LUIS PÉREZ-PEÑAS
JOAQUÍN PONS
ANA PEDROZA
ARTURO URRUTIA

RESPONSABILIDAD RESPECTO AL TRATAMIENTO DE DATOS PERSONALES POR PARTE DE TECNOLOGÍAS DE INTELIGENCIA ARTIFICIAL.

La normativa actual se caracteriza por garantizar la tutela judicial efectiva, sin perjuicio de una eventual tutela de los recursos administrativos que existan para señalar y sancionar un daño y, en consecuencia, una infracción de la normativa. También se añade la posibilidad de que organizaciones o entidades asuman la representación de los interesados afectados, para llevar a cabo una acción colectiva contra un responsable que les haya causado un daño.

1. El RGPD establece que el Responsable o el Encargado del tratamiento deben indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento, habiendo incumplido sus obligaciones. En particular, el artículo 82.1 establece que Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del Responsable o el Encargado del tratamiento una indemnización por los daños y perjuicios sufridos. Ello debe ser entendido incluyendo las vulneraciones presentes en las disposiciones de desarrollo del RGPD en los Estados Miembros, en el caso de España, la Ley Orgánica de Protección de datos y Garantía de Derecho Digitales (LOPDGDD).

   Dicha indemnización será totalmente independiente de los recursos administrativos o extrajudiciales disponibles – reclamaciones ante la Agencia Española de Protección de Datos -. El mismo RGPD reconoce el Derecho a los interesados a una tutela judicial efectiva para reclamar tales daños y perjuicios. El mismo artículo 79.2 señala que estas acciones contra un Responsable o Encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que tengan un establecimiento.

   Tal y como señala el artículo 80, hay que añadir que, dichas acciones, podrán ser promovidas por el mismo interesado o por entidades, organizaciones o asociaciones sin ánimo de lucro, debidamente establecida con arreglo al Derecho y cuyos objetivos sean el interés público en el ámbito de protección de los derechos y libertades en materia de protección de datos. En España, a modo de ejemplo, tales entidades podrían ser la Asociación de Consumidores y Usuarios en Acción (FACUA) o la Organización de Consumidores y Usuarios (OCU).

2. Tras mencionar las posibilidades del interesado de reclamar unos daños derivados del mal uso de sus datos, debemos señalar el régimen de responsabilidad al que se enfrentan los Responsables del tratamiento. El apartado 2 del artículo 82 del RGPD establece que cualquier Responsable que participe en una operación de tratamiento responderá de los daños y perjuicios causados en caso de que el tratamiento de datos vulnere los derechos del interesado. Este quedará exonerado si demuestra que no es en modo alguno responsable de causar el daño al interesado. Debido a ello, el Principio de responsabilidad proactiva del artículo 5.2 del RGPD cobra especial relevancia. Este principio debería proporcionar las herramientas necesarias para demostrar el cumplimento de la aplicación del RGPD, generando registros y custodiando documentos, para quedar exonerado de una eventual indemnización en favor del interesado.

   Merece especial mención el apartado 4 del artículo 82, que establece que cuando exista un tratamiento conjunto entre varios Responsables y/o Encargados, cada uno de ellos será responsable de todos los daños y perjuicios, a fin de garantizar una efectiva al interesado. No obstante, este tendrá derecho de repetición

contra el resto de los sujetos intervinientes – la responsabilidad es solidaria-. Es por ello por lo que, en caso de contratar con terceros – ya sean encargados del tratamiento o corresponsables – se debería valorar su cumplimiento de la norma y establecer un régimen de responsabilidad adecuado en el contrato.

3. Por tanto, lo más importante y perentorio, a la hora de abordar una reforma del RGPD en lo relativo a la responsabilidad de las tecnologías de inteligencia artificial, sería definir claramente los roles de Responsabilidad, Co-Responsabilidad y Encargo del tratamiento de datos llevado a cabo por dichas tecnologías, y establecer unos requisitos de claridad de la información relativa a tales Responsables y Encargados frente a los interesados titulares de dichos datos. Sería una reforma ambiciosa, pero concreta y circunscrita a la necesidad particular derivada del uso de dichas tecnologías, sin necesidad de promulgar nuevas normativas *ad hoc* y aprovechando el impulso regulatorio reciente en materia de protección de datos.

