NOTAS de la COMISION DE TRANSFORMACION DIGITAL DEL ILUSTRE COLEGIO DE LA ABOGACÍÁ DE BARCELONA (ICAB) AL LIBRO BLANCO SOBRE LA INTELIGENCIA ARTIFICIAL - UN ENFOQUE EUROPEO ORIENTADO A LA EXCELENCIA Y LA CONFIANZA DE LA COMISIÓN EUROPEA- Bruselas, 19.2.2020 COM(2020)

NOTA PRELIMINAR

De conformidad con lo que se contempla en el documento, se comparte la necesidad de posicionar a la Unión Europea en relación al desarrollo de la Inteligencia Artificial.

En especial, cuando ese liderazgo se plantea desde el respeto a los derechos humanos de las personas.

En ese escenario, es evidente que el marco regulador de los sistemas basados en Inteligencia Artificial no puede suponer un impedimento, ni puede entorpecer el desarrollo de los proyectos o la industria de la IA. En ningún caso, dicho régimen jurídico debe suponer un hándicap o una dificultad que suponga una desventaja competitiva y coloque a la UE en situación de pérdida de competitividad respecto de otras zonas o territorios.

Ello no debe obstar a la aspiración de alcanzar un marco regulador integral (y no exclusivamente limitado a los sistemas basados en IA que presenten mayores niveles de riesgo respecto de los derechos de las personas).

En este sentido, se propone que el marco regulador contemple los diferentes niveles de riesgo y ajuste las garantías exigidas por el marco regulador a los diferentes niveles de riesgo, exigiendo de menores a mayores garantías para los sistemas basados en IA en función del nivel de riesgo que presenten.

El marco jurídico del que se dote la UE en relación a los sistemas basados en IA ha de tener la vocación y llegar a ser un standard universal, al igual que en el ámbito de protección de datos lo es el RGPD.

Establecida esta nota preliminar de carácter general, procedemos a realizar comentarios y sugerencias de mejora, concretos, al texto.

1.- NOTA 1. AMBITO DE APLICACION DEL MARCO REGULADOR DE LA UE

El documento analizado establece, con respecto al ámbito de aplicación de un futuro marco regulador de la UE las siguientes conclusiones:

"C. ÁMBITO DE APLICACIÓN DE UN FUTURO MARCO REGULADOR DE LA UE pag 20 y ss

… Pag 21:

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. 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. 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 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. 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 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."*

COMENTARIO AL TEXTO

De dicho texto se deduce que el marco regulador solo ha de aplicarse a las situaciones consideradas de riesgo elevado.

Como hemos indicado en nuestra nota preliminar, somos partidarios de que el marco regulador debe ser aplicable a todos los sistemas IA, si bien estableciendo niveles de exigencia y garantías, según el concreto nivel de riesgo que presente el sistema de IA respecto de los derechos de las personas.

Los niveles de riesgo deberían ser, por ejemplo, en tres niveles:

- Un primer nivel, de riesgo inapreciable o tolerable, si el sistema basado en IA no implica violación de derechos.
- Un segundo nivel, si el sistema basado en IA puede implicar la violación de derechos no fundamentales o esenciales, y
- Un tercer nivel, intolerable, si el sistema basado en IA puede llevar a la vulneración de derechos fundamentales o esenciales

El marco legal regulador debería contemplar y exigir mayores requisitos y garantías en función de dicha clasificación, exigiendo mayores garantías a mayor nivel de riesgo.

NOTA 2.- TIPOS DE REQUISITOS LEGALES OBLIGATORIOS

El documento analizado establece en el apartado D los tipos de requisitos legales obligatorios a los que deben atender las partes pertinentes, y que deben concretarse en normas jurídicas comunitarias que conformen el marco común regulador de la IA en la UE:

"D. TIPOS DE REQUISITOS pág. 22 y ss.

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;*
- *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."

COMENTARIO AL TEXTO

El documento analizado establece en el apartado D los tipos de requisitos legales obligatorios a los que deben atender las partes pertinentes, y que deben concretarse en normas jurídicas comunitarias que conformen el marco común regulador de la IA en la UE, si bien dicho marco regulador se predica únicamente respecto a las aplicaciones de la IA que entrañen un riesgo elevado exclusivamente.

Como hemos comentado más arriba, el marco regulador debería ser aplicable íntegramente a todos los sistemas basados en IA, si bien estableciendo un escalado de requisitos y garantías según los diferentes niveles de riesgo que proponemos en la nota 1 precedente, de forma que los sistemas que presenten mayores niveles de riesgo estén sujetos a mayores requisitos y garantías que los que presente un riesgo menor.

