM(2018) 795].
[18] COM(2018) 237.

Europa no puede permitirse mantener el panorama actual de fragmentación de los centros de competencia, en el que ninguno de ellos alcanza la envergadura suficiente para competir con los organismos que se sitúan a la vanguardia mundial. Resulta clave crear más sinergias y redes entre los distintos centros de investigación europeos sobre la IA y armonizar los esfuerzos para mejorar la excelencia, mantener y atraer a los mejores investigadores y desarrollar las mejores tecnologías. Europa necesita un centro adalid en materia de investigación, innovación y conocimientos técnicos que coordine estos esfuerzos, que sirva de referente mundial de la excelencia en inteligencia artificial y que pueda atraer inversiones, así como a los mejores talentos del sector.

Los centros y las redes deben centrarse en los sectores en los que Europa cuenta con potencial para convertirse en líder mundial, como la industria, la sanidad, el transporte, las finanzas, las cadenas de valor agroalimentarias, la energía y el medio ambiente, la silvicultura, la observación terrestre y el espacio. En todos estos sectores, sigue librándose la carrera por el liderazgo mundial, y Europa ofrece un potencial, unos conocimientos y una pericia significativos[19]. Resulta igualmente importante crear emplazamientos de ensayo y experimentación que respalden el desarrollo y posterior adopción de las nuevas aplicaciones de inteligencia artificial.

- *Acción 2: La Comisión facilitará la creación de centros de excelencia y pruebas que puedan combinar las inversiones europeas, nacionales y privadas, probablemente con la introducción de un nuevo instrumento jurídico. La Comisión ha propuesto un importe ambicioso y dirigido a respaldar centros de ensayo de referencia mundial en Europa en el marco del Programa Europa Digital, completado, cuando así se requiera, por acciones de investigación e innovación de Horizonte Europa, como parte del marco financiero plurianual para el período 2021-2027.*

C. HABILIDADES

El enfoque europeo sobre la inteligencia artificial requerirá ser apuntalado por un sólido interés en las habilidades para hacer frente a la escasez de competencias[20]. La Comisión presentará pronto un apoyo a la Agenda de Capacidades que pretende garantizar que todo el mundo en Europa pueda beneficiarse de las transformaciones verde y digital de la economía de la UE. Las distintas iniciativas también pueden contar con el respaldo de los reguladores sectoriales para fomentar sus habilidades en IA, a fin de aplicar de manera eficiente y eficaz las normas pertinentes. El Plan de acción sobre educación digital actualizado contribuirá a hacer un mejor uso de los datos y de las tecnologías basadas en la inteligencia artificial, como el análisis del aprendizaje y el análisis predictivo, con el objetivo de mejorar los sistemas educativos y formativos y adaptarlos a la era digital. El Plan también incrementará la concienciación en torno a la inteligencia artificial en todos los niveles de la educación a fin de capacitar a los ciudadanos para que tomen decisiones con fundamento bajo una influencia cada vez mayor de la IA.

Desarrollar las habilidades necesarias para trabajar en el ámbito de la inteligencia artificial y mejorar las cualificaciones profesionales de los trabajadores para adaptarlas a la transformación que implica esta tecnología será una prioridad del Plan coordinado sobre la IA revisado que debe desarrollarse con los Estados miembros. Ello puede implicar transformar la lista de evaluación de las directrices éticas en un «currículo» indicativo para los desarrolladores de IA que se pondrá a disposición de las instituciones de formación. Es necesario realizar esfuerzos específicos para incrementar el número de mujeres que se forman y son contratadas en esta área.

[19] El futuro Fondo Europeo de Defensa y la Cooperación Estructurada Permanente (CEP) también ofrecerán oportunidades de investigación y desarrollo en el ámbito de la inteligencia artificial. Estos proyectos deben sincronizarse con los programas civiles de inteligencia artificial más generales de la UE.

[20] https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu.

Además, el centro de referencia de investigación e innovación en IA de Europa debe atraer a talentos de todo el mundo gracias a las posibilidades que puede ofrecer. También desarrollará y ampliará la excelencia de las habilidades que se originan y propagan por toda Europa.

- *Acción 3: Mediante el pilar de capacidades avanzadas del Programa Europa Digital, establecer y respaldar redes de universidades y centros de educación superior pioneros, a fin de atraer a los mejores académicos y científicos y de ofrecer programas de máster en IA que se sitúen a la vanguardia mundial.*

Más allá de la mejora de las cualificaciones profesionales, los trabajadores y las empresas experimentan las consecuencias directas del diseño y el uso de los sistemas de inteligencia artificial en el lugar de trabajo. La participación de los interlocutores sociales será un factor decisivo para garantizar un enfoque antropocéntrico de la IA en el trabajo.

D. PREOCUPARSE POR LAS PYMES

También será importante garantizar que las pymes puedan acceder a la inteligencia artificial y que la utilicen. Para ello, los centros de innovación digital[21] y la plataforma de «inteligencia artificial a la carta»[22] deben seguir reforzándose y potenciar la cooperación entre pymes. El Programa Europa Digital será clave para alcanzar este objetivo. Si bien todos los centros de innovación digital deben apoyar a las pymes para que entiendan y adopten la inteligencia artificial, será importante que al menos un centro de innovación por Estado miembro cuente con un elevado nivel de especialización en inteligencia artificial.

Las pymes y empresas emergentes necesitarán tener acceso a la financiación para adaptar sus procedimientos o innovar usando la IA. Mediante el inminente fondo de inversión piloto de 100 millones EUR para la inteligencia artificial y la cadena de bloques, la Comisión prevé seguir incrementando el acceso a la financiación en la IA en el marco de InvestEU[23]. La inteligencia artificial figura de manera explícita como uno de los sectores admisibles en InvestEU.

- *Acción 4: La Comisión trabajará con los Estados miembros para garantizar que al menos un centro de innovación digital por Estado miembro cuente con un elevado nivel de especialización en inteligencia artificial. Los centros de innovación digital pueden contar con el respaldo del Programa Europa Digital.*
- *La Comisión y el Fondo Europeo de Inversiones pondrán en marcha un plan piloto de 100 millones EUR en el primer cuatrimestre de 2020 con el objetivo de ofrecer financiación mediante fondos propios para el desarrollo innovador de la inteligencia artificial. A la espera de un acuerdo definitivo sobre el marco financiero plurianual, la intención de la Comisión es incrementar significativamente estos importes de 2021 en adelante, a través de InvestEU.*

E. ASOCIACIONES CON EL SECTOR PRIVADO

Además, resulta fundamental asegurarse de que el sector privado participe plenamente en la elaboración de la agenda de investigación e innovación y ofrezca el nivel de coinversión necesario. Ello exige que se establezca una asociación público-privada con carácter amplio, y que se garantice el compromiso de los altos cargos de las empresas.

[21] ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.
[22] www.Ai4eu.eu.
[23] https://europa.eu/investeu/home_es.

- *Acción 5: En el marco de Horizonte Europa, la Comisión creará una nueva asociación público-privada en materia de inteligencia artificial, datos y robótica, a fin de aunar esfuerzos, garantizar la coordinación de la investigación y la innovación en inteligencia artificial, colaborar con otras asociaciones público-privadas de Horizonte Europa y trabajar conjuntamente con las instalaciones de ensayo y los centros de innovación digital ya mencionados.*

F. PROMOVER LA ADOPCIÓN DE LA IA POR PARTE DEL SECTOR PÚBLICO

Resulta fundamental que las Administraciones Públicas, los hospitales, los servicios públicos y de transporte, los supervisores financieros y otras áreas de interés público empiecen a adoptar rápidamente productos y servicios que se basen en la inteligencia artificial en sus actividades. Se hará especial hincapié en los sectores de la atención sanitaria y el transporte, en los que la tecnología está suficientemente desarrollada para una adopción a gran escala.

- *Acción 6: La Comisión iniciará conversaciones por sector abiertas y transparentes, en las que dará prioridad a la atención sanitaria, las administraciones rurales y los operadores de servicios públicos, para presentar un plan de acción que facilite el desarrollo, la experimentación y la adopción de la inteligencia artificial. Las conversaciones por sector se emplearán para preparar un «Programa de adopción de la IA» específico que respaldará la contratación pública de sistemas de inteligencia artificial, y ayudará a transformar los propios procesos de esta contratación.*

G. ASEGURAR EL ACCESO A LOS DATOS Y LAS INFRAESTRUCTURAS INFORMÁTICAS

Las áreas de acción establecidas en el presente Libro Blanco completan el plan presentado en paralelo en el marco de la Estrategia Europea de Datos. Mejorar el acceso a los datos y la gestión de estos últimos resulta fundamental. Sin datos, el desarrollo de la IA y otras aplicaciones digitales resulta imposible. El enorme volumen de datos nuevos que está por generarse es una oportunidad para que Europa se posicione en la primera línea de la transformación en materia de datos e inteligencia artificial. Promover prácticas de gestión responsable de los datos e incentivar el cumplimiento, en lo que respecta a estos últimos, de los principios FAIR contribuirá a generar confianza y a posibilitar su reutilización[24]. La inversión en infraestructuras y tecnologías informáticas clave es igualmente importante.

La Comisión ha propuesto más de 4 000 millones EUR en el marco del Programa Europa Digital para respaldar la computación de alto rendimiento y la computación cuántica, especialmente la computación en el borde y la inteligencia artificial, así como las infraestructuras de la nube y de datos. La Estrategia Europea de Datos desarrolla estas prioridades con mayor detalle.

