FACULTAD DE DERECHO

"PROTECCIÓN DE DATOS Y GESTIÓN DE RIESGOS PARA LOS DERECHOS FUNDAMENTALES EN LA REGULACIÓN DE LA IA"

Autor: Cristina Torre de Silva Fuentes

5º E-3 B

Derecho Constitucional

Tutor: Miguel Ayuso Torres

Madrid

2023-2024

ÍNDICE

1. INTRODUCCIÓN

1.1 Objeto de la investigación y metodología

El objetivo de este trabajo de investigación es realizar un estudio sobre el nuevo régimen legal de la IA en relación con los riesgos que presenta para los derechos fundamentales. Esta nueva regulación consiste no sólo en el RGPD anteriormente existente sino también en el nuevo reglamento comunitario que establece normas armonizadas sobre inteligencia artificial (Ley de Inteligencia Artificial) y modifica ciertos actos legislativos de la Unión.

Es importante establecer reglas que eviten un conflicto entre la dignidad de las personas y el fomento de la innovación de las tecnologías emergentes.

En cuanto a la metodología no solo se tendrá en cuenta la legislación europea, sino que se hará una breve referencia al derecho comparado estadounidense y británico.

1.2 Contexto

Debido al rápido avance de estas tecnologías, la Unión Europea (UE) ha hecho de la regulación de la IA un área clave de debate político en los últimos años.

Los valores y principios de la Unión Europea deberían guiar el desarrollo de las nuevas tecnologías, y los responsables políticos se han comprometido a garantizar que estas tecnologías se desarrollen pensando en la dignidad del ser humano.

Es difícil delimitar la gran cantidad de textos de derecho indicativo que se han promulgado en los últimos años en Europa sobre la IA.

Se han establecido estrategias como el Plan Coordinado en la que se fijan una serie de pautas, fruto de un consenso entre la Comisión y los estados de la UE, con objetivos como el aumento de la coordinación de las inversiones en investigación sobre esta nueva área o la creación de bases de datos comunes europeas para facilitar el intercambio de datos entre países especialmente en sectores como la salud. También se promueve el fomento del talento y el continuo aprendizaje mediante programas de información y educación especializada en IA, y el desarrollo de una IA ética y confiable, trazando condiciones éticas para su uso, que respeten los derechos fundamentales. (Comisión Europea, 2018)

La Comisión Europea se comprometió en su Libro Blanco sobre Inteligencia Artificial de 2020 a fomentar la adopción de la IA y abordar los peligros relacionados

con aplicaciones específicas de esta tecnología punta. Con la publicación de sus directrices éticas no vinculantes de 2019 para una IA ética y digna de confianza y sus recomendaciones sobre políticas e inversiones, la Comisión Europea adoptó inicialmente un enfoque de Derecho indicativo. A raíz de la publicación del Libro Blanco, se abre el debate por primera vez sobre el uso de técnicas de reconocimiento facial en sitios públicos.

Sin embargo, desde entonces ha cambiado a un enfoque legislativo, pidiendo la adopción de normas armonizadas para el desarrollo, la comercialización y el uso de sistemas de IA.

2. LA IA. PANORAMA LEGAL Y NECESIDAD DE UNA REGULACIÓN.

2.1 Evolución y concepto de la IA y de IA fiable

La Inteligencia Artificial es la habilidad de una máquina de mostrar comportamientos humanos como el aprendizaje o la capacidad de tomar decisiones; permite que sistemas electrónicos razonen y solucionen problemas. Es la tecnología emergente por excelencia de la última década. (Boucher, 2020)

Siempre ha existido el concepto contemplado por la ciencia ficción de los robots, pero se concebía como algo futurista y prácticamente imposible. Es ahora por primera vez cuando las tecnologías han evolucionado de tal forma que los algoritmos permiten a las máquinas razonar y actuar con un criterio similar al humano, basado en el aprendizaje.

La IA fue definida por la Comisión Europea en su comunicación sobre la IA de 2021 como: "los sistemas que muestran un comportamiento inteligente analizando su entorno y actuando, con cierto grado de autonomía, para alcanzar determinados objetivos". (Comisión Europea, 2021) Esta definición se vio modificada más tarde por un grupo independiente de expertos designados por la Comisión para aclarar determinados matices y para ofrecer una explicación comprensible hacia la población no experta en el sector, y nuevamente por enmiendas realizadas por el Parlamento Europeo el 14 de junio de 2023.

El Parlamento Europeo ha planteado una nueva definición más concreta que menciona los diferentes niveles de autonomía que posee la IA y los resultados que se pueden obtener a través de la misma, y que sigue la definición de la OCDE.[1]. La definición propuesta por el Parlamento Europeo tiene los siguientes elementos: la autonomía de las máquinas, la IA siempre tiene objetivos, produce unos outputs (predicciones, contenido, decisiones) y tiene un efecto en el entorno.

Además, el Parlamento quiere recalcar que la definición que se establezca por la Unión Europea estará ligada estrechamente a aquella proporcionada por diferentes organizaciones internacionales, para lograr una mayor unificación y armonización. Un ejemplo de esta cooperación es la decisión conjunta del concepto de la "IA fiable" creado por organismos europeos y estadounidenses que defienden que la IA debe ser: (1) lícita y acorde a la ley, (2) ética y acorde a una serie de principios, y (3) robusta.

[1] "*Sistema de IA es un sistema basado en máquinas diseñado para operar con diferentes niveles de autonomía y que puede mostrar adaptabilidad después de su implementación, y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada recibida, cómo generar salidas tales como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.*" *(Parlamento Europeo, 2023)*

La inteligencia artificial puede ser integrada o a través de software. El software incluye todo aquello que sea virtual, y la integrada añade los drones, vehículos independientes y demás dispositivos físicos. Hay muchas otras formas de clasificar la IA, que han sido contempladas por diferentes expertos. (Tableau, s.f.)

Analizando su evolución con el paso del tiempo, la IA ha ido ganando cada vez más autonomía. En línea con la anterior clasificación en relación con la intensidad de la inteligencia, y siguiendo un orden cronológico:

La primera manifestación o la "IA simbólica" es la que utiliza relaciones lógicas y razonamiento simbólico para encontrar soluciones. Pueden ser sistemas expertos o de lógica difusa. Los sistemas expertos aprenden a través de algoritmos creados por peritos del sector, por lo que es al fin y al cabo se utiliza un razonamiento basado en experiencia humana. Es por ello, que este tipo de tecnología alcanza su mayor auge en entornos con reglas preestablecidas y que no evolucionan o cambian con frecuencia. Por otro lado, los sistemas de lógica difusa, un poco más evolucionados, no ofrecen únicamente una opción absoluta, sino que contemplan los grises de una situación en la que un resultado se puede ajustar más o menos a una categoría. Haciendo uso de muchas más variables, se siguen pautas establecidas por humanos para tomar decisiones.