En este sentido:

- los requisitos sobre la calidad de los datos y la transparencia u obligación de información deberían exigirse a todos los sistemas basados en IA, si bien en el caso de las situaciones en las que su aplicación no pueda comportar violaciones de derechos, podría aceptarse la exención de no información expresa, cuando dicha aplicación a través de sistema de IA sea evidente.

- los requisitos anteriores, más la solidez del sistema, y la supervisión humana y la posible responsabilidad objetiva se habrían de predicar de los sistemas que pueden implicar violaciones de derechos no fundamentales o esenciales de las personas.

- los requisitos anteriores más el registro obligatorio del sistema basado en IA ante el competente organismo público, se deberían aplicar a las aplicaciones que pueden llevar a cabo vulneraciones de derechos fundamentales o esenciales de las personas (aplicaciones en el ámbito de servicios sociales, policía, justicia).

Especialmente, la obligación de información ha de ser más completa en función de la complejidad del sistema basado en IA y de la afectación a los derechos de las personas que puede provocar.

Es necesario un importante debate político y social sobre los límites de la IA y muy especialmente sobre la identificación biométrica remota, sin que sea en estos momentos descartable la restricción de su uso a las fuerzas responsables de la seguridad nacional, en los casos legalmente previstos y bajo supervisión de la autoridad judicial.

NOTA 3.- SUMINISTRO DE INFORMACION

El documento analizado establece el requisito legal de ofrecer suministro de información respecto de las aplicaciones que hagan uso de sistemas de IA que entrañen un riesgo elevado, con la finalidad de generar confianza y garantías de reparación.

Pese a ello, respecto del requisito legal de informar claramente a los ciudadanos de cuando están interactuando con un sistema de IA, establece la posible exención en situaciones en las que ello sea evidente con la finalidad de evitar cargas innecesarias.

c) Suministro de información pág. 24

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, 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 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.*

COMENTARIO AL TEXTO

El documento analizado establece, el requisito legal de ofrecer suministro de información respecto de las aplicaciones que hagan uso de sistemas de IA que entrañen un riesgo elevado, con la finalidad de generar confianza y garantías de reparación.

Pese a ello, respecto del requisito legal de informar claramente a los ciudadanos de cuando están interactuando con un sistema de IA, establece la posible exención en situaciones en las que ello sea evidente con la finalidad de evitar cargas innecesarias.

Por el contrario, la presente propuesta considera que la obligación de prestar información ha de existir siempre, con la finalidad precisamente de ofrecer confianza a la ciudadanía. En este sentido, se ha de tener en cuenta la necesidad de proteger los derechos a información de personas y colectivos especialmente vulnerables (en situación de discapacidad, menores de edad, o personas de edad avanzada).

Subsidiariamente, solo en aquellas aplicaciones que no representen riesgos que puedan suponer violación de derechos se podría plantear una exención de información, siempre y cuando sea muy evidente que dicha aplicación utiliza sistemas de IA.

En las restantes categorías de sistemas basados en IA que hemos indicado en la nota 1 de este documento, es decir, todas aquellas que puedan implicar una vulneración de derechos y especialmente, de derechos esenciales, dicha obligación de transparencia ha de concretarse en la necesidad de ofrecer información expresa, clara, comprensible y detallada.

Debería contemplarse un doble sistema de información:

- uno visible en el propio “producto” o “servicio”, que pude estar basado en un sistema de iconos.
- otro accesible digitalmente en abierto y gratuito en un registro europeo único, que contemple información suficiente respecto del espacio territorial al que se extiende el sistema, duración, especificaciones, creador, titular, cesionario o explotadores sucesivos. Dicho sistema de registro debería contemplar todos los datos relevantes relacionados con el sistema basado en IA , ofreciendo una imagen fiel del mismo, sus potencialidades y uso efectivo, debiendo ser un requisito para que se pueda operar en la UE, aun cuando su creación o explotación proceda de fuera de la UE.

La publicidad y transparencia ha de permitir la verificación por terceros.

NOTA 4.- SUPERVISION HUMANA

El documento analizado establece, el requisito legal de supervisión humana respecto de las aplicaciones de IA de riesgo elevado.

e) Supervisión humana, pag 25

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).*

COMENTARIO AL TEXTO

El documento analizado establece, el requisito legal de supervisión humana respecto de las aplicaciones de IA de riesgo elevado. Y establece, como consecuencia de dicha necesidad de supervisión humana, determinados sistemas, básicamente:

- No efectividad del sistema IA hasta la intervención humana.
- Efectividad del sistema IA, pero posibilidad de revisión humana.
- Posibilidad de desactivación del sistema IA en tiempo real.
- Establecimiento de restricciones operativas a la IA desde el diseño.