H. ASPECTOS INTERNACIONALES

Europa se encuentra en una buena posición para asumir el liderazgo mundial a la hora de crear alianzas en torno a valores compartidos y promover el uso ético de la inteligencia artificial. El trabajo de la UE sobre inteligencia artificial ya ha tenido influencia en distintas negociaciones internacionales. A la hora de elaborar sus directrices éticas, el grupo de expertos de alto nivel contó con la participación de varias organizaciones de fuera de la UE y de diversos observadores gubernamentales. Paralelamente, la UE colaboró estrechamente en la elaboración de los principios éticos de la OCDE en materia de IA[25]. Posteriormente, el G20 suscribió estos principios en su Declaración Ministerial sobre Comercio y Economía Digital de junio de 2019.

De manera simultánea, la UE admite que está realizando una importante labor sobre la inteligencia artificial en otros foros multilaterales, como el Consejo de Europa, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Organización Mundial del Comercio y la Unión Internacional de

[24] Fáciles de encontrar, accesibles, interoperables y reutilizables, tal como se contempla en el informe final y el Plan de Acción del Grupo de Expertos en datos FAIR de la Comisión, de 2018 (https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf).

[25] https://www.oecd.org/going-digital/ai/principles/.

Telecomunicaciones (UIT). En las Naciones Unidas, la UE participa en el seguimiento del informe del Panel de Alto Nivel sobre la Cooperación Digital, incluida su recomendación sobre inteligencia artificial.

La UE seguirá cooperando en torno a la IA con países de mentalidad similar, pero también con terceras partes de todo el mundo, sobre la base de un enfoque fundamentado en las normas y valores de la UE (por ejemplo, respaldando una mayor convergencia normativa; mediante el acceso a recursos clave, como los datos; o creando un entorno de igualdad de condiciones). La Comisión seguirá de cerca las políticas de terceros países que limitan los flujos de datos y hará frente a las restricciones indebidas en las negociaciones comerciales bilaterales y mediante acciones en el contexto de la Organización Mundial del Comercio. La Comisión está convencida de que la cooperación internacional sobre cuestiones relativas a la IA debe basarse en un enfoque que promueva el respeto de los derechos fundamentales, especialmente la dignidad humana, el pluralismo, la inclusión, la ausencia de discriminación y la protección de la privacidad y de los datos personales[26], y se esforzará por exportar estos valores al resto del mundo[27]. Igualmente, resulta evidente que un desarrollo y un uso responsables de la IA pueden ser un motor para alcanzar los Objetivos de Desarrollo Sostenible y progresar en la Agenda 2030.

5. UN ECOSISTEMA DE CONFIANZA: EL MARCO REGULADOR DE LA IA

Como sucede con toda nueva tecnología, el uso de la IA presenta tanto oportunidades como amenazas. Los ciudadanos temen quedarse indefensos a la hora de proteger sus derechos y su seguridad frente a los desequilibrios informativos de la toma de decisiones mediante algoritmos, y las empresas sienten inquietud debido a la inseguridad jurídica. Si bien la inteligencia artificial puede ayudar a proteger la seguridad de los ciudadanos y permitirles gozar de sus derechos fundamentales, a estos también les preocupa el hecho de que la IA pueda tener efectos imprevistos o incluso que pueda utilizarse con fines malintencionados. Es preciso tener en cuenta esos recelos. Además, a la falta de inversión y de habilidades, es preciso añadir la falta de confianza como uno de los principales obstáculos para una adopción más amplia de la IA.

Esta es la razón por la que, el 25 de abril de 2018, la Comisión estableció una estrategia sobre IA[28] que abordaba los aspectos socioeconómicos junto con un aumento de la inversión en investigación, innovación y capacidad en materia de IA en toda la UE. También aprobó un Plan coordinado[29] con los Estados miembros para armonizar estrategias. La Comisión creó, además, un grupo de expertos de alto nivel que, en abril de 2019, publicó directrices para una IA fiable[30].

La Comisión publicó una Comunicación[31] según la cual acogía favorablemente los siete requisitos esenciales contemplados en las directrices del grupo de expertos de alto nivel, a saber:

- acción y supervisión humanas;
- solidez técnica y seguridad;
- gestión de la privacidad y de los datos;
- transparencia;
- diversidad, no discriminación y equidad;

[26] En el marco del Instrumento de Asociación, la Comisión financiará un proyecto de 2,5 millones EUR que facilitará la cooperación con socios de mentalidad similar, a fin de promover las directrices éticas en materia de IA de la UE y de adoptar principios y conclusiones operativas.
[27] Presidenta von der Leyen, «Una Unión que se esfuerza por lograr más resultados. Mi agenda para Europa», página 17.
[28] COM(2018) 237.
[29] COM(2018) 795.
[30] https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top.
[31] COM(2019) 168.

- bienestar social y medioambiental;
- rendición de cuentas.

Además, las directrices facilitan una lista para que las empresas comprueben en la práctica si se cumplen los requisitos. Durante la segunda mitad de 2019, más de 350 organizaciones probaron esta lista y enviaron sus observaciones al respecto. El grupo de expertos de alto nivel está revisando las directrices a partir de estas observaciones y terminará esta labor de aquí a junio de 2020. Una observación fundamental tras el proceso de consultas es que, si bien varios de los requisitos se recogen ya en los regímenes jurídicos o reguladores, aquellos relativos a la transparencia, el seguimiento y la supervisión humana no se contemplan de manera específica en la legislación en vigor de numerosos sectores económicos.

Además de este conjunto de directrices no vinculantes del grupo de expertos de alto nivel, y de conformidad con las orientaciones políticas de la presidenta, un marco regulador claro para Europa generaría confianza entre los consumidores y las empresas con relación a la IA, y, por consiguiente, aceleraría su adopción. Dicho marco regulador debe ser coherente con otras acciones destinadas a promover la capacidad innovadora y la competitividad de Europa en el sector. Además, debe garantizar resultados óptimos desde el punto de vista social, medioambiental y económico, así como su conformidad con la legislación, los principios y los valores de la UE. Ello resulta especialmente relevante en sectores en los que los derechos de los ciudadanos se vean afectados de manera más directa; por ejemplo, en el caso de las aplicaciones de IA empleadas por los cuerpos y fuerzas de seguridad y el poder judicial.

Los desarrolladores e implementadores de la inteligencia artificial ya están sujetos a la legislación europea en materia de derechos fundamentales (la protección de datos, la privacidad o la no discriminación, entre otros), protección de los consumidores y normas sobre la seguridad de los productos y responsabilidad civil. Los consumidores esperan el mismo nivel de seguridad y respeto de sus derechos independientemente de si un producto o un sistema está basado en la IA o no. Sin embargo, algunas características específicas de la IA (como la opacidad) pueden hacer que la aplicación y ejecución de la legislación sea más compleja. Por esta razón, resulta necesario analizar si la legislación actual puede hacer frente a los riesgos de la IA y si su observancia es factible o si, por el contrario, es necesario adaptarla o se requiere nueva legislación.

Debido a la rapidez con la que evoluciona la inteligencia artificial, el marco regulador debe dejar margen para abordar su desarrollo en el futuro. Toda modificación debe limitarse a aquellos problemas detectados con claridad para los que existan soluciones factibles.

Los Estados miembros señalan la actual falta de un marco común europeo. El Comité alemán sobre ética en materia de datos propone un sistema de regulación de cinco niveles basado en el riesgo, que va desde la ausencia de regulación en el caso de los sistemas de IA más inocuos hasta la prohibición absoluta en el caso de los más peligrosos. Dinamarca acaba de poner en marcha un prototipo de «sello de ética de los datos». Malta ha incorporado un sistema voluntario de certificación de la IA. Si la UE no es capaz de ofrecer un enfoque a escala de la Unión, existe un riesgo real de fragmentación del mercado interior, que pondría en peligro los objetivos de la confianza y la seguridad jurídica, así como el de la adopción de la IA en el mercado.

Un marco regulador europeo sólido que garantice una IA fiable protegerá a todos los ciudadanos europeos y contribuirá a crear un mercado interior sin fricciones de cara al desarrollo y adopción futuros de la IA, y reforzará los cimientos industriales de Europa en el sector de la inteligencia artificial.

A. DEFINICIÓN DE LOS PROBLEMAS

Aunque la IA puede ofrecer muchas ventajas, por ejemplo, mejorando la seguridad de los productos y los procedimientos, también puede resultar nociva. Los daños pueden ser tanto materiales (para la seguridad y la salud de las personas, con consecuencias como la muerte, y menoscabos al patrimonio) como inmateriales (pérdida de privacidad, limitaciones del derecho de libertad de expresión, dignidad humana, discriminación en el acceso al empleo, etc.) y pueden estar vinculados a una gran variedad de riesgos. El marco regulador debe centrarse en cómo minimizar los distintos riesgos de sufrir daños, especialmente los más significativos.

Los principales riesgos relacionados con el uso de la inteligencia artificial afectan a la aplicación de las normas diseñadas para proteger los derechos fundamentales (como la protección de los datos personales y la privacidad, o la no discriminación) y la seguridad[32], así como a las cuestiones relativas a la responsabilidad civil.

Riesgos para los derechos fundamentales, especialmente la protección de los datos personales y de la privacidad y la no discriminación

El uso de la inteligencia artificial puede afectar a los valores sobre los que se fundamenta la UE y provocar la conculcación de derechos fundamentales[33], como la libertad de expresión, la libertad de reunión, la dignidad humana, la ausencia de discriminación por razón de sexo, raza u origen étnico, religión o credo, discapacidad, edad u orientación sexual, y, en su aplicación en determinados ámbitos, la protección de los datos personales y de la vida privada [34], el derecho a una tutela judicial efectiva y a un juicio justo, o la protección de los consumidores. Estos riesgos pueden ser resultado de defectos en el diseño general de los sistemas de IA (especialmente en lo que se refiere a la supervisión humana) o del uso de datos que puedan ser sesgados sin una corrección previa (por ejemplo, se entrena un sistema utilizando única o principalmente datos relativos a hombres, y ello se traduce en resultados peores con relación a las mujeres).