Más tarde, el aprendizaje automático o Machine Learning agilizó el aprendizaje a través de algoritmos, gracias al aumento de la disponibilidad de los datos facilitado por internet. Se crean patrones a partir de ellos, para aplicarlos a diversas situaciones. Inicialmente, se trataba de aprendizaje supervisado (con datos etiquetados)

En último lugar, la IA más avanzada (basada en redes neuronales) es capaz de formar "large language models" o "LLM", mediante aprendizaje no supervisado (con datos no etiquetados), y así proporcionar resultados más precisos. Uno de los tipos de IA recientes más novedosos es la IA Generativa. Este tipo de inteligencia, se define en la "Executive Order" de 30 de octubre de 2023 de EEUU como: *"the class of AI models that emulate the structure and characteristics of imput data inorder to generate synthetic content. This can include images, videos, audio, text, and other digital content".* (Gobierno de los EEUU, 2023).

Por tanto, la IA generativa, puede crear contenido nuevo por primera vez, a través de texto, imágenes, sonido, etc. A partir de datos que le son proporcionados anteriormente, puede resolver problemas completamente nuevos. Con aplicaciones como Chat GPT, ha sido sin duda un paso muy grande en este tipo de sistemas y ha resultado en numerosos beneficios como la optimización de operaciones en empresas, realizando tareas de síntesis o búsqueda; o el aumento de productividad de los trabajadores. Por otra parte, también supone un mayor riesgo a la hora de proteger

derechos fundamentales como el de la privacidad y el honor, por ejemplo, por el uso de imágenes no autorizadas.

Los derechos fundamentales son los inherentes a los seres humanos, y son inviolables, inalienables e irrenunciables. Deben ser respetados en todo caso, limitando las actuaciones de otras personas y de los poderes públicos en caso de que sea necesario. Están incluidos en la Constitución y protegidos a nivel internacional, por la UE en la Carta de Derechos Fundamentales.

El impacto de la IA en los derechos fundamentales es un asunto cada vez más preocupante, y ha sido recurrentemente analizado por la Agencia de la Unión Europea de Derechos Fundamentales.

Como he mencionado antes, la Unión Europea busca establecer una "IA fiable". Para ello, es necesario que se cumplan una serie de principios éticos que respeten los derechos fundamentales. El Grupo independiente de expertos sobre IA de la UE trazó una serie de requisitos clave que debe cumplir esta tecnología como que debe estar supervisada por seres humanos, debe ser segura y tener una técnica robusta y fiable, debe cumplir con los principios de no discriminación y equidad, ser acorde al bienestar social y ser transparente y respetar la privacidad de las personas y sus datos. Este último punto es el que trataré con mayor profundidad en los siguientes epígrafes. (M.Recio Gayo, 2023)

2.2 Riesgos que presenta la IA para los derechos fundamentales

Los desafíos y nuevas oportunidades que presenta la IA han hecho imprescindible su regulación. La administración y planificación de la misma no puede tomarse a la ligera, ya que, al fin y al cabo, su evolución conllevará consecuencias como la toma de decisiones por algoritmos, el desarrollo de la autonomía de las máquinas, la reestructuración del panorama laboral y de las industrias, y la posible intrusión en los derechos fundamentales de las personas.

Los derechos fundamentales son los inherentes a los seres humanos, y son inviolables, inalienables e irrenunciables. Deben ser respetados en todo caso, limitando las actuaciones de otras personas y de los poderes públicos en caso de que sea necesario. Están incluidos en la Constitución y protegidos a nivel internacional, por la UE en la Carta de Derechos Fundamentales.

El impacto de la IA en los derechos fundamentales es un asunto cada vez más preocupante, y ha sido recurrentemente analizado por la Agencia de los Derechos Fundamentales de la Unión Europea.

Hay muchos ejemplos del uso contrario a los derechos fundamentales de la IA. Existe por ejemplo un sistema del crédito social establecido en China, que está en vigor desde el año 2021 y establece que cada ciudadano tiene una serie de puntos según tu comportamiento social, vigilando el comportamiento a través de videocámaras y restringiendo tus libertades en función de esa puntuación. Hay sanciones para los que no cumplen esta "diligencia cívica". Es un sistema expresamente prohibido en la ley de IA, ya que vulnera claramente los derechos fundamentales, empezando por la privacidad, el derecho a la tutela judicial efectiva…

Han existido, además, muchos casos de manipulación del electorado a través de IA, utilizando bots para influir la opinión pública. Eso ha pasado en la elección de Gustavo Petro en Colombia por ejemplo o con Donald Trump en Estados Unidos. Es una manipulación muy preocupante

También hay casos en los que se utilizan estos sistemas para cometer delitos y estafas como los conocidos "deepfakes" utilizados para realizar estafas telefónicas, y suplantar a sujetos generando una duplicación de sus voces a través de estos sistemas para conseguir por ejemplo una transferencia fraudulenta. Esto es un atetado claro al derecho fundamental a la seguridad recogido en el artículo 17 de la CE.

Incluso podrían llegar a plantearse otras formas más extremas de manipulación como la manipulación religiosa. Algunos expertos argumentan que si la IA sigue adquiriendo este poder podría incluso crear religiones para adoctrinar y controlar a los seres humanos, que al final, son muy influenciables.

Está claro que todas estas formas de manipulación afectan gravemente a la sociedad y a los derechos fundamentales de los individuos, como al derecho de protección de datos y privacidad en el ámbito familiar que desarrollaremos más adelante (artículos 7 y 8 de CDFUE), al derecho de igualdad en casos de discriminación por categorizaciones de datos basadas en aspectos como la raza (artículo 14 CE), o incluso al de seguridad y libertad de los individuos (artículo 17 CE). Por ende, es necesario plantear una serie de salvaguardas normativas que respondan a esta amenaza estableciendo una serie de límites.

2.3 La respuesta internacional a los desafíos generados por la IA EEUU y Reino Unido

a. La respuesta en Estados Unidos

La respuesta normativa de EEU a este problema tiene dos elementos:

- La “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” de 30 de octubre de 2023”. (Executive Order).
- Numerosas regulaciones aprobadas por reguladores de toda índole de forma no centralizada.