En relación a la supervisión humana se ha de diferenciar al explotador del sistema basado en IA en el que la persona humana ha de tener la última palabra, de la que hace el usuario.

El sistema según el cual se establezca un régimen jurídico aplicable a cualquier sistema basado en IA con independencia de su riesgo, y de que los requisitos y garantías de los diferentes sistemas que se establezcan se incrementen según el concreto riesgo que presente el sistema, según se propone en este documento, permite establecer la posibilidad de que el sistema IA opere y sea efectivo por sí solo, si bien sujeto a revisión posterior, siempre que ello sea aplicable y se predique exclusivamente de aquellos sistemas de IA cuya aplicación no provoquen ni puedan provocar vulneración de derechos.

El requisito de que el sistema basado en IA no sea efectivo hasta la intervención humana debería predicarse de aquellos sistemas que pueden suponer un riesgo para los derechos de las personas.

La desactivación del sistema IA en tiempo real y el establecimiento de restricciones operativas desde el diseño deberían aplicarse cuando el sistema basado en IA pueda representar un riesgo para los derechos fundamentales de las personas.

En este sentido, se ha de delimitar el traspaso de responsabilidad en el proceso, si el sistema puede ser desconectado por la intervención humana.

NOTA 5.- DESTINATARIOS

El documento analizado apunta bajo el epígrafe de DESTINATARIOS, la cuestión de los obligados por la normativa reguladora, la distribución de las responsabilidades de cumplimiento de dicha normativa y apunta hacia un posible sistema de responsabilidad.

E. DESTINATARIOS pág. 27

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.

COMENTARIO AL TEXTO

El documento analizado apunta bajo el epígrafe de DESTINATARIOS, la cuestión de los obligados por la normativa reguladora, la distribución de las responsabilidades de cumplimiento de dicha normativa y apunta hacia un posible sistema de responsabilidad, que parece derivar al sistema de responsabilidad civil por productos defectuosos.

En los supuestos de sistemas basados en IA que puedan suponer riesgos para los derechos de las personas, se debería contemplar un sistema de responsabilidad teniendo en cuenta los diferentes ámbitos del Derecho. En este sentido, se debería contemplar:

- Ámbito de responsabilidad civil, cuando el funcionamiento del sistema basado en IA resulte defectuoso, sin intervención de dolo o imprudencia grave, con el estudio de la posibilidad de establecer como garantía la existencia de aseguramiento obligatorio, que garantice el resarcimiento de los posibles daños provocados.

En este sentido se ha de valorar la posibilidad de establecer responsabilidades civiles solidarias de todos los explotadores del sistema, del establecimiento de un sistema de responsabilidad objetiva.

- Ámbito de responsabilidades penales, cuando intervenga dolo o la imprudencia grave en cualquier fase del ciclo de vida del sistema basado en IA (diseño, implementación, mejoras y versiones ulteriores, revisiones posteriores) y se produzcan violaciones de derechos, especialmente si éstos son derechos fundamentales de las personas.

- Responsabilidades administrativas, ante el incumplimiento de los requisitos legales de carácter formal (falta de inscripción en registros previos obligatorios en caso de sistemas utilizados que puedan provocar violaciones de derechos esenciales, o falta de contratación del aseguramiento de la responsabilidad civil obligatoria, falta de información al afectado por el proceso de toma de decisión basado en IA, por ejemplo).

  En los supuestos de incumplimientos muy graves se habría de prever la posibilidad de cese cautelar de la explotación del sistema, sin perjuicio del posterior control jurisdiccional.

NOTA 6.- SISTEMA DE ETIQUETADO VOLUNTARIO

El documento analizado apunta bajo el epígrafe G. SISTEMA DE ETIQUETADO VOLUNTARIO PARA LAS APLICACIONES QUE NO SE CONSIDERAN DE RIESGO ELEVADO, un sistema de etiquetado voluntario en el caso de aplicaciones de IA que no se consideren de riesgo elevado.

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.

COMENTARIO AL TEXTO

El documento analizado apunta bajo el epígrafe indicado que en los supuestos en que el sistema IA no presente riesgo elevado sea posible el establecimiento de un sistema de etiquetado voluntario.