La inteligencia artificial puede desempeñar muchas funciones que antes solo podían realizar los humanos. Como resultado, los ciudadanos y las personas jurídicas serán, cada vez más, objeto de acciones y decisiones adoptadas por sistemas de inteligencia artificial o con ayuda de estos; dichas acciones y decisiones, en ocasiones, pueden resultar difíciles de entender o de rebatir eficazmente cuando se requiera. Además, la IA incrementa las posibilidades de hacer un seguimiento y un análisis de las costumbres cotidianas de las personas. Por ejemplo, existe el riesgo potencial de que, incumpliendo las normas de la UE en materia de protección de datos u otras normas, las autoridades estatales y otros organismos recurran a la IA para la vigilancia masiva, o las empresas la utilicen para observar cómo se comportan sus empleados. Al analizar grandes cantidades de datos y detectar la conexión existente entre ellos, la IA también puede utilizarse para rastrear y desanonimizar datos relativos a personas, y generar así nuevos riesgos en torno a la protección de los datos personales con relación a conjuntos de datos que, en sí mismos, no contienen datos personales. Los intermediarios de la red también utilizan la IA para ordenar la información para sus usuarios por prioridades y moderar

[32] Como la ciberseguridad, los problemas vinculados a las aplicaciones de IA en infraestructuras clave, o el uso malintencionado de la IA.

[33] Según el trabajo de investigación del Consejo de Europa, un gran número de derechos fundamentales podría verse afectado por el uso de la IA (https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5).

[34] El Reglamento General de Protección de Datos y la Directiva sobre la privacidad y las comunicaciones electrónicas (nuevo Reglamento sobre la privacidad y las comunicaciones electrónicas en fase de negociación) aborda estos riesgos, aunque puede que sea necesario examinar si los sistemas de IA plantean riesgos adicionales. La Comisión supervisará y evaluará la aplicación del RGPD de manera continuada.

los contenidos. El tratamiento de los datos, el modo en el que se diseñan las aplicaciones y la envergadura de la intervención humana pueden afectar a los derechos de libertad de expresión, protección de los datos personales, privacidad y libertad política.

Los prejuicios y la discriminación son riesgos inherentes a toda actividad social o económica. La toma de decisiones de las personas no es ajena al error ni a la subjetividad. No obstante, en el caso de la IA, esta misma subjetividad puede tener efectos mucho más amplios, y afectar y discriminar a numerosas personas sin que existan mecanismos como los de control social que rigen el comportamiento humano[35]. Puede suceder también que el sistema de IA «aprenda» mientras está funcionando. En tales casos, cuando los resultados no puedan preverse ni anticiparse en la fase de diseño, los riesgos no se deberán a fallos en el diseño original del sistema, sino más bien a las repercusiones prácticas de las correlaciones

> Puede suceder que el uso de determinados algoritmos de la IA para predecir la reincidencia delictiva dé lugar a prejuicios raciales o de género, y prevea una probabilidad de reincidencia distinta para hombres y mujeres o para nacionales y extranjeros. *Fuente: Tolan S., Miron M., Gomez E. and Castillo C. "Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia", Best Paper Award, International Conference on AI and Law, 2019.*
>
> Algunos programas de IA de análisis facial muestran prejuicios raciales o de género, y presentan un bajo nivel de error a la hora de determinar el género de hombres de piel más clara, pero un elevado nivel de error al determinar el género de mujeres de piel más oscura. Fuente: *Joy Buolamwini, Timnit Gebru; Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018.*

o de los modelos que reconozca el sistema en un gran conjunto de datos.

Las características particulares de numerosas tecnologías de IA, como la opacidad («efecto caja negra»), la complejidad, la imprevisibilidad y un comportamiento parcialmente autónomo, pueden hacer difícil comprobar el cumplimiento de la legislación vigente de la UE sobre la protección de los derechos fundamentales e impedir su cumplimiento efectivo. Puede ser que las fuerzas y cuerpos de seguridad y las personas afectadas carezcan de los medios para comprobar cómo se ha tomado una decisión determinada con ayuda de la IA y, por consiguiente, si se han respetado las normas pertinentes. Las personas físicas y las personas jurídicas pueden enfrentarse a dificultades en el acceso efectivo a la justicia en situaciones en las que estas decisiones les afecten negativamente.

Riesgos para la seguridad y el funcionamiento eficaz del régimen de responsabilidad civil

Las tecnologías de IA pueden presentar nuevos riesgos de seguridad para los usuarios cuando estén integradas en productos y servicios. Por ejemplo, como resultado de un defecto en la tecnología de reconocimiento de objetos, un vehículo autónomo puede detectar erróneamente un objeto en la carretera y causar un accidente que provoque heridos y daños materiales. Como sucede con los riesgos para los derechos fundamentales, estos riesgos pueden proceder de defectos en el diseño de la tecnología de IA,

[35] El Comité consultivo para la igualdad de oportunidades entre mujeres y hombres de la Comisión está preparando en la actualidad un dictamen sobre la inteligencia artificial, que analiza, entre otras cuestiones, las repercusiones de esta última en la igualdad de género, y cuya adopción por el Comité está prevista a principios de 2020. La Estrategia de la UE para la igualdad de género 2020-2024 también aborda el vínculo entre la IA y la igualdad de género. La red europea de organismos para la igualdad (Equinet) publicará un informe (de Robin Allen y Dee Masters) titulado «La regulación de la IA: el nuevo papel de los organismos para la igualdad. Cómo hacer frente a los retos en materia de igualdad y no discriminación derivados de la mayor digitalización y uso de la IA», previsto para principios de 2020.

estar relacionados con problemas de disponibilidad o calidad de los datos, u otros derivados del aprendizaje de las máquinas. Aunque algunos de estos riegos no se limitan a los productos o servicios que dependen de la IA, el uso de esta última puede aumentar o agravar los riesgos.

Además de los riesgos a los que se enfrentan estas personas, la falta de disposiciones claras en materia de seguridad para abordarlos puede crear inseguridad jurídica entre las empresas que comercializan productos que utilicen IA en la UE. Las autoridades encargadas de supervisar el mercado o de ejecutar las normas pueden encontrarse en una situación en la que les resulte confuso cómo intervenir, puesto que tal vez no estén facultadas para tomar medidas o no cuenten con la capacidades técnicas adecuadas para examinar los sistemas[36]. Por consiguiente, la inseguridad jurídica puede reducir los niveles globales de seguridad y minar la competitividad de las empresas europeas.

Si los riesgos de seguridad se materializan, la falta de requisitos claros y las características de las tecnologías de IA mencionadas anteriormente pueden complicar la trazabilidad de las decisiones potencialmente problemáticas que se hayan tomado con ayuda de sistemas de IA. A su vez, esto puede dificultar a las personas damnificadas recibir compensaciones en el marco de la normativa en materia de responsabilidad civil en vigor en la UE y los distintos países[37].

En el marco de la Directiva sobre responsabilidad por los daños causados por productos defectuosos, un fabricante es responsable de los daños causados por un producto defectuoso. No obstante, en el caso de un sistema basado en la IA, como un vehículo autónomo, puede resultar difícil demostrar la existencia de un defecto en el producto, el daño que este ha generado y el nexo causal entre ambos. Además, hay cierta incertidumbre sobre cómo y en qué medida resulta aplicable la Directiva sobre responsabilidad por los daños causados por productos defectuosos en el caso de algunos tipos de defectos, por ejemplo, cuando estos se deban a una falla en la ciberseguridad del producto.

Por consiguiente, la dificultad para hacer un seguimiento retrospectivo de las decisiones potencialmente problemáticas adoptadas mediante sistemas de IA y contempladas anteriormente con relación a los derechos fundamentales es aplicable tanto a los problemas de seguridad como de responsabilidad civil. Es posible que las personas que hayan sufrido daños no dispongan de un acceso efectivo a las pruebas necesarias para llevar un caso ante los tribunales, por ejemplo, y tengan menos probabilidades de obtener una reparación efectiva en comparación con situaciones en las que los daños sean causados por tecnologías tradicionales. Estos riesgos aumentarán a medida que se generaliza el uso de la IA.

[36] Un ejemplo pueden ser los relojes de pulsera inteligentes para niños. Es posible que este producto no cause daños directos a quienes lo utilizan, pero si no se prevé un nivel mínimo de seguridad, puede convertirse fácilmente en una herramienta de acceso al niño. Es posible que las autoridades encargadas de supervisar el mercado tengan dificultades para intervenir en casos en los que el riesgo no esté vinculado al producto en sí mismo.

[37] Finalmente, en el informe de la Comisión adjunto al presente Libro Blanco, se analizan las repercusiones de la inteligencia artificial, el internet de las cosas y otras tecnologías digitales para la normativa en materia de seguridad y responsabilidad civil.

B. POSIBLES ADAPTACIONES DEL MARCO NORMATIVO EN VIGOR EN LA UE CON RELACIÓN A LA IA

Un amplio volumen de la legislación en vigor en la UE en materia de seguridad de los productos y responsabilidad civil[38], especialmente determinadas normas sectoriales, completadas a su vez por la legislación nacional, resulta pertinente y de potencial aplicación a varias de las nuevas aplicaciones de IA.