Por lo que respecta a la Executive Order, los principios que la inspiran establecidos en su artículo 2 establecen que la IA debe ser:

- Segura (lo cual requiere evaluaciones robustas, confiables, repetibles y estandarizadas de los sistemas de la IA y políticas para entender y mitigar los riesgos.
- Respaldada por mecanismos para determinar que haya procedencia del contenido, de cuándo el contenido ha sido generado o no por la IA.
- Consistente con los derechos civiles y respetuosa (no debe favorecer la discriminación o los sesgos)
- Acorde a unas reglas de privacidad.

b. La aproximación británica. Declaración de Betchley.

El Reino Unido no tiene una regulación unificada en materia de IA, aunque sí diversa regulación dispersa, en general menos restrictiva que el IA Act europeo.

En el Reino Unido se celebró una reunión internacional denominada: “AI Safety Summit” los días 1 y de 2 de noviembre de 2023 que concluyeron en la “Betchley Declaration by Countries Attending the AI Safety Summit 1 2 November 2023” dónde se dice que: “*Para el bien de todos, la inteligencia artificial debe ser diseñada, desplegada y utilizada de manera segura, de modo que sea centrada en el ser humano, confiable y responsable”.*

Esta declaración se refiere en especial a los riesgos que plantean los modelos de IA de propósito general que plantean riesgos sustanciales asociados a usos incorrectos bien intencionados o no, especialmente en áreas como la ciberseguridad y la tecnología. Anima a los países a identificar los riesgos de seguridad en materia de IA y a crear “risk-based policies”.

Los países firmantes de esta declaración incluyen a la UE a China a EEUU al Reino Unido y a muchos otros países como Corea, Singapur, Suiza, Turquía, Kenia, Indonesia o Brasil. La lista excluye a Rusia.

Es un primer intento de lograr un alineamiento internacional de las posturas de este tema.

2.4 La respuesta Comunitaria

a. Propuesta del Convenio del Consejo de Europa

Existe un proyecto de "Framework Convention on IA, human rights, democracy and the rule of law" elaborado por el "Committee on AI" (CAI) del Consejo de Europa. Este proyecto de Convenio Internacional no sólo está dirigido a los miembros del Consejo de Europa sino también a cualesquiera otros países que quieran firmarlo.

Su texto todavía no está cerrado, pero parece que incluirá una aproximación basada en el riesgo como en la ley de inteligencia artificial europea.

b. Normativa comunitaria en materia de IA.

En cuanto a la normativa ya vigente Comunitaria en el ámbito de la IA, existe ya legislación en vigor aplicable: por ejemplo, el RGPD en materia de protección de datos, la directiva traspuesta en España de la ley de servicios de la sociedad de la información de 2022, la legislación sobre consumidores y usuarios y la legislación sobre responsabilidad por daños causados por productos defectuosos de 1985.

También existen otras directivas relativas a la utilización de datos del sector público como la Directiva 2019/1024 de 20 de junio de 2019 o la Directiva 016/680 de 27 de abril de 2016 que protege a las personas con respecto de los poderes o autoridades que tienen acceso o se les permite el tratamiento de sus datos con donde de investigación o prevención de crímenes. Otra directiva relevante es la Directiva 2002/58/CE, que se traspuso en España en 2012 conocida como ley de servicios de la sociedad de la información y de comercio electrónico (LSSI). En Europa, la denominada "ley de cookies" es aquella por la que los encargados del tratamiento de los datos de los usuarios debían solicitar el consentimiento del uso de estos pequeños archivadores de información que crean el perfil de la persona en cuestión en una web. (Martínez Rodríguez, 2021)

Además, hay leyes que regulan la forma en la que las empresas pueden acceder a los datos que tienen otras empresas o las Administraciones públicas (en el caso de que sean datos de carácter personal se exigirá el correspondiente consentimiento). Desde diciembre de 2023 es aplicable la regulación relativa a la protección de datos europea. Es el reglamento 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos, la actual "Ley de Gobernanza de Datos".

La Ley de Gobernanza de Datos regula la gestión de los datos, pero no únicamente los personales. Regula aspectos como la cesión e intercambio de datos entre empresas y al sector público. Esta ley se completa con otras iniciativas que entrarán en vigor en los próximos años como la Ley de Datos, que entró en vigor en

enero de 2024 y será aplicable en 2025, que resulta esencial para la nueva economía del dato

Además, ya hay jurisprudencia al respecto sobre este tema. Una Sentencia indispensable es la ST de 5/02/2020 del Tribunal de la Haya que declara a un sistema automatizado "SyRI" contrario al artículo 8 de la CEDH. Esta fue la primera sentencia que declaró ilegal un algoritmo con fines gubernamentales utilizado en Países Bajos para predecir el peligro y la probabilidad de estafa de los ciudadanos a hacienda.

El sistema utilizado por el Gobierno interfería en la vida privada de las personas, y no alcanzaba el interés social que podría justificar su intromisión. Este fue uno de los argumentos del tribunal, entre otros, como que no se preveía ningún requisito de informar a las personas cuyos datos se recababan. (Instituto Hermes, 2020). A la hora de emitir el fallo, se tuvieron en cuenta las reglas del RGPD, del CEDH y sobre todo la normativa de transparencia y limitación del objetivo que exigen que la regulación del algoritmo sea transparente, exacta y comprensible.

No obstante, en cuanto a los proyectos futuros, existen en este momento tres importantes normas en distintos estados de tramitación que van a abordar importantes aspectos de la cuestión, como son:

- El proyecto de directiva sobre responsabilidad civil derivada del uso de sistemas de IA. (Propuesta de Directiva)
- El proyecto de modificación de la Directiva sobre la responsabilidad por los daños provocados a raíz de productos defectuosos. (Propuesta de Directiva)
- El Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial ("IA Act")

El contenido de estos textos se desarrollará más adelante del cuerpo de este trabajo. Sin embargo, cabe adelantar los rasgos fundamentales de los mismos. Abordan aspectos tan trascendentales como la privacidad y el respeto de los derechos fundamentales.

Las dos propuestas de directivas tratan sobre la responsabilidad civil derivada del uso de productos o sistemas de Inteligencia Artificial, pero dándole un enfoque distinto.

a) En cuanto al proyecto de directiva para la adaptación de las reglas de responsabilidad extracontractual a los sistemas de IA; las normas existentes de carácter nacional que abordan este aspecto, sobre todo aquellas que se basan en la culpa, no son las más idóneas para tratar os casos de denuncias por daños originados por sistemas que utilizan la IA.