   En un segundo lugar, la normativa debería dar un trato distinto y distinguir entre datos de entrenamiento (que alimentan la IA) en fase de pre-producción, que son la base del funcionamiento automatizado de la IA y pueden determinar, por tanto, su buen o mal funcionamiento, y, por otro lado, los datos a los que accederá en fase de producción, es decir, los datos que de manera automática la IA recabará y tratará con el fin de desempeñar las tareas para las que fue programada. De manera que la normativa de protección de datos sea más clara a la hora de determinar las consecuencias del tratamiento automatizado de datos por parte de este tipo de tecnologías, y también de los diferentes requisitos que debe reunir en un caso o en otro.

   Por último, sería interesante que la normativa de protección de datos incluyese un apartado destacado para regular el papel del humano durante el funcionamiento automático de las tecnologías de IA, de manera que se establezca: (i) por un lado, los casos en los que se requiere la intervención humana, la definición de casos de emergencia y contingencia, así como una descripción a "alto nivel" de los planes y protocolos para abordar tales eventualidades; y (ii) por otro lado, el grado de responsabilidad del humano que ha intervenido en su monitorización y toma de control. La normativa debe dar ciertas pautas que permitan contestarnos preguntas como: ¿Es siempre posible la intervención humana de emergencia y la monitorización? ¿Es deseable? ¿En qué casos?

PROPUESTA SOBRE LA OBLIGATORIEDAD DE DISPONER DE SEGURO DE RESPONSABILIDAD CIVIL EN LOS PRODUCTOS QUE UTILICEN INTELIGENCIA ARTIFICIAL PARA GARANTIZAR A LOS CONSUMIDORES Y USUARIOS LA PERCEPCIÓN DE INDEMNIZACIÓN EN EL SUPUESTO DE CAUSAR UN DAÑO O PERJUICIO.

1.- INTRODUCCIÓN: EL LIBRO BLANCO SOBRE INTELIGENCIA ARTIFICIAL PONE DE MANIFIESTO QUE UNO DE LOS RIESGOS ES DETERMINAR LA RESPONSABILIDAD CIVIL.

El Libro Blanco sobre la inteligencia artificial denominado "un enfoque europeo orientado a la excelencia y a la confianza" de fecha 19 de febrero de 2020, emitido por la Comisión Europea pone de manifiesto el desarrollo sumamente rápido de la inteligencia artificial y su enorme potencial para mejorar y aumentar la eficiencia de los procesos, productos, cadenas de producción, etc, hasta el punto que indica que "cambiará nuestras vidas" y que, en el entorno extremadamente competitivo mundial en el que nos encontramos, la Unión Europea no puede quedarse atrás sino que debe potenciar su desarrollo y uso más aun con la llegada de nueva tecnología como el 5G.

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 inteligencia artificial 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.

Sin embargo, también, pone de manifiesto que el uso y desarrollo de la inteligencia artificial conllevará una serie de riesgos potenciales que deberán ser analizados y, en la medida de lo posible, eliminados o, al menos, mitigados para dotar de seguridad en el uso de productos que utilicen inteligencia artificial que, además, dé confianza a los futuros usuarios y consumidores de dichos productos.

En particular, entre otros, la Comisión Europea considera que conviene mejorar el marco normativo para abordar los riesgos y situaciones siguientes: "*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*."

2.- REGULACIÓN ACTUAL: DIRECTIVA 85/374/CEE DEL CONSEJO, DE 25 DE JULIO DE 1985, RELATIVA A LA APROXIMACIÓN DE LAS DISPOSICIONES LEGALES, REGLAMENTARIAS Y ADMINISTRATIVAS DE LOS ESTADOS MIEMBROS EN MATERIA DE RESPONSABILIDAD POR LOS DAÑOS CAUSADOS POR PRODUCTOS DEFECTUOSOS.

La Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos, establece con carácter general que el productor o fabricante será responsable de los daños causados por los defectos de sus productos.

Asimismo, sin perjuicio de la responsabilidad genérica del productor del producto, la persona que importe un producto para su distribución en un estado miembro tendrá la misma responsabilidad que el productor e, incluso, el suministrador de dicho producto será considerado como su productor a efectos de responsabilidad, a no ser que informará al perjudicado de la identidad del productor o de la persona que le suministró el producto dentro de un plazo de tiempo razonable.

Y lo más importante, es que la persona a la que se le ha causado un daño tiene la obligación de probar el daño, el defecto en el producto y la relación causal entre el defecto y el daño que, ya desde hace años y en muchas ocasiones, es imposible o muy complicado poder acreditar dicha relación causal que implica tener que asumir grandes costes en la contratación de peritajes.

Si ya en el año 1985 era muy complicado establecer la relación causal, en la revolución tecnológica actual del siglo xxi parece que será prácticamente imposible determinar dicha relación causal y, en ningún caso, puede implicar que el consumidor final de un producto que sufre un daño no reciba la correspondiente indemnización

o introducir falta de seguridad jurídica a las empresas que se dediquen a la importación o comercialización de productos.

3.- CONCLUSIÓN: NECESIDAD DE ACTUALIZAR LA LEGISLACIÓN EUROPEA EN MATERIA DE RESPONSABILIDAD CIVIL DE PRODUCTOS.

Las tecnologías que utilicen sistema de inteligencia artificial pueden presentar nuevos riesgos de seguridad para los usuarios cuando estén integradas en productos y servicios y se podrán dar situaciones en las que, como resultado de un defecto en la tecnología basada en la inteligencia artificial 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.

Los nuevos riesgos basados en decisiones adoptadas de forma autónoma de máquinas con inteligencia artificial hace aún más complicado conocer la procedencia del responsable final dado que en dichas decisiones participa desde el fabricante del producto o maquinaria que obedece las instrucciones de un software que, a su vez, ha sido creado por otra empresa diferente que se basa en inteligencia artificial desarrollada por otra empresa y que, todo a la vez, haga posible que el producto tenga la autonomía de tomar sus propias decisiones.

La falta de normativa específica que regule estos nuevos supuestos en materia de seguridad, además de suponer una desprotección a los usuarios y consumidores, puede crear inseguridad jurídica entre las empresas que comercializan productos que utilicen inteligencia artificial en el ámbito de la Unión Europea que puede desincentivar la competitividad e inversión de las empresas europeas.

Si los indicados riesgos de seguridad se materializan, la falta de requisitos claros y las características de las tecnologías de inteligencia artificial pueden complicar la trazabilidad de las decisiones potencialmente problemáticas que se hayan tomado con ayuda de sistemas de inteligencia artificial que, a su vez, puede dificultar a las personas damnificadas recibir compensaciones en el marco de la normativa en materia de responsabilidad civil.

La dificultad para hacer un seguimiento sobre la participación de todas las personas o empresas implicadas en la toma de decisiones potencialmente problemáticas adoptadas mediante sistemas de inteligencia artificial puede dar lugar a problemas de seguridad y de responsabilidad civil, pudiéndose dar el supuesto que personas que hayan sufrido daños no dispongan de un acceso efectivo a las pruebas necesarias para llevar un caso ante los tribunales y tengan menos probabilidades de obtener una reparación efectiva en comparación con situaciones en las que los daños sean causados por tecnologías tradicionales.

Como hemos explicado en al apartado anterior, 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, sin embargo, en el caso de un sistema basado en inteligencia artificial, 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, existe 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.

El uso de productos basados en la inteligencia artificial debe garantizar el mismo nivel de protección que las personas que hayan sufrido daños causados por otras tecnologías por lo que resulta necesario que la normativa en materia de responsabilidad civil sea actualizada a las tecnologías actuales que, permitan a su vez, el desarrollo e innovación dentro de la Unión Europea.