En lo que se refiere a la protección de los derechos fundamentales y los derechos de los consumidores, el marco normativo de la UE contiene legislación como la Directiva sobre igualdad racial[39], la Directiva sobre igualdad de trato en el empleo y la ocupación[40], las Directivas relativas a la igualdad de trato entre mujeres y hombres con relación al empleo y el acceso a los bienes y servicios[41], varias normas de protección de los consumidores[42] y normas sobre la protección de los datos personales y la privacidad, especialmente el Reglamento General de Protección de Datos y otra legislación sectorial en la que se contempla la protección de los datos personales, como la Directiva sobre protección de datos en el ámbito penal[43]. Además, a partir de 2025, resultarán de aplicación las normas sobre los requisitos de accesibilidad de bienes y servicios establecidas en el Acta Europea de Accesibilidad[44]. Por otra parte, es necesario respetar los derechos fundamentales cuando se ejecuten otras normas de la UE, como las relativas al sector de los servicios financieros, la migración o la responsabilidad de los intermediarios en línea.

Si bien la legislación de la UE resulta, en principio, plenamente aplicable independientemente del uso de IA, resulta importante evaluar si puede ejecutarse de manera adecuada para abordar los riesgos que generan los sistemas de IA, o si se requiere adaptar instrumentos jurídicos específicos.

Por ejemplo, los agentes económicos siguen siendo plenamente responsables de que la IA respete las normas existentes en materia de protección de los consumidores. Igualmente, debe prohibirse todo uso de los algoritmos con relación al comportamiento de los consumidores cuando se vulneren las normas existentes, y tales vulneraciones deben sancionarse en consecuencia.

La Comisión considera que conviene mejorar el marco normativo para abordar los riesgos y situaciones siguientes:

- *Aplicación y ejecución efectivas de la legislación nacional y de la UE en vigor*: Las características fundamentales de la IA entrañan dificultades para garantizar la correcta aplicación y ejecución de la legislación nacional y de la UE. La falta de transparencia (opacidad de la IA) hace difícil detectar y demostrar los posibles incumplimientos de la legislación, especialmente las disposiciones legales que protegen los derechos fundamentales, imputan responsabilidades y permiten reclamar una indemnización. Por tanto, a fin de garantizar una aplicación y ejecución efectivas, puede resultar necesario adaptar o clarificar la legislación en

[38] El marco jurídico de la UE sobre la seguridad de los productos lo componen la Directiva sobre seguridad general de los productos (Directiva 2001/95/CE), a modo de red de seguridad, y varias normas sectoriales que engloban distintas categorías de productos, que van desde las máquinas, los aviones y los vehículos, hasta los juguetes y los productos sanitarios, destinadas a ofrecer un alto nivel de salud y seguridad. La legislación sobre responsabilidad civil por los productos la completan distintos sistemas responsabilidad civil por los daños ocasionados por los productos o servicios.

[39] Directiva 2000/43/CE.

[40] Directiva 2000/78/CE.

[41] Directiva 2004/113/CE; Directiva 2006/54/CE.

[42] Como la Directiva sobre las prácticas comerciales desleales (Directiva 2005/29/CE) y la Directiva sobre los derechos de los consumidores (Directiva 2011/83/CE).

[43] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

[44] Directiva (UE) 2019/882, sobre los requisitos de accesibilidad de los productos y servicios.

vigor en algunos sectores, como sucede en el caso de la responsabilidad civil, tal como se detalla en el informe adjunto al presente Libro Blanco.

- *Limitaciones del ámbito de aplicación de la legislación existente de la UE*: Uno de los centros de interés fundamentales de la legislación sobre seguridad de los productos en la UE lo constituye la comercialización de los productos. Aunque, en la legislación de la UE en materia de seguridad de los productos, los programas informáticos que forman parte de un producto final deben respetar las normas de seguridad del producto pertinentes, existe la duda de si un programa autónomo se rige por la legislación de seguridad de los productos de la UE, salvo en aquellos sectores que cuentan con normas explícitas[45]. La legislación general de la UE en materia de seguridad en vigor resulta de aplicación a los productos y no a los servicios, y, por consiguiente, *a priori* no se aplica tampoco a los servicios basados en las tecnologías de IA (como servicios sanitarios, financieros o de transporte).

- *Cambios en la funcionalidad de los sistemas de IA*: La incorporación de programas informáticos, incluida la IA, en los productos puede modificar el funcionamiento de tales productos y sistemas a lo largo de su ciclo de vida. Ello resulta particularmente cierto en el caso de los sistemas que requieren actualizaciones informáticas frecuentes o que se basan en el aprendizaje automático. Estas características pueden dar lugar a nuevos riesgos que no existían en el momento en que se introdujo el sistema en el mercado. Estos riesgos no se abordan adecuadamente en la legislación en vigor, que se centra sobre todo en los riesgos de seguridad en el momento de la comercialización.

- *Incertidumbre en lo que se refiere a la imputación de responsabilidades entre los distintos agentes económicos de la cadena de suministro*: En general, la legislación de la UE sobre la seguridad de los productos imputa la responsabilidad al productor del producto comercializado, incluidos todos sus componentes, como los sistemas de IA. Sin embargo, estas normas pueden resultar poco claras cuando la IA es incorporada al producto, una vez que este se ha comercializado, por alguien que no es el productor. Además, la legislación de la UE sobre la responsabilidad civil por los productos regula la responsabilidad de los productores y deja que las normas nacionales en materia de responsabilidad civil se encarguen de los demás participantes en la cadena de suministro.

- *Cambios en el concepto de seguridad*: El uso de la IA en los productos y los servicios puede generar riesgos que la legislación de la UE no aborda de manera explícita en la actualidad. Estos riesgos pueden estar vinculados a ciberamenazas, a la seguridad personal (por ejemplo, con relación a nuevos usos de la IA, como en el caso de los aparatos domésticos), a la pérdida de conectividad, etc., y pueden existir en el momento de comercializar los productos o surgir como resultado de la actualización de los programas informáticos y del aprendizaje automático del producto cuando este último se está utilizando. La UE debe hacer un uso pleno de las herramientas que están a su disposición para reforzar su base empírica sobre los riesgos potenciales asociados a las aplicaciones de IA, y aprovechar especialmente la experiencia de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) para evaluar el panorama de amenazas de la IA.

[45] Por ejemplo, de acuerdo con el Reglamento sobre los productos sanitarios [Reglamento (UE) 2017/745], los programas informáticos destinados a fines médicos por el fabricante se consideran productos sanitarios.

Como se ha señalado, ya hay varios Estados miembros que están valorando alternativas en su legislación nacional para hacer frente a los retos que presenta la IA. Esto a su vez conlleva el riesgo de que se fragmente el mercado único. Es probable que las diferencias entre normas nacionales creen obstáculos para las empresas que deseen vender y utilizar sistemas de IA en el mercado único. Garantizar

Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica

El informe, adjunto al presente Libro Blanco, analiza el marco jurídico pertinente. Señala las incertidumbres sobre la aplicación de este marco con relación a los riesgos concretos que presentan los sistemas de IA y otras tecnologías digitales.

Llega a la conclusión de que la legislación vigente sobre seguridad de los productos ya recoge un concepto amplio de protección de la seguridad frente a todo tipo de riesgos derivados del producto en función de su uso. No obstante, cabe introducir disposiciones que aborden de manera explícita los nuevos riesgos derivados de las tecnologías digitales emergentes, a fin de ofrecer mayor seguridad jurídica.

- El comportamiento autónomo de algunos sistemas de IA a lo largo de su ciclo de vida puede conllevar importantes cambios en los productos y tener repercusiones en la seguridad, lo que puede requerir una nueva evaluación de riesgos. Además, es probable que se requiera la supervisión humana como garantía, desde la fase de diseño y a lo largo de todo el ciclo de vida de los productos y sistemas de IA.
- También pueden valorarse obligaciones explícitas para los productores con relación a los riesgos para la salud mental de los usuarios cuando así se requiera (por ejemplo, en el caso de la colaboración con robots humanoides).
- La legislación de la UE sobre seguridad de los productos puede prever requisitos específicos para abordar los riesgos derivados de los datos incorrectos en la fase de diseño, así como mecanismos para garantizar que la calidad de los datos se mantenga mientras se usen los productos y sistemas de IA.
- La opacidad de los sistemas basados en algoritmos puede abordarse mediante requisitos de transparencia.
- Es posible que sea necesario adaptar y clarificar las normas en vigor en el caso de los programas autónomos comercializados separadamente o descargados en un producto tras la comercialización de este último, cuando tengan repercusiones en la seguridad.
- Dada la complejidad creciente de las cadenas de suministro en lo que se refiere a las nuevas tecnologías, las disposiciones que exigen de manera específica colaboración entre los agentes económicos de la cadena y los usuarios pueden aportar seguridad jurídica.

Las características de las tecnologías digitales emergentes, como la inteligencia artificial, el internet de las cosas y la robótica, pueden poner en cuestión algunos elementos de los marcos de responsabilidad civil y reducir su eficacia. Algunas de estas características podrían dificultar la trazabilidad de los daños sufridos por una persona, lo que resultaría necesario en el caso de una demanda de responsabilidad civil subjetiva según la mayoría de las normas nacionales. Ello podría aumentar significativamente los costes para las víctimas, y haría más difícil exigir o demostrar la responsabilidad civil de los agentes que no sean los productores.

- Las personas damnificadas por sistemas de IA deben poder disfrutar del mismo nivel de protección que las personas que hayan sufrido daños causados por otras tecnologías, aunque al mismo tiempo es necesario permitir el avance de la innovación tecnológica.
- Es necesario valorar todas las alternativas para alcanzar este objetivo, incluidas las posibles modificaciones de la Directiva sobre responsabilidad por los daños causados por productos defectuosos o la posibilidad de seguir adaptando las medidas nacionales en materia de responsabilidad civil. Por ejemplo, la Comisión está recabando opiniones sobre cómo y en qué medida puede ser necesario atenuar las consecuencias de la complejidad mediante una adaptación de la carga de la prueba exigida por las normas nacionales sobre responsabilidad civil en el caso de los daños causados por el funcionamiento de las aplicaciones de IA.

un enfoque común a escala de la UE permitirá a las empresas europeas beneficiarse de un acceso sencillo al mercado único y respaldar su competitividad en los mercados mundiales.