Realmente, buscar al sujeto culpable de un daño originado por un sistema no humano es lo que hace imposible asemejar estos casos con otros de responsabilidad civil en los que se ha de demostrar un daño causado por una persona física o jurídica. Esto ha supuesto un gran sentimiento de consternación a nivel nacional en cada país de la UE, que ha impulsado a la regulación de una responsabilidad por IA que regule la protección de las víctimas afectadas por los daños, y que la equipare a la producida por otros productos.

b) La Propuesta de Directiva de Responsabilidad por Daños Originados por Productos Defectuosos, tiene como objetivo la compensación de aquellos que han sufrido daños causados por productos que tienen esta condición, y que además son complejos al tratarse de productos informáticos o inteligentes. El Parlamento Europeo quiere garantizar la protección de los consumidores dándoles una protección efectiva, que en este caso se logra mediante el aseguramiento de la existencia de una empresa que tenga su sede en la Unión y sea la responsable de la comercialización de estos productos.

c) El primer proyecto, el "IA Act" es la primera iniciativa de legislación de IA en el mundo, excepto la "Executive Order" de EEUU anteriormente mencionada, que es más programática y menos detallada.

   Tiene como objetivo principal establecer una serie de normas o reglas de armonización que se apliquen en todos los Estados Miembros y regulen los usos y la comercialización de la Inteligencia Artificial en los mismos. Lucha por promover una IA fiable que salvaguarde los derechos fundamentales de los ciudadanos. La tramitación del IA Act ha sido fruto de numerosos estudios y conversaciones entre el Parlamento, el Consejo y la Comisión, que analizaremos más adelante, cuyo objetivo es llegar a definir un texto final. La ley ha sido aprobada el pasado 13 de marzo de 2024 por el Parlamento Europeo.

Antes de entrar a analizar los pasos que se han tomado hacia la regulación del IA Act, es conveniente mencionar los aspectos en los que se basan los legisladores de todos los países que regulan estas materias, que luchan por conseguir un objetivo común de reducir los riesgos que pueda generar esta tecnología y así potenciar un uso seguro de la misma que beneficie social y económicamente a la población.

Según un estudio reciente realizado por EY, la normativa en materia de IA tiene una serie de puntos comunes en diferentes jurisdicciones.

1. Siguen las pautas y principios de la IA definidos por la OCDE, entre los que abarcan el respeto de los derechos humanos y la gestión de riesgos.
2. La normativa gira alrededor de los riesgos que puede generar en relación con aspectos como la transparencia o la privacidad.

3. Se están estableciendo normas sectoriales concretas para completar la regulación general y la elaboración de otras normas relacionadas con la IA en materia de protección de datos y ciberseguridad.

Se promueve la colaboración tanto del sector público como del privado en el desarrollo de normas que promuevan una IA segura y ética. (EY, 2023)

El IA Act es el resultado de un proceso muy deliberado y meticulosamente elaborado con el objetivo de incentivar el desarrollo de este tipo de tecnología innovadora y de proteger los derechos fundamentales básicos de los seres humanos. Entre ellos, los que tienen más relevancia en este ámbito son los enunciados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE: el derecho al respeto de la vida privada y familiar y el derecho a la protección de datos de carácter personal.

El Parlamento Europeo aprobó el pasado miércoles 13 de marzo de 2024 la primera ley de IA en Europa. Es el fruto de numerosas negociaciones y acuerdos entre Estados Miembros que ha resultado en una mayoría aplastante de votos que se posicionan a favor de la creación de una base legal para esta nueva realidad tecnológica que se presenta. Tanto la ley como la Propuesta que se hizo sobre IA, publicada en abril de 2021, pretenden establecer el marco necesario para el desarrollo y la aplicación de sistemas de IA fiables en la Unión, garantizando así el correcto funcionamiento del mercado único.

El Reglamento establece una estructura jurídica uniforme que favorece la creación, la introducción de sistemas en el mercado de la Unión y la aplicación de bienes y servicios de IA. Además, la ley de IA pretende alcanzar otros objetivos específicos como que los sistemas sean acordes con la normativa europea o que se promueva el efectivo respeto y cumplimiento de los derechos fundamentales. (Madiega, 2023)

El IA Act es un Reglamento Comunitario cuyo fundamento jurídico es una gestión de riesgos. A la hora de incorporar el uso de sistemas de inteligencia artificial en la vida cotidiana de las personas, es importante hacer un análisis de los riesgos que se puedan derivar del mismo y que afecten a los derechos fundamentales de cada una de ellas.

La Comisión Europea lanzó su Propuesta en abril de 2021. Consistía en el establecimiento de un concepto neutral de IA y en la clasificación de sus sistemas según el riesgo que se asocie al uso de los mismos. Dependiendo del nivel de riesgo que presenten, el uso de este tipo de tecnología será prohibido, o se le impondrán diferentes requisitos y obligaciones para introducirse en el mercado comunitario. Los cuatro grupos principales serán los de riesgo “inaceptable”, “alto”, “limitado” y “bajo o mínimo”.

En el año 2022 el Consejo aprobó una propuesta transaccional de fecha de 25 de noviembre. En diciembre de este año, el Consejo llegó a un consenso sobre un mandato general de negociación que dio pie a diálogos tripartitos (trílogos) posteriores con el Parlamento y con la Comisión.

El Parlamento, por su parte, incluyó numerosos cambios en su propuesta de 14 de junio que, a su juicio, deberían implementarse, como los siguientes:

- En primer lugar, la definición establecida por la Propuesta debía ir en línea por la previamente acordada por la OCDE.
- En cuanto a los sistemas de alto riesgo, el Parlamento matizó que, para incluirse en esta categoría, los sistemas debían representar un riesgo considerable, que abarcaba a todos los que podrían suponer una amenaza a los derechos fundamentales. Se especificó que es necesaria la realización de una evaluación exhaustiva del impacto que pudieran tener estos sistemas en los derechos fundamentales, antes de su uso.
- En relación con los sistemas de identificación biométrica, adoptó un criterio muy restrictivo.
- Restricciones más estrictas debían aplicarse a todos aquellos proveedores de modelos fundacionales en relación a la protección del medio ambiente y de los derechos de los ciudadanos. En cuanto a los sistemas de IA generativa, que crean contenido de diferentes formas, debían someterse a pautas de transparencia, importante para evitar la intrusión en derechos de imagen y generación de contenido ilegal.
- Se promovió el establecimiento de una Oficina Central de IA Europea para aplicar la nueva legislación de forma armonizada en todos los Estados Miembros y para establecerse como órgano de organización y dirección y respuesta a las posibles reclamaciones de ciudadanos que vean sus derechos truncados.

El proceso legislativo, por tanto, ha sido fruto de numerosas conversaciones entre las principales instituciones europeas. El Consejo y el Parlamento Europeo llegaron por fin a un acuerdo provisional en diciembre del año pasado sobre la Propuesta, que intenta asegurar la protección de los derechos fundamentales e incentivar la innovación en el continente europeo. Y por fin, en marzo de este año, el Parlamento ha dado luz verde a la aprobación de la ley.