Si consideramos que el usuario final debe estar siempre informado de la aplicación de un sistema basado en IA, con la finalidad de generar confianza en la ciudadanía, el etiquetado debiere ser obligatorio en todos los supuestos. Caso distinto sería el de la adopción de un sello o un estándar de calidad, los cuales, siguiendo nuestra tradición jurídica, sí deberían ser de voluntaria adopción.

Subsidiariamente, como se ha indicado en la nota 3 de este documento, solo en aquellas aplicaciones que no representen riesgos que puedan suponer violación de derechos se podría plantear una exención de información, siempre y cuando sea muy evidente dicha aplicación a través de sistemas de IA.

Reproducimos aquí los comentarios incluidos en la nota 3 de este documento.

NOTA 7.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El documento analizado incluye varias referencias a protección de datos de carácter personal, tales como las que se incluyen a continuación:

- *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. (Página 24)*

- *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, es posible que se necesiten requisitos adicionales para alcanzar los objetivos anteriormente mencionados. (Página 24)*

- *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. 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. (Página 27)*

- *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. (Página 27)*

- *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. (Página 31)*

COMENTARIO AL TEXTO

Cuando en los sistemas de Inteligencia Artificial (en adelante, “IA”) se utilicen datos personales será de aplicación el establecido en el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos y por el cual se deroga la Directiva 95/46/CE (en adelante, “RGPD

En primer lugar, para llevar a cabo un tratamiento de datos personales en el uso y desarrollo de los sistemas de IA, de acuerdo con el principio de licitud establecido en el artículo 5 del RGPD, es necesario que el Responsable cuente con una de las bases legales del artículo 6 del RGPD.

En el contexto de la IA se debe tener en cuenta que las bases legales más utilizadas podrían ser el consentimiento, la ejecución de un contrato o el interés legítimo.

Independientemente de cuál sea la base legitimadora que ampare el tratamiento, de acuerdo con la normativa aplicable en materia de protección de datos (arts. 12, 13 y 14 del RGPD), en cualquier caso, se tendrá que informar a los Interesados del tratamiento que se llevará a cabo respeto sus datos.

Además, en el contexto del uso de sistemas de IA, se tendrá que informar a los Interesados expresamente de lo siguiente:

- "la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y como mínimo en estos casos, se tendrá que facilitar información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de este tratamiento para el interesado" (artes. 13 y 14 RGPD).
- "el derecho a obtener intervención humana del responsable, a expresar su punto de vista y a impugnar la decisión" (arte. 22 RGPD).
- El derecho de obtener del Responsable (…) "información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de este tratamiento para el interesado (arte. 15) [incluyendo] una explicación de la decisión tomada después de esta evaluación" (considerando 71).

De conformidad con el artículo 35 del RGPD, respeto los tratamientos que impliquen "la evaluación sistemática y exhaustiva de aspectos personales de personas físicas basada en un tratamiento automatizado, como la elaboración de perfiles" es obligatorio realizar una evaluación de impacto relativa a la protección de datos ("EIPD"), en cuanto que comportan un alto riesgo por los derechos y las libertades de los Interesados.

Esta EIPD permitirá comprobar si las medidas de control adoptadas cubren y mitigan la exposición al riesgo inherente del tratamiento. Así mismo, si se considera que el riesgo residual continúa siendo alto, se tendrá que formular una consulta previa ante la autoridad de control competente antes de proceder al tratamiento, de acuerdo con el que dispone el artículo 36 del RGPD.

En cualquier tratamiento de datos personales, que se realicen en el desarrollo o uso de un sistema de IA, se tendrán que cumplir con los principios establecidos en el artículo 5.1 del RGPD, estos son: (y) licitud, lealtad y transparencia; (ii) limitación de la finalidad; (iii) minimización de datos, (iv) exactitud, (v) limitación del plazo de conservación y (vino) la integridad y confidencialidad de los datos.

Adicionalmente, el RGPD establece en su artículo 25 los principios de privacidad desde el diseño y por defecto, que comportan, entre otras cuestiones, que por un lado, el Responsable, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, tiene que implantar las medidas técnicas y organizativas adecuadas, como la seudoanonimización, para aplicar de manera efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos exigidos por la normativa aplicable en materia de protección de datos, así como para proteger los derechos de los Interesados (privacidad desde el diseño) .

En este sentido, la autoridad de control en el Reino Unido (conocida bajo las siglas, "ICO") considera que cuando se quiera utilizar sistemas de IA se tendrá que considerar el contexto en el que este operará, para poder reflexionar sobre los potenciales impactos que generará su uso.