A la luz de todo lo expuesto, la Comisión llega a la conclusión de que, además de las posibles adaptaciones de la legislación vigente, puede que se requiera nueva legislación específica sobre IA, a fin de adaptar el marco jurídico de la UE a la evolución tecnológica y comercial actual y futura.

C. ÁMBITO DE APLICACIÓN DE UN FUTURO MARCO REGULADOR DE LA UE

Un elemento clave para la elaboración de un futuro marco regulador específico sobre la IA es determinar su ámbito de aplicación. La hipótesis de trabajo es que el marco regulador debe resultar de aplicación a los productos y servicios basados en la IA. Por consiguiente, es necesario definir claramente la IA a los efectos del presente Libro Blanco y de toda posible iniciativa de elaboración de políticas del futuro.

En su Comunicación sobre la inteligencia artificial para Europa, la Comisión ofrecía una primera definición de la IA[46]. El grupo de expertos de alto nivel perfeccionó esta definición[47].

En los nuevos instrumentos jurídicos, la definición de la IA tendrá que ser suficientemente flexible para adaptarse al progreso técnico al tiempo que mantiene un nivel de precisión adecuado para ofrecer la seguridad jurídica necesaria.

A los efectos del presente Libro Blanco, así como de todo posible debate sobre iniciativas políticas en el futuro, parece importante clarificar cuáles son los principales elementos que integran la IA, a saber: los «datos» y los «algoritmos». La IA puede incorporarse en los equipos informáticos. En lo que se refiere a las técnicas de aprendizaje automático, que constituyen un subapartado de la IA, los algoritmos son entrenados para inferir determinados modelos a partir de un conjunto de datos, a fin de determinar las acciones que se requieren para alcanzar un objetivo determinado. Los algoritmos pueden seguir aprendiendo mientras se utilizan. Aunque los productos basados en la IA pueden funcionar de manera autónoma a partir de su percepción del entorno y sin seguir un conjunto predefinido de instrucciones, su comportamiento lo definen y restringen en gran medida sus desarrolladores. Los objetivos los definen y programan las personas, y los sistemas de IA deben optimizarse para alcanzarlos.

> En el caso de la conducción automática, por ejemplo, el algoritmo usa, en tiempo real, los datos del vehículo (velocidad, consumo del motor, amortiguadores, etc.) y de los sensores que examinan el entorno global (carretera, señales, otros vehículos, peatones, etc.) para determinar qué dirección tomar, o qué aceleración y velocidad requiere el vehículo para llegar a determinado destino. A partir de los datos observados, el algoritmo se adapta a la situación de la carretera y las condiciones exteriores, como el comportamiento de otros conductores, para ofrecer la conducción más cómoda y segura posible.

[46] COM(2018) 237 final, p. 1: «El término "inteligencia artificial" (IA) se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción —con cierto grado de autonomía— con el fin de alcanzar objetivos específicos.
Los sistemas basados en la IA pueden consistir simplemente en un programa informático (p. ej. asistentes de voz, programas de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento facial y de voz), pero la IA también puede estar incorporada en dispositivos de hardware (p. ej. robots avanzados, automóviles autónomos, drones o aplicaciones del internet de las cosas)».

[47] Según la definición del grupo de expertos de alto nivel, p. 8: Los sistemas de inteligencia artificial (IA) son programas informáticos (y posiblemente también equipos informáticos) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno mediante la adquisición de datos, la interpretación de los datos estructurados o no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la información, fruto de estos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el objetivo fijado.

La UE cuenta con un marco jurídico estricto para garantizar, entre otros, la protección de los consumidores, la lucha contra las prácticas comerciales desleales y la protección de los datos personales y la privacidad. Además, el acervo de la UE cuenta con normas específicas en el caso de algunos sectores (como la sanidad o el transporte). Estas disposiciones del Derecho de la UE seguirán siendo de aplicación con relación a la IA, aunque puede que se requieran algunas actualizaciones del marco correspondiente a fin de reflejar la transformación digital y el uso de la IA (véase el apartado B). Como consecuencia, aquellos elementos que ya se abordan en la legislación horizontal y sectorial vigente (como es el caso de los equipos médicos[48] o de los sistemas de transporte) seguirán rigiéndose por dicha legislación.

En principio, el nuevo marco regulador en materia de IA debe ser eficaz para alcanzar sus objetivos sin ser excesivamente prescriptivo, lo que podría generar una carga desproporcionada, en especial para las pymes. Para alcanzar este equilibrio, la Comisión considera que debe seguir un enfoque basado en el riesgo.

Un enfoque basado en el riesgo resulta importante para asegurar que la intervención reguladora sea proporcionada. No obstante, requiere de criterios claros para establecer diferencias entre las distintas aplicaciones de IA, en especial para determinar si entrañan un riesgo elevado o no[49]. La definición de qué es una aplicación de IA de riesgo elevado debe ser clara y fácil de entender y de aplicar para todas las partes interesadas. No obstante, incluso cuando no se considere que una aplicación de IA entraña un riesgo elevado, esta debe seguir estando sujeta a las normas vigentes en la UE.

La Comisión considera que, en general, una aplicación de IA determinada debe considerarse de riesgo elevado en función de lo que esté en juego, y considerando si tanto el sector como el uso previsto suponen riesgos significativos, en especial desde la perspectiva de la protección de la seguridad, los derechos de los consumidores y los derechos fundamentales. De manera más específica, una aplicación de IA debe considerarse de riesgo elevado cuando presente la suma de los dos criterios siguientes:

- En primer lugar, que la aplicación de IA se emplee en un sector en el que, por las características o actividades que se llevan a cabo normalmente, es previsible que existan riesgos significativos. El primer criterio vela por que la intervención reguladora se centre en aquellas áreas en las que, de manera general, se considere que hay más probabilidad de que surjan riesgos. En el nuevo marco regulador deben detallarse de manera específica y exhaustiva los sectores que englobe. Por ejemplo, la sanidad, el transporte, la energía y determinados ámbitos del sector público[50]. Esta lista debe revisarse periódicamente y modificarse cuando proceda en función de los desarrollos pertinentes en la práctica.
- En segundo lugar, que la aplicación de IA en el sector en cuestión se use, además, de manera que puedan surgir riesgos significativos. Este segundo criterio refleja el reconocimiento de que no toda utilización de la IA en los sectores señalados implica necesariamente riesgos significativos. Por ejemplo, si bien la atención sanitaria puede ser un sector importante, un fallo en el sistema de asignación de citas de un hospital no supondrá en principio un riesgo significativo que justifique la intervención legislativa. La evaluación del nivel de riesgo de un uso determinado puede basarse en las repercusiones para las partes afectadas. Por ejemplo, el

[48] Por ejemplo, las consideraciones de seguridad y las implicaciones jurídicas son distintas en el caso de los sistemas de IA que ofrecen información médica especializada a los médicos, los sistemas de IA que ofrecen información médica al paciente y los sistemas de IA que ofrecen por sí solos prestaciones médicas al paciente directamente. La Comisión está examinando estos retos de seguridad y responsabilidad civil, que son distintos de la asistencia sanitaria.

[49] Puede que la legislación de la UE ofrezca categorías de «riesgos» distintas a las que se presentan aquí, en función del sector, como sucede, por ejemplo, en el caso de la seguridad de los productos.

[50] El sector público debe incluir ámbitos como el asilo, la migración, los controles fronterizos y el poder judicial, la seguridad social y los servicios de empleo.

uso de aplicaciones de IA con efectos jurídicos o similares en los derechos de un particular o de una empresa; aplicaciones que presenten el riesgo de causar lesiones, la muerte, o daños materiales o inmateriales significativos; aplicaciones que produzcan efectos que las personas físicas o jurídicas no puedan evitar razonablemente.

La aplicación de los dos criterios debe garantizar que el ámbito del marco regulador se adapte a lo necesario y ofrezca seguridad jurídica. En principio, los requisitos obligatorios contemplados en el nuevo marco regulador en materia de IA (véase el apartado D a continuación) deben resultar de aplicación únicamente a las aplicaciones que se consideren de elevado riesgo de conformidad con la suma de los dos criterios esbozados.

No obstante lo anterior, también puede haber casos excepcionales en los que, debido a lo que esté en peligro, el uso de aplicaciones de IA para determinados fines se considere de elevado riesgo en sí mismo; es decir, independientemente del sector de que se trate y cuando los requisitos que se presentan más abajo sigan siendo de aplicación[51]. Por ejemplo, cabría pensar en lo siguiente:

- En vista de su importancia para las personas y del acervo de la UE en materia de igualdad de empleo, el uso de las aplicaciones de IA en los procedimientos de contratación y en situaciones que repercutan en los derechos de los trabajadores debe considerarse siempre de «riesgo elevado» y, por consiguiente, los requisitos que se presentan a continuación han de ser aplicables en todos los casos. También pueden considerarse otras aplicaciones específicas con repercusiones en los derechos de los consumidores.

- El uso de aplicaciones de IA para la identificación biométrica remota[52] y otras tecnologías de vigilancia intrusiva deben considerarse siempre de «riesgo elevado» y, por tanto, los requisitos que se presentan a continuación deben resultar de aplicación en todos los casos.