La nueva normativa va dirigida a todos aquellos que promuevan el uso de IA entre los países miembros o aquellos que introduzcan sistemas en el mercado de la UE. Sin embargo, no será de aplicación en materia de seguridad nacional, ni en otros casos excepcionales como el uso de sistemas que se utilicen únicamente para objetivos de defensa, ni para aquellos dedicados a propósitos de I+D.

El Reglamento presenta una clasificación de sistemas con estructura piramidal basada en los riesgos, según la cual se establece un nivel de intervención legal u otro. (Noticias Parlamento Europeo, 2023). Esta clasificación se basa en el uso o los usos a los que se destinen los sistemas en cuestión. Un mismo sistema podría generar distintos tipos de riesgo según el fin al que se destine.

La clasificación según el uso de los sistemas de IA es la siguiente:

- Prácticas prohibidas
- Sistemas cuyo uso genera un alto riesgo
- Sistemas de riesgo medio o mínimo

Además de esta división, que veremos más adelante en profundidad, existe una excepción que se refiere a aquellos modelos de IA de propósito general.

Este nuevo Reglamento también recoge el ámbito de la responsabilidad de los usuarios y proveedores de la tecnología. Se establecen multas de cantidades predeterminadas o en base a lo que facture la empresa infractora en cuestión, con límites distintos para empresas de diferentes tamaños y antigüedad.

En cuanto a la protección de derechos fundamentales, el aspecto más novedoso de la nueva regulación es la evaluación del impacto de los sistemas sobre los derechos, que he mencionado anteriormente. Se han establecido numerosos requisitos para los proveedores de estos sistemas de alto riesgo de transparencia, y de información a los usuarios del tratamiento de los datos que proporcionan a veces de forma inconsciente.

Además de todas estas nuevas medidas, en aras de incentivar la innovación, se han establecido medidas que favorecen el uso de la IA, y que pueden suponer enormes ventajas como la agilización de procesos laborales y el alivio de carga administrativa para las empresas. (Administración electrónica del Gobierno de España, 2023)

Es por ello que surge la necesidad de establecer unas reglas armonizadas por las que se rijan todos. Las máquinas no tienen sentido de la moral o la ética, por lo que el nuevo reglamento propone una serie de condiciones o requisitos para que los sistemas que entren en la categoría de alto riesgo, sean fiables. Por otro lado, no podemos aceptar ciegamente los resultados generados por IA, ya que no son del todo precisos. Aunque haya un porcentaje ínfimo de error, es importante tenerlo en cuenta por si se les da un uso que pueda afectar directamente a las personas; (imaginemos un caso en que alguien inocente es reconocido por un sistema de identificación como culpable).

En aras de obtener información fiable de usuarios de sistemas de esta índole, es importante recabar el mayor número de datos; por ejemplo, de las características de las personas si se estuviera realizando un estudio de no discriminación. La disyuntiva que se plantea en este caso es el choque generado entre la recopilación de estos datos y la protección de los mismos. Es aquí donde surge el conflicto entre los derechos de

privacidad de las personas y el uso responsable de sistemas de IA. El nuevo reglamento de la IA intenta lograr un equilibrio en el que los sistemas que supongan un alto riesgo hagan una evaluación íntegra del grado de afectación a los derechos fundamentales. (Pehlivan, 2023).

3. PROTECCIÓN DE DATOS EN EL ÁMBITO DE LA IA. EL RGPD.

3.1 Introducción

Existen numerosas leyes que regulan la protección de datos a nivel europeo. En primer lugar, destaca un Reglamento General de Protección de datos y otras leyes relevantes en esta materia como el Reglamento de Servicios Digitales y la Ley de Ciber resiliencia.

En cuanto al Reglamento General de Protección de Datos, se fija su objeto en su artículo 1: "*El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos."*

Asimismo, hace referencia a esa especial protección que merecen los derechos fundamentales en este ámbito: *"El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales."* (Parlamento Europeo y Consejo, 2016).

El RGPD, por tanto, defiende el derecho de los individuos a que no se traten sus datos personales sin una base legitimadora adecuada.

La aplicación de este reglamento tiene una particularidad: serán protegidos todos aquellos usuarios que estén establecidos en la Unión, aunque el tratamiento de los mismos se realice fuera de la misma, la protección no depende del lugar de contratación de los servicios.

Todas estas leyes abordan la protección de los datos en la era digital a nivel europeo, pero también existen otras a nivel nacional como es la Ley General de Protección de Datos en España (Ley Orgánica 3/2018, de 5 de diciembre) cuyo objetivo es proteger la intimidad de los usuarios de la tecnología emergente. Tanto esta última ley como el reglamento mencionado anteriormente regulan el tratamiento de datos personales, pero la LGPD española añade aspectos no contenidos en la regulación europea como una serie de artículos que velan por la protección de derechos digitales (80-97) y otros que se relacionan con los datos personales de personas difuntas y el uso que pueden darle sus familiares.

3.2 Conceptos, obligaciones y consentimiento informado del uso de datos.

El avance exponencial de la IA lleva consigo una amenaza hacia derechos indispensables como son la privacidad de los usuarios y la protección de datos. La

recopilación masiva de datos en la actualidad y el uso de los mismos por algoritmos autónomos como la IA nos hace plantearnos los dilemas éticos que acompañan a esta revolución tecnológica. Una de las soluciones para establecer un equilibrio entre innovación y protección de la vida privada de los ciudadanos es establecer un marco legal robusto, y es por ello que se están promoviendo nuevas iniciativas legales. En aras de realizar un análisis del modo en que estas nuevas propuestas abordan estos derechos fundamentales, y los límites que no deberían sobrepasar, es importante tener claro el ámbito objetivo de los mismos y donde se recogen.

En el Título II de la Carta de los Derechos Fundamentales de la UE, se recogen una serie de libertades, entre las cuales se encuentran el respeto a la vida privada y familiar y la protección de datos de carácter personal:

- Respeto de la vida privada y familiar (recogido en el artículo 7 CDFUE, y a su vez en los artículos 8 del CEDH y 18 de la CE)
  "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones"
- Protección de datos de carácter personal (recogido en el artículo 8.1 de la CDFUE y a su vez en el 16.1 del TFUE y 18.4 de la CE)
  "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
  2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
  3. El respeto de estas normas estará sujeto al control de una autoridad independiente"

Vemos que el ámbito de protección establecido en estos derechos se limita a los datos de carácter personal de personas físicas, sólo este es un derecho fundamental.