La indicada necesidad ya ha sido formulada por la Organización Europea de Consumidores y 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 inteligencia artificial. [1]

4.- PROPUESTA: OBLIGATORIEDAD DE DISPONER DE UN SEGURO DE RESPONSABILIDAD CIVIL QUE GARANTICE A LOS CONSUMIDORES Y USUARIOS LA PERCEPCIÓN DE UNA INDEMNIZACION DERIVADO DE UN DEFECTO DE PRODUCTOS QUE UTILICEN INTELIGENCIA ARTIFICIAL.

Como se ha explicado en al apartado anterior y como consecuencia de la revolución digital y aparición de sistemas inteligentes basados en inteligencia artificial capaces de tomar decisiones de forma autónoma, es necesario que la Unión Europea proceda a actualizar la normativa europea en materia de responsabilidad civil de productos que regule el uso de nuevas tecnologías y, muy especialmente, el uso de productos basados en inteligencia artificial.

Sin perjuicio de la actualización de la regulación de responsabilidad civil derivado del uso de productos (tarea que no parece sencilla y que incluso se está valorando dotar a maquinas con inteligencia artificial de "personalidad jurídica" propia) y dado que el uso de productos con inteligencia artificial puede implicar las siguientes cuestiones:

a) Que personas que hayan sufrido daños no dispongan de un acceso efectivo a las pruebas ("cajas negras") necesarias para llevar un caso ante los tribunales.
b) La imposibilidad de acreditar la relación causal que permita imputar la responsabilidad a un agente concreto que participe del proceso de toma de las decisiones de la inteligencia artificial.
c) Que el responsable del daño sea la propia inteligencia artificial por ser capaz de tomar decisiones autónomas no programadas ni previstas por sus desarrolladores.

Y, en consecuencia, que los consumidores puedan verse privados de obtener la reparación del daño causado mediante el pago de la correspondiente indemnización e incluso que éstos no estén motivados para la compra y uso de la nueva tecnología que, a su vez, retrasaría el uso de dicha tecnología perdiendo la Unión Europea competitividad respecto de otros países.

Para evitar las anteriores cuestiones, se propone que la Unión Europea regule la obligatoriedad de disponer de un seguro de responsabilidad civil cualquier productos o bienes que se comercialicen o distribuyan dentro de la Unión Europea que utilicen inteligencia artificial capaz de causar un daño relevante a sus usuarios de que dichos productos.

En España existe ejemplos en los que el legislador exige la obligatoriedad de contratar determinados seguros de responsabilidad civil, como, por ejemplo, en el uso de vehículos a motor o en los supuestos de construcción de viviendas que se exige la obligación de contratar seguro de garantía decenal.

Por último, aunque no es objeto de la propuesta, se recomienda a la Unión Europea que valore en la actualización de la normativa en materia de responsabilidad civil que, en caso de que no se pudiera imputar la responsabilidad a un agente concreto, que todos los partícipes del producto o bien fuesen responsables de forma solidaria y, a esos efectos, deban contratar determinadas pólizas de seguros.

EL RECONOCIMIENTO FACIAL

1.- EL RECONOCIMIENTO FACIAL EN EL LIBRO BLANCO

El reconocimiento facial, entendido como la recopilación y uso de datos biométricos (los "**DB**") consistentes en los rasgos físicos del rostro de cada persona para su identificación personal (el "**RF**"), es uno de los temas considerados en Libro Blanco sobre la inteligencia artificial (la "**IA**") publicado por la Comisión Europea en fecha 19 de febrero de 2020 (el "**LB**").

Más allá de que la identificación del uso del RF por una IA se identifica como un riesgo a lo largo de todo el LB, las principales conclusiones a las que parece llegar la Comisión en el LB son que:

(i) Las normas de protección de datos de la UE ya prohíben, en principio, el tratamiento de DB dirigido a identificar de manera unívoca a una persona física, siendo que 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; y

(ii) 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.

2.- CONSIDERACIONES PREVIAS EN RELACIÓN CON LA REGULACIÓN EXISTENTE EN MATERIA DE RF

2.1. La imagen del rostro de una persona como Dato Personal

No cabe duda de que la imagen del rostro de una persona constituye un dato personal (de acuerdo con el art. 3.1 RGPD) y, por tanto, el tratamiento de este dato personal para el RF debe estar sujeto a todas las normas aplicables de protección de datos personales.