D. TIPOS DE REQUISITOS

Cuando se diseñe el futuro marco regulador de la IA, será necesario determinar los tipos de requisitos legales obligatorios a los que deben atenerse las partes pertinentes. Estos requisitos pueden concretarse mediante normas. Como se señala en el apartado C, además de la legislación vigente, dichos requisitos deben aplicarse a las aplicaciones de IA que entrañen un riesgo elevado únicamente, para garantizar que toda intervención reguladora sea específica y proporcionada.

Teniendo en cuenta las directrices del grupo de expertos de alto nivel y lo previsto hasta el momento, los requisitos para las aplicaciones de IA que entrañen un riesgo elevado pueden contar con las características clave siguientes, que se abordan en mayor detalle en los subapartados posteriores:

- datos de entrenamiento;
- datos y registros de datos;
- información que debe facilitarse;
- solidez y exactitud;

[51] Cabe destacar que también otros ámbitos de la legislación de la UE pueden resultar de aplicación. Por ejemplo, cuando las aplicaciones de IA se integren en un producto de consumo, puede que su seguridad esté sujeta a la Directiva sobre seguridad general de los productos.

[52] La identificación biométrica remota debe distinguirse de la autenticación biométrica (esta última es un procedimiento de seguridad que se basa en las características biológicas exclusivas de una persona para comprobar que es quien dice ser). La identificación biométrica remota consiste en determinar la identidad de varias personas con la ayuda de identificadores biométricos (huellas dactilares, imágenes faciales, iris, patrones vasculares, etc.) a distancia, en un espacio público y de manera continuada o sostenida contrastándolos con datos almacenados en una base de datos.

- supervisión humana;
- requisitos específicos en el caso de determinadas aplicaciones de IA, como las empleadas para la identificación biométrica remota.

Con objeto de garantizar la seguridad jurídica, estos requisitos se detallarán para ofrecer una referencia clara a todas las partes que deban respetarlos.

a) Datos de entrenamiento

Es más importante que nunca promover, reforzar y defender los valores y normas de la UE, en especial los derechos que concede a los ciudadanos el Derecho de la UE. Sin duda, estos esfuerzos pueden extrapolarse a las aplicaciones de IA en venta y empleadas en la UE, y que se analizan en el presente documento.

Como se ha señalado anteriormente, sin datos, no hay inteligencia artificial. El funcionamiento de muchos sistemas de IA y las acciones y decisiones a las que pueden llevar dependen en gran medida del conjunto de datos que se haya utilizado para entrenar los sistemas. Por consiguiente, deben adoptarse las medidas necesarias para garantizar que, en lo que se refiere a los datos utilizados para entrenar los sistemas de IA, se respeten los valores y normas de la UE, concretamente con relación a la seguridad y la legislación vigente para la protección de los derechos fundamentales. Es posible prever los requisitos siguientes con relación a los conjuntos de datos que se empleen para entrenar los sistemas de IA:

- Requisitos destinados a ofrecer garantías razonables de que el uso posterior de los productos o servicios mediante IA es seguro, en la medida en que cumple los estándares previstos en la normativa de la UE aplicable en materia de seguridad (tanto la vigente como la que puede completarla). Por ejemplo, requisitos que garanticen que los sistemas de IA se entrenan con conjuntos de datos suficientemente amplios y que engloban todos los escenarios pertinentes para evitar situaciones peligrosas.

- Requisitos destinados a adoptar medidas razonables para velar por que dicho uso posterior de los sistemas de IA no genere resultados que conlleven una discriminación ilícita. Estos requisitos pueden suponer, en particular, la obligación de utilizar conjuntos de datos que sean suficientemente representativos, especialmente para garantizar que todas las dimensiones de género, etnicidad y otras posibles razones de discriminación ilícita queden correctamente reflejadas en estos conjuntos de datos.

- Requisitos destinados a garantizar que la privacidad y los datos personales estén adecuadamente protegidos mientras se usen los productos y servicios basados en IA. En cuanto a las cuestiones que correspondan a los ámbitos de aplicación del Reglamento General de Protección de Datos y de la Directiva sobre protección de datos en el ámbito penal respectivamente, son estos instrumentos los que las regulan.

b) Conservación de registros y datos

Teniendo en cuenta algunos elementos como la complejidad y la opacidad de muchos sistemas de IA y las dificultades que pueden surgir al respecto para verificar de manera efectiva el cumplimiento de las normas aplicables y ejecutarlas, se necesitan requisitos con relación a la conservación de registros sobre la programación de algoritmos, los datos empleados para entrenar sistemas de IA de elevado riesgo y, en algunos casos, la conservación de los datos en sí mismos. Básicamente, estos requisitos facilitan el seguimiento y la comprobación de las acciones o decisiones de los sistemas de IA potencialmente problemáticas. Con ello, no solo se facilita la supervisión y la ejecución, sino que además aumentan los

incentivos para que los agentes económicos afectados tengan en cuenta desde el principio la necesidad de respetar estas normas.

Para ello, el marco regulador puede exigir la conservación de lo siguiente:

- registros exactos sobre el conjunto de datos utilizado para entrenar y probar los sistemas de IA, especialmente una descripción de sus principales características y el modo en que se escogió el conjunto de datos;

- en determinados casos justificados, los propios conjuntos de datos;

- documentación sobre las metodologías de programación[53] y entrenamiento, los procesos y las técnicas utilizados para construir, probar y validar los sistemas de IA; especialmente con el fin de proteger la seguridad y de evitar sesgos que puedan dar lugar a un quebrantamiento de la prohibición de discriminación, cuando sea necesario.

Los registros, la documentación y, cuando proceda, los conjuntos de datos, deben conservarse durante un período de tiempo limitado y razonable para garantizar la aplicación efectiva de la legislación pertinente. Deben adoptarse medidas para garantizar que todos ellos se faciliten previa solicitud, especialmente para los ensayos o las inspecciones efectuadas por las autoridades competentes. Cuando sea necesario, deben adoptarse medidas para proteger la información confidencial, como los secretos comerciales.

c) Suministro de información

La transparencia también se requiere más allá de los requisitos de conservación de registros enumerados en el apartado C. A fin de alcanzar los objetivos perseguidos, en particular la promoción del uso responsable de la IA, la creación de confianza y las garantías de reparación cuando proceda, resulta importante que se facilite información adecuada de manera proactiva en torno a cómo usar los sistemas de IA de elevado riesgo.

En este sentido, cabe valorar los siguientes requisitos:

- Facilitar información clara con respecto de las capacidades y limitaciones del sistema de IA, en especial sobre el objetivo al que se destinan los sistemas, las condiciones en las que se espera que funcione según lo previsto y el nivel de exactitud esperado en la consecución del objetivo mencionado. Esta información es especialmente importante en el caso de los implementadores de los sistemas, pero también puede ser pertinente para las autoridades competentes y las partes afectadas.

- Independientemente, debe informarse claramente a los ciudadanos de cuándo están interactuando con un sistema de IA y no con un ser humano. Si bien la legislación de protección de datos de la UE ya recoge algunas normas de este tipo[54], es posible que se necesiten requisitos adicionales para alcanzar los objetivos anteriormente mencionados. En tal caso, deben evitarse las cargas innecesarias. Así, no es necesario facilitar dicha información, por ejemplo, en situaciones en las que sea inmediatamente evidente para los ciudadanos que están interactuando

[53] Por ejemplo, información sobre el algoritmo, especialmente sobre qué debe mejorar el modelo, qué importancia se asigna a ciertos parámetros desde el principio, etc.

[54] En concreto, de acuerdo con el artículo 13, apartado 2, letra f) del RGPD, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales,

la información necesaria sobre la existencia de decisiones automatizadas y determinada información adicional, a fin de garantizar un tratamiento de datos leal y transparente.

con un sistema de IA. Es importante también que la información facilitada sea objetiva, concisa y fácilmente comprensible. La manera en que ha de presentarse la información debe adaptarse al contexto específico.

d) Solidez y exactitud

Los sistemas de IA (y desde luego las aplicaciones de IA de riesgo elevado) deben ser técnicamente sólidos y exactos para ser fiables. Esto supone que estos sistemas deben desarrollarse de manera responsable y tras una valoración previa adecuada de los riesgos que conllevan. Su desarrollo y funcionamiento han de ser de tal manera que garanticen que los sistemas de IA se comporten con la fiabilidad prevista. Deben adoptarse todas las medidas razonables para reducir al mínimo el riesgo de que se produzcan daños.

En este sentido, cabe valorar los siguientes elementos:

- Requisitos que garanticen que los sistemas de IA son sólidos y exactos, o al menos que reflejan correctamente su nivel de exactitud, a lo largo de todas las fases de su ciclo de vida.

- Requisitos que garanticen la reproducibilidad de los resultados.

- Requisitos que garanticen que los sistemas de IA son capaces de lidiar correctamente con los errores o las incoherencias a lo largo de todas las fases de su ciclo de vida.

- Requisitos que garanticen que los sistemas de IA son resilientes ante los ataques abiertos y los intentos más sutiles de manipulación de los propios datos o algoritmos, y que, llegado el caso, aseguren que se toman medidas para combatirlos.

e) Supervisión humana

La supervisión humana ayuda a garantizar que un sistema de IA no socave la autonomía humana o provoque otros efectos adversos. El objetivo de una IA fiable, ética y antropocéntrica solo puede alcanzarse garantizando una participación adecuada de las personas con relación a las aplicaciones de IA de riesgo elevado.