Por otro lado, en la versión más definitiva que existe actualmente sobre el futuro IA Act, se menciona la necesidad de realizar una evaluación de impacto en los derechos fundamentales; pero se hace hincapié en que no será esencial cuando estos derechos sean cubiertos por otras obligaciones legales como la evaluación de impacto en derechos como el de protección de datos por el RGPD. Vemos, por tanto, que es necesario asegurarse previamente de que no haya impacto en la privacidad de los individuos según lo establecido en esta ley.

Por todo lo anterior, es importante establecer el impacto real que tiene este RGPD en la regulación de la inteligencia artificial, para entender de qué forma queda protegido por la nueva ley.

En primer lugar, debemos analizar el ámbito de aplicación de este Reglamento, referido a datos de carácter personal de personas físicas. En su artículo 4 se delimita el concepto de dato de carácter personal, que son todos aquellos que incluyen toda aquella información sobre una persona identificada o identificable. Se incluyen tanto los más básicos como el nombre como otros aspectos asociados a la actividad, la economía o cultura de esa persona. Se excluye por tanto todo aquello que se refiera a fenómenos no humanos y a la información que no se refiera a individuos en particular.

Todo aquello que no entre dentro de este ámbito se consideraría datos de carácter no personal y no quedan protegidos por esta legislación. Y es que, muchos sistemas de IA procesan datos personales. En algunos casos se utilizan para crear el algoritmo para su continuo aprendizaje y en otros para estudiar o predecir el comportamiento de un individuo con diferentes fines. Pero, aun estando sometidos a todo tipo de controles muy estrictos, existe un margen de error que se deriva de la gestión no humana de la información. Y aquí es donde empieza la controversia, cuando se crean sesgos, resultados discriminatorios o que puedan crear un efecto injusto o no del todo exacto.

Existen formas de eliminar los riesgos que conllevan la identificación de las personas como la anonimización. A través de este procedimiento, se pueden reducir las posibilidades de identificación de un individuo, manteniendo la claridad de los datos proporcionados, es decir, sin implicar su distorsión.

Al relacionar información sobre individuos con categorizaciones y anticipaciones correspondientes, la inteligencia artificial aumenta la capacidad de crear perfiles, y realizar juicios y elecciones basadas en esta información. Aunque el RGPD se enfoque en el perfilado realizado a individuos concretos y no a grupos, es posible que los individuos dentro de un estudio de grupo salgan perjudicados y otros injustamente beneficiados. En su artículo 4.4 el RGPD define perfilado como un modo de tratar datos personales que permite deducir otra información acerca de un individuo mediante predicciones. (Parlamento Europeo, 2020)

Este perfilado se realiza sobre datos personales, de forma automatizada y para examinar características de una persona. Al ser personales, se les aplica la protección que estamos analizando. En el caso de que se creen este tipo de perfiles, los sujetos implicados deben tener acceso a la información utilizada en un principio y también a aquella originada como resultado de la inferencia. En cuanto a la rectificación de la información que se ha deducido a través de este proceso, los individuos en cuestión tienen derecho a rectificarla, independientemente de la verificabilidad de las predicciones. Porque existen casos en los que una predicción no pueda aplicarse a otras. Por ejemplo, los alumnos de un colegio A son mejores en deportes que en el colegio B, esto es una estimación general que no tendría por qué aplicarse a los

mejores atletas del colegio B. Por todo lo anterior, se argumenta que debería otorgarse un derecho a la "inferencia razonable de datos" que respete los fundamentos éticos de la sociedad. (Agencia Europea de Protección de Datos, 2020)

Para lograr esta inferencia prudente, deben tenerse en cuenta una serie de criterios elaborados por expertos legales tras un estudio exhaustivo de la cuestión:

- Los datos iniciales que se proporcionan deben ser aceptables según un baremo normal y racional; excluyendo por ejemplo datos más íntimos como preferencias sexuales.
- La información resultante, lo inferido, debe ser importante para el objetivo al que se quiere llegar al tomar la decisión, debe estar ligada al mismo.
- Los datos iniciales, deben ser lo más verosímiles y confiables posibles.

En cuanto al consentimiento para el tratamiento de los datos; es una afirmación específica expresada sin coacciones de forma libre, evidente, y basada en conocimientos informados, por la que se acepta este tratamiento sobre sus datos personales. (Parlamento Europeo, 2020)

Además de los anteriores requisitos para que sea un consentimiento válido deben dirigirse a todos los fines para los que van a ser tratados los datos. La necesidad de especificar uno por uno los propósitos en el consentimiento es lo que conforma un consentimiento granulado.

- La aportación del consentimiento del tratamiento de datos para fines específicos, plantea la posibilidad de extender este alcance al uso de la IA de los mismos para su aprendizaje y el análisis de datos. Debido a la especificidad requerida en el consentimiento para unos fines concretos, no debería ser posible. Sin embargo, si el tratamiento de datos tiene un objetivo legítimo, está respaldado por un marco legal y no desvirtúa el objetivo del agrupamiento de datos inicial, no tiene por qué ser un problema. Un ejemplo de esto podría ser destinarlos al ámbito de la investigación.
- La no coacción u obligación de aportar estos datos puede desdoblarse en dos enfoques. No existe libertad cuando no es posible la retirada de la aceptación del tratamiento y este consentimiento estaba abarcando más de lo inicialmente pactado, ni cuando la elección de proporcionar la información que se solicita no es genuina. Cuando una empresa se encuentra en una posición dominante y genera una dependencia en los usuarios que la utilizan, pueden forzar de alguna forma la aprobación del titular de los datos que no quiere verse privado de los servicios que aportan estos entes. Lo mismo ocurre con los poderes públicos que actúan desde una posición de superioridad. En cuanto a la IA, ya está formando parte de nuestra sociedad y vida cotidiana actualmente, y cada vez se generará una dependencia mayor de los usuarios a medida que vaya

evolucionando, por lo que es esencial la regulación de unos límites que eviten abusos basados en consentimientos no genuinos de tratamiento de datos.

- El hecho de que hablemos de un consentimiento granulado, implica que aquel que aporte los datos nunca va a verse forzado a aceptar conjuntamente el uso de sus datos para diferentes fines y que, por ejemplo, al decir que sí el interesado al uso de los datos para áreas específicas, o para beneficiarse de una utilidad, no necesariamente da su consentimiento hacia la creación de perfiles por parte de la IA.

Sin el consentimiento, no se puede entender el derecho a la protección de datos. Se pretende proteger el uso de datos propios, mediante la información y el requisito de aceptación por la persona afectada. De todas formas, existen algunas críticas hacia este planteamiento, que hacen plantearse hasta qué punto queda protegido este derecho de protección.