2.2. El RF como Tratamiento de una Categoría Especial de Datos Personales

A este respecto, conviene diferenciar entre:

(i) RF para la verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico, como proceso de comparación entre sus DBs (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (por ejemplo, para identificar al individuo como legítimo usuario de una funcionalidad) y que funcionaría, en términos prácticos, como una clave/pin.

(ii) RF para la identificación biométrica: la identificación de un individuo por un sistema biométrico como proceso de comparar sus DBs (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).

A pesar de que el tenor literal del art. 4 RGPD consideraría ambos tipos de RF como DB (y, por tanto, una "categoría especial de datos"), parece una cuestión pacífica en la doctrina que únicamente el RF para la identificación biométrica constituye una categoría especial de datos (de acuerdo con lo expuesto en el LB o el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo del Artículo 29).

2.3. Características del RF como Tratamiento de Datos Personales

Pueden destacarse las siguientes características:

(i) Le aplican los principios relativos al tratamiento del art. 5 RGPD.

(ii) La identificación por reconocimiento biométrico resulta en el tratamiento de una categoría especial de datos, si se trata de un RF para la identificación biométrica.

(iii) El impacto sobre el interesado tiene un potencial de riesgo muy alto.

(iv) Debe justificarse la necesidad del tratamiento (que no haya alternativas menos lesivas).

(v) Debe probarse un correcto equilibro entre los posibles riesgos para el interesado y los beneficios que supone autorizar el tratamiento de estos datos personales.

(vi) El volumen de DBs capturado de un mismo interesado debe ser el mínimo necesario para la finalidad que se persigue en el caso de que no sólo se realice reconocimiento facial.

(vii) Las garantías a adoptar serán las que resulten del correspondiente análisis de riesgos y de la evaluación de impacto y que deberá valorar el responsable del tratamiento.

(viii) Se deberá consultar a la autoridad de protección de datos competente antes de proceder al tratamiento cuando la evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo (artículo 36), salvo que el responsable sea capaz de garantizar que el riesgo puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación (Considerando 94 del RGPD)

(ix) Cuando el tratamiento se vaya a realizar por un encargado del tratamiento, deberá seleccionarse uno que ofrezca garantías suficientes y haberse suscrito un contrato con el contenido del artículo 28 RGPD, en el que deberá quedar plenamente garantizado que el encargado actuará solo siguiendo instrucciones del responsable, debiendo dichas instrucciones contemplar todas las garantías adecuadas.

(x) Deberán adoptarse las medidas de seguridad necesarias conforme a lo previsto en el artículo 32 del RGPD, Esquema Nacional de Seguridad.

(xi) Debe mediar un consentimiento explícito por parte de los afectados (salvo que exista una habilitación legal, por ejemplo, en el marco del 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).

3.- ELEMENTOS A INTRODUCIR EN EL DEBATE EUROPEO SOBRE RF

Se propone introducir los siguientes elementos para el debate europeo al que alude el LB:

(i) En primer lugar, cabría aclarar de forma nítida la diferencia entre el RF para la verificación/autenticación biométrica del RF para la identificación biométrica. Asimismo, se propondría la distinción del RF para la verificación/autenticación biométrica de los supuestos de prohibición de tratamiento del art. 9.1 RGPD.

Lo anterior por las numerosas ventajas que da poder operar con el RF para la verificación/autenticación (al final, sirve como clave privada agilizando y asegurando procesos).

(ii) En segundo lugar, y en relación con el RF para la identificación biométrica, cabría establecer criterios que proporcionaran seguridad jurídica en relación con:

(a) La obtención del consentimiento. En este sentido, en el contexto de la contratación de un bien o servicio, se podría considerar la obtención del consentimiento expreso del afectado, similar al consentimiento que se otorga para recibir correo comercial del prestador o no, regulado en la LSSI española: con un 'check' de aceptación en relación con ese tratamiento en el momento de la contratación (y que hubiera forma de saber las ventajas que proporciona aceptar este tratamiento).