A pesar de que todas las aplicaciones de IA que se tienen en cuenta en el presente Libro Blanco de cara a un régimen jurídico específico se consideran de riesgo elevado, el tipo y nivel adecuado de supervisión humana puede variar de un caso a otro. Dependerá en particular del uso previsto de los sistemas y de los efectos que el uso pueda tener en el caso de las personas físicas o jurídicas afectadas. Ello se entenderá sin perjuicio de los derechos legales previstos en el RGPD cuando el sistema de IA trate datos personales. La supervisión humana puede traducirse en las consecuencias siguientes, entre otras:

- El resultado del sistema de IA no es efectivo hasta que un humano no lo haya revisado y validado (por ejemplo, la decisión de denegar una solicitud de prestaciones de seguridad social solo podrá adoptarla un ser humano).

- El resultado del sistema de IA es inmediatamente efectivo, pero se garantiza la intervención humana posterior (por ejemplo, la decisión de denegar una solicitud de tarjeta de crédito puede tramitarse a través de un sistema de IA, pero debe posibilitarse un examen humano posterior).

- Se realiza un seguimiento del sistema de IA mientras funciona y es posible intervenir en tiempo real y desactivarlo (por ejemplo, un vehículo sin conductor cuenta con un procedimiento o botón

de apagado para las situaciones en las que un humano determine que el funcionamiento del vehículo no es seguro).

- En la fase de diseño, se imponen restricciones operativas al sistema de IA (por ejemplo, un vehículo sin conductor dejará de funcionar en determinadas condiciones de visibilidad reducida en las que los sensores sean menos fiables, o mantendrá una cierta distancia con el vehículo que lo preceda en una situación dada).

f) Requisitos específicos en el caso de la identificación biométrica remota

La recopilación y el uso datos biométricos[55] para la identificación remota[56], por ejemplo mediante la instalación de sistemas de reconocimiento facial en lugares públicos, entraña riesgos específicos para los derechos fundamentales[57]. Las repercusiones de la utilización de sistemas de IA de identificación biométrica remota en los derechos fundamentales pueden variar considerablemente en función del objetivo, el contexto y el alcance de dicho uso.

Las normas de protección de datos de la UE ya prohíben, en principio, el tratamiento de datos biométricos dirigido a identificar de manera unívoca a una persona física, excepto en condiciones específicas[58]. En concreto, con arreglo al RGPD, este tratamiento solo puede tener lugar en un número limitado de situaciones, principalmente por motivos de interés público significativo. En este caso, el tratamiento debe tener lugar sobre la base del Derecho nacional o de la UE, estar sujeto al requisito de proporcionalidad, al respeto del derecho a la protección de los datos y a garantías adecuadas. Con arreglo a la Directiva sobre protección de datos en el ámbito penal, para efectuar dicho tratamiento debe existir una necesidad estricta al respecto; en principio, una autorización de la legislación nacional o de la UE y garantías adecuadas. Puesto que todo tratamiento de datos biométricos dirigido a identificar a una persona física de manera unívoca estaría vinculado con una excepción a una prohibición establecida en la legislación de la UE, dicho tratamiento ha de atenerse a la Carta de Derechos Fundamentales de la UE.

Por consiguiente, de conformidad con las normas vigentes en materia de protección de datos y con la Carta de Derechos Fundamentales de la UE, la IA solo puede utilizarse con fines de identificación biométrica remota cuando dicho uso esté debidamente justificado, sea proporcionado y esté sujeto a garantías adecuadas.

---

[55] Por «datos biométricos» se entienden los «datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos [huella dactilar]» [artículo 3, apartado 13 de la Directiva sobre protección de datos en el ámbito penal; artículo 4, apartado 14, del RGPD; artículo 3, apartado 18, del Reglamento (UE) 2018/1725].

[56] En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos.

[57] Por ejemplo, la dignidad de las personas. Con relación a este aspecto, los derechos al respeto de la vida privada y a la protección de los datos personales son parte primordial de la preocupación en torno a los derechos fundamentales cuando se utiliza la tecnología de reconocimiento facial. Tiene, además, un efecto fundamental en el derecho a la no discriminación y los derechos de grupos específicos, como los niños, las personas mayores o las personas con discapacidad. Además, no deben socavarse los derechos de expresión, asociación y reunión mediante el uso de esta tecnología. Véase: «La tecnología del reconocimiento facial: consideraciones relativas a los derechos fundamentales en el marco de la aplicación de las leyes» (en inglés)
https://fra.europa.eu/en/publication/2019/facial-recognition.

[58] Artículo 9 del RGPD y artículo 10 de la Directiva sobre protección de datos en el ámbito penal. Véase también el artículo 10 del Reglamento (UE) 2018/1725 (aplicable a las instituciones y organismos de la UE).

A fin de abordar las posibles preocupaciones sociales con relación al uso de la IA para tales fines en lugares públicos, y con el objetivo de evitar la fragmentación del mercado interior, la Comisión abrirá un debate europeo sobre las circunstancias específicas, si las hubiera, que puedan justificar dicho uso, así como sobre las garantías comunes.

E. DESTINATARIOS

En lo que se refiere a los destinatarios de los requisitos legales que resulten de aplicación en el caso de las aplicaciones de IA de elevado riesgo contempladas anteriormente, existen dos cuestiones fundamentales que deben tenerse en cuenta.

En primer lugar, se plantea la cuestión de cómo repartir las obligaciones entre los agentes económicos que participen en el proceso. Hay numerosas partes involucradas en el ciclo de vida de un sistema de IA. Entre ellas, el desarrollador, el implementador (la persona que utiliza un producto o servicio provisto de IA) y otras partes potenciales (productor, distribuidor o importador, proveedor de servicios, usuario profesional o particular).

La Comisión considera que, en un futuro marco regulador, cada obligación debe dirigirse a la(s) persona(s) que esté(n) en mejor posición para abordar todo posible riesgo. Por ejemplo, mientras que los desarrolladores de IA pueden ser los que estén en mejor posición para abordar los riesgos derivados de la fase de desarrollo, su capacidad de controlar los riesgos durante la fase de uso puede ser más limitada. En este caso, el implementador debe ser objeto de la obligación correspondiente. Ello debe entenderse sin perjuicio de determinar qué parte debe ser responsable de los daños causados, a efectos de la responsabilidad civil ante los usuarios finales u otras partes que sufran daños, y de ofrecer un acceso efectivo a la justicia. Con arreglo a la legislación de la UE sobre responsabilidad con relación a los productos, la responsabilidad civil por los productos defectuosos se atribuye al productor, sin perjuicio de la legislación nacional, que también puede contemplar una indemnización a cargo de otras partes.

En segundo lugar, se plantea la cuestión del alcance geográfico de la intervención legislativa. Según la Comisión, es esencial que todos los agentes económicos que ofrezcan productos o servicios provistos de IA en la UE, independientemente de que estén o no establecidos en la Unión, estén sujetos a los requisitos. De lo contrario, los objetivos de la intervención legislativa, a los que se hacía referencia anteriormente, no podrán alcanzarse plenamente.

F. CUMPLIMIENTO Y EJECUCIÓN

A fin de garantizar que la IA sea fiable y segura y que respete los valores y normas europeos, deben cumplirse en la práctica los requisitos jurídicos aplicables, y las autoridades nacionales y europeas competentes, así como las partes interesadas, deben garantizar su cumplimiento eficazmente. Las autoridades competentes deben ser capaces de investigar los casos particulares y de evaluar su impacto en la sociedad.

En vista del alto riesgo que suponen determinadas aplicaciones de IA para los ciudadanos y nuestra sociedad (véase el apartado A), la Comisión considera en esta fase que sería necesario un control objetivo previo de la conformidad para verificar y garantizar el cumplimiento de algunos de los requisitos obligatorios previamente mencionados por parte de las aplicaciones de elevado riesgo (véase el apartado D). El control previo de la conformidad puede incluir procedimientos de ensayo, inspección

o certificación[59]. Puede contar también con controles de los algoritmos y de los conjuntos de datos utilizados en la fase de desarrollo.

Los controles de la conformidad de las aplicaciones de IA de elevado riesgo deben ser parte de los mecanismos de evaluación de la conformidad que ya existen en el caso de un gran número de productos comercializados en el mercado interior de la UE. Cuando ninguno de estos mecanismos existentes sea fiable, puede que sea necesario establecer mecanismos similares, a partir de las mejores prácticas y de la posible aportación de las partes interesadas y de las organizaciones europeas de normalización. Todo nuevo mecanismo debe ser proporcionado y no discriminatorio y utilizar criterios transparentes y objetivos que cumplan con las obligaciones internacionales.

Al diseñar e implantar un sistema que dependa de una evaluación de conformidad previa, debe prestarse especial atención a lo siguiente:

- Puede que no todos los requisitos enumerados anteriormente se adecúen a una evaluación de conformidad previa. Por ejemplo, el requisito relativo a la información que debe facilitarse no suele prestarse a una verificación compatible con este tipo de evaluación.

- Debe tenerse especialmente en cuenta la posibilidad de que determinados sistemas de IA evolucionen y aprendan de la experiencia, lo que puede requerir evaluaciones reiteradas a lo largo del ciclo de vida de dichos sistemas.

- La necesidad de verificar los datos utilizados en el entrenamiento, así como las técnicas, procesos y metodologías de programación y entrenamiento empleados para construir, probar y validar los sistemas de IA.

- Cuando una evaluación de la conformidad muestre que un sistema de IA no cumple los requisitos, por ejemplo, los relativos a los datos empleados para entrenarlo, los fallos detectados tendrán que ser corregidos mediante, por ejemplo, un nuevo entrenamiento del sistema en la UE de tal manera que se garantice el cumplimiento de todos los requisitos aplicables.