En primer lugar, el consentimiento muchas veces carece de fundamento al no basarse en una decisión informada realmente, y por tanto consistir en una decisión más bien tomada a ciegas. En la mayoría de los casos, cuando se nos solicita permiso para el acceso y manipulación de nuestros datos, no sabemos realmente qué implica este consentimiento, no tenemos los conocimientos o habilidades para comprender el riesgo que implica nuestra aceptación debido a la complejidad de este tratamiento.

Por otra parte, rechazar el uso de los mismos puede, en ocasiones, limitar el acceso o la utilización de servicios que se consideran básicos o cruciales para la persona implicada. La no aceptación por tanto puede tener implicaciones perjudiciales para el individuo que pretende proteger su derecho de privacidad, y además puede resultar en un perjuicio de investigaciones o hallazgos futuros como por ejemplo en el caso de registros sanitarios para realizar el seguimiento de un brote de gripe o la detección de blanqueo de capitales a través de controles financieros.

Queda por tanto abierto el debate sobre hasta qué punto este consentimiento es realmente libre y por tanto válido, pero está claro que la autorización propia del afectado es esencial para el acceso a los datos personales. El desarrollo de la IA y sus múltiples ventajas que abrirán numerosas puertas en un futuro debe encontrar un equilibrio con esta protección del ser humano y el consentimiento informado sobre su aportación personal a estos sistemas, que se nutren y aprenden a través de ellos.

3.3 Compatibilidad de los principios del RGPD con los usos de la IA

Es esencial que contrastemos los riesgos que pueden derivarse del uso de la IA contrastados con los principios de protección de datos recogidos en el RGPD que no pueden pasarse por alto. Estos son: (1) la licitud, transparencia y lealtad, (2) la limitación

de la finalidad, (3) la minimización de datos, (4) la exactitud, (5) la limitación del plazo de conservación y (6) la confidencialidad e integridad. (Agencia Europea de Protección de Datos, 2020)

1. La transparencia

En el artículo 5.1 a) del reglamento se especifica que los datos que se traten deben ser manipulados de forma lícita, equitativa y transparente con respecto del que los aporta. (Servicio de Investigación del Parlamento Europeo, 2020))

Centrándonos en la transparencia de los datos, se analiza la accesibilidad de los datos, la medida en que la información aportada es comprensible y con un lenguaje común, que sea certera y fácilmente alcanzable.

Es importante realizar una distinción clave para diferenciar la transparencia en la aportación de datos y lo que se conoce como "IA explicativa". En el RGPD se diferencian dos tipos de equidad, una meramente informativa que intenta evitar que los titulares de los datos sean manipulados o reciban información poco clara que les conduzca a tomar una decisión involuntaria y otra más sustantiva que hace referencia a la exactitud con la que se procesan los datos, que deben estar sometidos a un proceso estadístico adecuado y generar soluciones con el menor número de fallos, minimizando de esta forma el riesgo para los que los aportan.

Por tanto, para que el tratamiento de datos sea justo, los titulares deben ser informados de los fines del mismo y de la forma en que van a ser procesados. Se espera además que se cumplan los objetivos para los que se aportó la información; el resultado del tratamiento genera responsabilidad. He aquí el problema, cuando hablamos de IA y el procesamiento complejo de los datos relacionados con la misma; muchas veces no están claros ni los objetivos del tratamiento ni el proceso por el cual se consigue esta automatización de sistemas. Por eso es necesario que se detalle el origen de las decisiones de estos sistemas y sobre todo cuando se acumulan una cantidad de datos muy considerable, para que no exista discriminación o injusticia en el proceso.

2. La limitación de la finalidad

Pasando al apartado b) de este mismo artículo, la limitación de la finalidad se refiere a la especificidad de los objetivos o metas para los que se facilitan los datos. Tienen que ser propósitos específicos, explícitos y legítimos (Servicio de Investigación del Parlamento Europeo, 2020) y su procesamiento tiene que ser acorde a los mismos, con excepción de algunos fines con un interés superior como de aportación a la ciencia, historia o estadísticos que no choquen o sean contrarios a los objetivos iniciales.

La IA puede entrar en conflicto con esta limitación de propósito drásticamente, ya que parte de su naturaleza y funcionamiento se basa en la asociación de información que se reutiliza para sacar conclusiones y se acaba destinando a otros fines, como pueden ser el análisis de un sector o de la opinión de los consumidores para influir en un proceso de marketing, por ejemplo.

Por esto hay que examinar la legitimidad de este reciclaje de información, viendo si se alinea con los objetivos iniciales que se propusieron, y, por tanto, si es compatible con los mismos. Se han planteado formas de analizar esta compatibilidad examinando la cercanía o proximidad de objetivos, el impacto de la reutilización y cómo afecta al interés de los individuos y las medidas de protección establecidas para prevenir riesgos nuevamente originados. Dependiendo de si esta inferencia es personalizada para un individuo concreto o forma parte del entrenamiento de un sistema que recoge datos de muchas personas distintas, habrá unas consecuencias u otras.

3. La minimización de datos

En el apartado c) del artículo 5.1 del Reglamento se establece que los datos deben ser limitados y deben atenerse a los fines a los que son destinados. Realmente, el uso de la IA deriva en muchas ocasiones en el logro de objetivos inimaginables o inesperados que surgen por la interpretación de datos iniciales. Es por ello que se establecen excepciones a esta minimización en caso en los que de la inclusión de más datos a un proceso tenga como meta la obtención de una ventaja considerable. De todos modos, se debe asegurar un equilibrio razonable con la minimización.

Un ejemplo de menor control en cuanto a la cantidad de datos aportada se aprecia en estudios de carácter estadístico, que acaban siendo usados para un fin como una investigación, no meramente con el objetivo de la recopilación de los mismos. El riesgo surge cuando los datos que se reunieron para elaborar una estadística son usados finalmente de forma extralimitada. Lo que se tiene en consideración es si los patrones que existen entre diferentes personas que la IA asocia a un grupo se utilizan para realizar predicciones sobre un individuo en particular que pertenece al grupo o sobre el grupo en general. En este último caso, no existe protección de datos como tal para los miembros del grupo.

4. La exactitud

La exactitud establecida en el artículo 5 del Reglamento hace referencia a la necesidad de que los datos aportados sean precisos y estén actualizados en la medida en la que se requiera. También hace referencia a la rectificación o eliminación de datos incorrectos que no alcanzan este grado de exactitud.

Los datos que no cumplen con este principio suponen un riesgo hacia los sujetos, en situaciones en las que son procesados y no representan la identidad del sujeto. Una forma de mitigar esta amenaza es la anonimización que se ha mencionado anteriormente.