Por otro lado, el Responsable tiene que aplicar las medidas técnicas y organizativas adecuadas con la intención de garantizar que, por defecto, únicamente se tratan los datos personales necesarios para cada una de las finalidades específicas del tratamiento, es decir, tanto en cuanto a la cantidad de los datos personales recogidos, al alcance del tratamiento, al plazo de conservación y a la accesibilidad de los datos. Estas medidas tienen que garantizar en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas (privacidad por defecto) o a sistemas basados en IA.

En línea con los anteriores principios, el artículo 5.2 del RGPD establece el principio de responsabilidad proactiva, es decir, que el Responsable del tratamiento será responsable del cumplimiento de los principios anteriormente expuestos, y tendrá que tener la capacidad para demostrarlo.

En este sentido, tal como apunta el ICO, todos los procesos y resultados del sistema se tienen que documentar, en un modelo que se pueda revisar y auditar. En concreto, se tendrá que documentar: (i) cómo se han considerado los riesgos para los individuos de los cuales se tratan sus datos personales; (ii) la metodología para identificar y evaluar las compensaciones en el ámbito; (iii) las razones para adoptar o rechazar determinados enfoques técnicos (si procede); (iv) los criterios de priorización y la justificación de su decisión final; y (v) como la decisión final encaja en el riesgo general.

Por último, en multitud de ocasiones, suele ser habitual que de conformidad con el artículo 44 del RGPD, el tratamiento de datos en un entorno de IA pueda comportar una transferencia internacional de datos, que se entiende como toda comunicación o revelación de datos fuera del Espacio Económico Europeo.

Esto se debe a que, a todos los efectos, todos los países fuera del Espacio Económico Europeo no prevén un nivel de protección equivalente en materia de protección de datos al que garantiza el RGPD, salvo algunas excepciones que han sido habilitadas por parte de la Comisión Europea. Por ende, deberán de adoptarse especiales cautelas al respecto.

NOTA 8.- OTRAS CUESTIONES NO CONTEMPLADAS EN EL DOCUMENTO

8.1.- Tutela judicial

Sería conveniente prever que la tutela judicial de los derechos de la ciudadanía, empresas, entidades e Instituciones contemple la posibilidad de verificación de las funcionalidades reales de los sistemas basados en IA, o que el marco procesal de dicha tutela contemple supuestos de legitimación activa institucional o colectiva.

8.2.- Fiscalidad

Se ha de proceder, asimismo, al estudio de un nuevo sistema de fiscalidad, en tanto los sistemas basados en IA tienen una dimensión económica que escapa de los sistemas fiscales tradicionales.

8.3.- Protección de los derechos derivados de la creación y explotación

Es preciso, asimismo, contemplar que los sistemas de IA están protegidos por derechos de propiedad intelectual, y valorar, si es preciso un refuerzo de la misma.

8.4.- Usos militares

Finalmente se ha de contemplar los usos de los sistemas basados en IA con fines armamentísticos o que puedan tener doble uso, civil y militar, para dotarlos de un marco regulador especifico.

9.- CONCLUSIÓN FINAL

De forma general, es preciso velar para evitar las desviaciones que puedan presentar los sistemas basados en IA que puedan ser contrarias a los principios de la UE, al reconocimiento s de los derechos humanos y al buen gobierno de las Instituciones democráticas, de forma que los usos de dichos sistemas permitan beneficios de mejora colectiva.

Barcelona, a 6 de mayo de 2020

Equipo de trabajo para la redacción del presente documento:

- *Mª Belen Arribas. Abogada Col.27700 ICAB*
- *Carles Basteiro. Abogado Col. 31669 ICAB*
- *Albert Castellanos. Abogado. Col. 40492 ICAB.*
- *Xavier Duch. Director IT ICAB*
- *Pau Enseñat. Abogado. Col. 37027 ICAB*
- *Eduardo López- Roman. Abogado. Col. 34529 ICAB*
- *Mª Angeles Montoya. Abogada. Col 15593 ICAB*
- *Mireia Romero. Jurista..*
- *Miquel Àngel Vallès. Abogado Col. 20424 ICAB*

El presente documento ha sido aprobado por la Junta de Gobierno del Ilustre Colegio de la Abogacía de Barcelona (ICAB) en sesión de fecha 13 de mayo de 2020 para su presentación ante la Comisión de la UE en el proceso de información pública del LIBRO BLANCO SOBRE LA INTELIGENCIA ARTIFICIAL - UN ENFOQUE EUROPEO ORIENTADO A LA EXCELENCIA Y LA CONFIANZA DE LA COMISIÓN EUROPEA- Bruselas, 19.2.2020 COM(2020)

.