Las evaluaciones de conformidad deben ser de obligado cumplimiento para todos los agentes económicos sujetos a los requisitos, independientemente del lugar en que estén establecidos[60]. A fin de limitar la carga para las pymes, puede preverse alguna estructura de apoyo, especialmente mediante los centros de innovación digital. Además, es posible contar con medidas y herramientas especializadas en línea para facilitar el cumplimiento.

Toda evaluación previa de la conformidad debe realizarse sin perjuicio de la supervisión del cumplimiento y de la posterior ejecución por parte de las autoridades nacionales competentes. Este es el caso de las aplicaciones de IA de riesgo elevado, pero también de otras aplicaciones de IA sujetas a requisitos legales, aunque el elevado riesgo de las aplicaciones en cuestión pueda justificar que las autoridades nacionales competentes presten especial atención a las primeras. Los controles *ex post* deben facilitarse mediante una adecuada documentación de la aplicación de IA pertinente (véase el apartado E) y, cuando proceda, ofreciendo la posibilidad de que terceros (como las autoridades competentes) prueben dichas aplicaciones. Ello puede resultar especialmente importante cuando surjan riesgos para

[59] El sistema debe basarse en los procedimientos de evaluación de la conformidad de la UE —véase la Decisión n.º 768/2008/CE o el Reglamento (UE) 2019/881 (Reglamento sobre ciberseguridad)—, teniendo en cuenta las especificidades de la IA. Véase la «Guía azul» sobre la aplicación de la normativa europea relativa a los productos, de 2014.

[60] En lo que se refiere a la estructura de gobernanza pertinente, como los organismos designados para llevar a cabo las evaluaciones de conformidad, véase el apartado H.

los derechos fundamentales que dependan del contexto. Este control del cumplimiento debe ser parte de un sistema de vigilancia constante del mercado. Los aspectos relativos a la gobernanza se tratan más detalladamente en el apartado H.

Además, en el caso de las aplicaciones de IA de riesgo elevado y de otras aplicaciones de IA, debe garantizarse una acción judicial efectiva para las partes que hayan sufrido repercusiones negativas derivadas de los sistemas de IA. Las cuestiones relativas a la responsabilidad civil se tratan más detalladamente en el informe sobre el marco de seguridad y responsabilidad civil, adjunto al presente Libro Blanco.

G. SISTEMA DE ETIQUETADO VOLUNTARIO PARA LAS APLICACIONES QUE NO SE CONSIDERAN DE RIESGO ELEVADO

En el caso de las aplicaciones de IA que no se consideren de riesgo elevado (véase el apartado C) y que, por tanto, no estén sujetas a los requisitos obligatorios esbozados (véanse los apartados D, E y F), existe la opción de establecer un sistema de etiquetado voluntario, además de la legislación aplicable.

Con este sistema, los agentes económicos interesados que no estén sujetos a los requisitos obligatorios pueden optar por someterse, con carácter voluntario, bien a dichos requisitos, bien a un conjunto de requisitos similares, creados de manera específica a los efectos del sistema voluntario. Los agentes económicos interesados obtendrán entonces una etiqueta de calidad para sus aplicaciones de IA.

La etiqueta voluntaria permitirá a los agentes económicos interesados mostrar que los productos y servicios provistos de IA que ofrecen son fiables. Además, permitirá a los usuarios distinguir fácilmente si los productos y servicios en cuestión respetan ciertos referentes objetivos y normalizados a escala de la UE, que van más allá de las obligaciones legales aplicables normalmente. Ello contribuirá a incrementar la confianza de los usuarios en los sistemas de IA y fomentará una adopción generalizada de esta tecnología.

Esta opción conlleva la creación de un nuevo instrumento jurídico para establecer un marco de etiquetado voluntario para los desarrolladores y/ o implementadores de los sistemas de IA que no se consideren de alto riesgo. Si bien la participación en el sistema de etiquetado debe ser voluntaria, una vez que el desarrollador o implementador opte por usar la etiqueta, todos los requisitos serán vinculantes. La combinación de estas imposiciones *ex ante* y *ex post* debe garantizar que se cumplan todos los requisitos.

H. GOBERNANZA

Se requiere una estructura de gobernanza europea sobre IA en forma de un marco para la cooperación de las autoridades nacionales competentes, a fin de evitar la fragmentación de responsabilidades, incrementar las capacidades de los Estados miembros y garantizar que Europa se provea a sí misma de la capacidad necesaria para probar y certificar los productos y servicios provistos de IA. En este contexto, conviene respaldar a las autoridades nacionales competentes para que puedan cumplir su mandato cuando se utilice la IA.

La estructura de gobernanza europea puede desempeñar diversas funciones, como la de foro para el intercambio periódico de información y mejores prácticas, la detección de tendencias emergentes y el asesoramiento sobre la actividad de normalización y sobre la certificación. Además, debe desempeñar un papel clave a la hora de facilitar la ejecución del marco jurídico, por ejemplo, mediante la formulación de orientaciones, emitiendo dictámenes y compartiendo sus conocimientos técnicos. Para ello, debe apoyarse en una red de autoridades nacionales, así como en redes sectoriales y autoridades reguladoras,

tanto a escala nacional como de la UE. Además, un comité de expertos puede prestar asistencia a la Comisión.

La estructura de gobernanza debe garantizar la mayor participación de partes interesadas posible. Debe consultarse a las partes interesadas (organizaciones de consumidores e interlocutores sociales, empresas, investigadores y organizaciones de la sociedad civil) sobre la aplicación y futuro desarrollo del marco.

Dadas las estructuras vigentes en ámbitos como el financiero, el farmacéutico, el de la aviación, el de los productos sanitarios, el de la protección de los consumidores o el de la protección de datos, la estructura de gobernanza propuesta no debe duplicar funciones existentes. Por el contrario, debe establecer vínculos estrechos con otras autoridades competentes nacionales y de la UE en los distintos sectores, a fin de completar los conocimientos técnicos y de ayudar a las autoridades actuales a controlar y supervisar las actividades de los agentes económicos en lo que respecta a los sistemas de IA y los productos y servicios provistos de IA.

Finalmente, si se opta por esto, el desarrollo de las evaluaciones de conformidad podrá encomendarse a organismos notificados designados por los Estados miembros. Los centros de ensayo deben facilitar la auditoría y evaluación independientes de los sistemas de IA, de acuerdo con los requisitos expuestos anteriormente. Las evaluaciones independientes incrementarán la confianza y garantizarán la objetividad. También pueden facilitar el trabajo de las autoridades competentes.

La UE dispone de excelentes centros de ensayo y evaluación y debe desarrollar sus capacidades también en el ámbito de la IA. Los agentes económicos establecidos en terceros países que deseen acceder al mercado interior pueden recurrir tanto a los organismos designados establecidos en la UE como a organismos de terceros países designados para llevar a cabo dicha evaluación, previo acuerdo de reconocimiento mutuo con terceros países.

La estructura de gobernanza relativa a la IA y las posibles evaluaciones de la conformidad que se tratan en el presente documento deben mantener inalteradas las competencias y responsabilidades derivadas del Derecho vigente de la UE en lo que se refiere a las autoridades competentes en sectores o cuestiones específicos (financiero, farmacéutico, aviación, productos sanitarios, protección de los consumidores, protección de datos, etc.).

6. CONCLUSIÓN

La inteligencia artificial es una tecnología estratégica que ofrece numerosas ventajas a los ciudadanos, las empresas y la sociedad en su conjunto, siempre y cuando sea antropocéntrica, ética y sostenible y respete los derechos y valores fundamentales. La IA aporta importantes mejoras de la eficiencia y la productividad que pueden reforzar la competitividad de la industria europea y mejorar el bienestar de los ciudadanos. También puede contribuir a encontrar soluciones a algunos de los problemas sociales más acuciantes, como la lucha contra el cambio climático y la degradación medioambiental, los retos relacionados con la sostenibilidad y los cambios demográficos, la protección de nuestras democracias y, cuando sea necesario y proporcionado, la lucha contra la delincuencia.

Para que Europa aproveche plenamente las oportunidades que ofrece la IA, debe desarrollar y reforzar las capacidades industriales y tecnológicas necesarias. Tal como se establece en la Estrategia Europea de Datos adjunta, ello también requiere de medidas que permitan a la UE convertirse en un centro de datos mundial.

El enfoque europeo sobre la IA aspira a promover la capacidad de innovación de Europa en el sector de la IA, e incentiva el desarrollo y la adopción de una IA ética y fiable en toda la economía de la UE. La IA debe estar al servicio de las personas y ser una fuerza positiva para la sociedad.

Con el presente Libro Blanco y el informe sobre el marco de seguridad y responsabilidad civil adjunto, la Comisión pone en marcha una amplia consulta de la sociedad civil, la industria y el mundo académico de los Estados, para que ofrezcan propuestas concretas en torno a un enfoque europeo sobre la IA.

La Comisión invita a que se envíen observaciones sobre las propuestas recogidas en el Libro Blanco mediante una consulta pública abierta disponible en https://ec.europa.eu/info/consultations_es. La consulta será accesible hasta el 19 de mayo de 2020.

Es práctica habitual de la Comisión publicar los comentarios recibidos en respuesta a una consulta pública. Sin embargo, se puede solicitar que los comentarios o ciertas partes de los mismos sean confidenciales. De ser así, indique claramente en la portada de su documento que no deben hacerse públicos y remita también una versión no confidencial a la Comisión para su publicación.

Ambos prevén medios estratégicos para incentivar las inversiones en investigación e innovación, reforzar el desarrollo de habilidades y respaldar la adopción de la IA por parte de las pymes, y ofrecen propuestas en relación con los elementos clave para un futuro marco regulador. Esta consulta permitirá desarrollar un diálogo amplio con todas las partes interesadas que servirá de base a los siguientes pasos que dé la Comisión.