(b) Los criterios de proporcionalidad en la ventaja que supone para el usuario la autorización de estos datos personales en concreto.

Es este sentido, ayudaría también a que se reforzara la información acerca: (1) del tiempo que se va a custodiar el dato personal hasta su cancelación; y (2) las formas de revocar el consentimiento a este tratamiento.

(iii) En tercer lugar, en relación con el art. 35.4 RGPD (sobre el establecimiento y publicación de la lista de tipos de tratamiento que requieran evaluación de impacto por la autoridad de control), se propone crear un grupo de trabajo público – privado (representantes del Comité Europeo de Protección de Datos y de la empresa privada) para ir evaluando y aprobando casos de uso de RF de forma ágil pero a la vez permitiendo la revocación las evaluaciones de impacto positivas si se encuentran defectos durante la monitorización de las soluciones de RF.

Tal y como se establece en el LB, la colaboración público – privada es conveniente para el avance rápido y seguro de la IA en Europa. A este respecto, podrían considerarse los "Digital Innovation Hubs" (DIH) como foros de evaluación de impacto.

EL ETIQUETADO VOLUNTARIO

Para poder determinar si la adopción de un sistema de etiquetado voluntario sería útil para los sistemas de IA que no se consideran de alto riesgo, consideramos necesario realizar una comparación con otros sistemas de certificación de carácter voluntario ya existentes como, por ejemplo, el regulado en los artículos 42 y 43 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y el artículo 39 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPD), de los que se pueden extraer las siguientes características principales son:

- Carácter voluntario y disponible a través de un proceso transparente.
- No limita la responsabilidad del responsable en cuanto al cumplimiento de la normativa aplicable.
- Debe ser expedida por organismos de certificación homologados o por la autoridad de control competente.
- Tiene un período de validez y puede ser revocada.
- Creación de un registro con todas las certificaciones y que el mismo sea de acceso público.

- Actualizable y modificable con objeto de adaptarse a nuevos cambios o desarrollos.

Pues bien, partiendo de que el sistema de etiquetado voluntario que adopte la Comisión Europea, según nuestro criterio, debería tener como mínimo las características mencionadas, consideramos que en un principio este instrumento puede fomentar la transparencia y el cumplimiento de la normativa que en materia de IA adopte la UE, ya que permite a las partes interesadas evaluar rápidamente el nivel de adecuación de sus sistemas de IA a los estándares establecidos por la Comisión de un modo preventivo o proactivo. No obstante, para ello deberán implementarse mecanismos de certificación a fin de unificar los criterios para validar que un sistema de IA reúne los requisitos legales establecidos, lo cual deberá adaptarse y casar con la naturaleza potestativa o voluntaria del propio sistema de etiquetado.

Asimismo, consideramos que un eje fundamental para que el sistema de etiquetado voluntario alcance la utilidad y finalidad pretendida por la UE, es determinar de forma tasada las condiciones que deben reunir los organismos de certificación y el establecimiento por parte de la autoridad competente de instrucciones las cuales deberán ser respetadas por dichos organismos de certificación a fin de obtener el carácter o la categoría de homologados.

Finalmente, entendemos que el sistema de etiquetado voluntario, una vez sea adoptado por las partes interesadas debe tener carácter vinculante, gozar de presunción *iuris tantum* en el cumplimiento de la normativa en materia de IA y ser considerado como un acto de buena fe. Esto último, va en relación con el posible establecimiento de un régimen sancionador por parte de UE, en el sentido de que en caso de que una determinada organización acredite la adopción de todas las medidas técnicas y organizativas a su alcance para garantizar el cumplimiento de la normativa en materia de IA y se produzca un perjuicio por la utilización de su sistema basado en IA, deberá tenerse en cuenta para la determinación de la cuantía de la sanción correspondiente. Todo lo expuesto, consideramos que puede suponer para aquellas organizaciones que empleen IA un aliciente para someterse al sistema de etiquetado voluntario y superar así su propio carácter potestativo.