5. Limitación del plazo de conservación

Este principio hace referencia al almacenamiento de los datos y está recogido en el apartado e) del mismo artículo. La limitación del tiempo en que se conserven los datos es importante también en relación con el principio de la limitación de la finalidad. Los datos se almacenan para un fin y deben conservarse el tiempo que se necesite para lograr conseguir este fin.

Existen algunas excepciones en las que sería posible dilatar este periodo de tiempo en tanto en cuanto los objetivos de su almacenamiento estén relacionados con ámbitos como la investigación histórica o científica, entre otros, siempre que se respeten las restricciones necesarias que se apliquen a estos casos concretos.

6. La confidencialidad e integridad

En el último punto del artículo 5 del RGPD se recalca la importancia de que los datos estén sometidos a unas medidas de seguridad que garanticen su entereza e imparcialidad en lugar de perderse o dañarse y que se revelen únicamente en relación con el fin al que se destinan.

En el contexto de IA, teniendo en cuenta que se procesan y tratan cantidades muy grandes de datos, este principio cobra especial importancia por la naturaleza sensible de los mismos. Prácticas que fomenten la seguridad como la encriptación de datos o la autenticación de usuarios ayudan a proteger la integridad y confidencialidad de los datos personales.

3.4 Tratamiento de datos e IA. Base legitimadora.

Una vez analizado como se relacionan los principios establecidos en el RGPD con los usos de la IA, debemos ver si el tratamiento de datos en el contexto de la IA está justificado y atiende a fines legítimos. Esta validación debe realizarse antes de comenzar con el procesamiento de los datos. Sin ella no se debería poner en marcha el proceso. Para analizar esta relación con los principios del RGPD se han publicado numerosos informes y estudios como el de la Agencia Europea de Protección de Datos "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial." y el estudio del Parlamento Europeo "El impacto del Reglamento General de Protección de Datos (RGPD) en la inteligencia artificial", cuyas conclusiones se analizarán a continuación.

Es importante primero de todo tener una noción de los momentos en que es posible realizar este tratamiento de información personal haciendo uso de IA.

Teniendo en cuenta las etapas de la vida de un sistema de inteligencia artificial, podemos diferenciar:

- La concepción o inicio del proceso: donde se establecen las medidas para implementar la opción desarrollada por la IA. Este es el punto inicial del procesamiento con IA, en el cual se diseñan y planifican las metas que se quieren alcanzar.
- El desenvolvimiento o desarrollo del sistema; es la etapa en la que se desarrolla el sistema como tal. Incluye fases como el entrenamiento, el aprendizaje o la validación del mismo.
- La fase de operación: es la fase que implica llevar a cabo actividades como fusión, implementación, toma de decisiones, desarrollo continuo etc. Una vez recopilada la información y tras haber pasado por este entrenamiento previo, se sacan conclusiones y se genera una solución.
- La eliminación final del tratamiento. Puede ser originada por la cesación del uso del sistema de IA por parte del propio usuario o porque el sistema se retira por completo.

Es esencial recordar que tanto el bloque IA como los diferentes componentes individualizados que lo integran se deben considerar en su totalidad. Estas fases pueden coincidir, superponerse o ocurrir simultáneamente.

Teniendo en cuenta estas etapas del ciclo de vida de un sistema, se produce el tratamiento de datos personales en momentos como el entrenamiento (que incluye sistemas automáticos de aprendizaje que recopilan datos). Necesitan de estos datos personales para fines como la obtención de las fuentes en las que se basa su aprendizaje o la división de los datos en diferentes subconjuntos que se utilizan con diferentes propósitos como para observar el rendimiento de un modelo.

En cuanto a la validación de los datos, que implica utilizar datos personales reales para evaluar la efectividad y precisión de un modelo, es importante tener en cuenta que muchas veces los datos utilizados para examinar el modelo, los de verificación, pueden ser distintos a los utilizados para su entrenamiento. Además, la verificación puede ser incluso realizada por un tercero para garantizar que el modelo cumple con ciertos requisitos o estándares de calidad y precisión.

En la fase de operación, podemos encontrar procesos que necesitan del tratamiento de datos, como la inferencia, consistente en la recogida de información para llegar a una conclusión. También se aprecia este tratamiento en la toma de decisiones, e incluso para el desarrollo del propio sistema de IA. Mediante la

aportación de datos por parte de los usuarios, en el momento en que se usen para cambiar el modelo o para renovarlo o hacer que evolucione mediante su incorporación.

En los casos definidos, en los que se tratan datos personales, el sistema o elemento de IA debe regirse por las normas que dicta el RGPD. Puede ser que se produzca un tratamiento de datos en una sola etapa del ciclo de vida del sistema de IA, en cuyo caso esta deberá someterse al Reglamento. Es importante determinar el carácter de los datos para saber si entran dentro del ámbito del RGPD, distinguiendo si son o no personales.

Teniendo claras las diferentes etapas que sigue un sistema de esta índole, pasamos a recalcar si el procesamiento de los datos que se requiere para su desarrollo es realmente legítimo. Y para esto, nos remitimos al artículo 6 del RGPD:

> *"El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*
>
> *a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.*
> *Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.*(RGPD, 2016)

Este artículo expone las bases que legitiman el procesamiento de datos de carácter personal en este contexto. Los seis fundamentos jurídicos (6.1 a)…f)) se dividen en tres más generales y otros para situaciones con un mayor grado de excepcionalidad. Con carácter general, son bases jurídicas legitimadoras del tratamiento de datos personales:

1. La resolución de un contrato requiere del procesamiento de estos datos personales o para fijar requisitos antes de la contratación
2. El logro de un interés legítimo que no se sobreponga o choque con los de los del individuo que aporte sus datos personales, y que espera la protección de los mismos.

3. La aceptación de los titulares de los datos que hayan expresado su consentimiento de forma evidente para que se traten sus datos.

Además de estos motivos de carácter general podemos apreciar otros casos cuyo fundamento reside en:

4. La salvaguarda de los intereses vitales de aquel que no esté capacitado para protegerlos o para mostrarse receptivo al tratamiento. (artículo 9 del RGPD)
5. Por motivos de interés público o por el ejercicio de poderes públicos, (como en ciertos casos sanitarios o de control de fronteras).
6. Por cumplir con requisitos legales.

En el caso (5) y (6) las bases legitimadoras deben ser fijadas por órganos jurídicos de la Unión, no es suficiente con la mera atribución de las mismas por parte del usuario titular de los datos. (Agencia Europea de Protección de Datos, 2020)

De todas formas, independientemente de la legitimidad del tratamiento basada en estos fundamentos legales, se deben tener en cuenta los principios que se mencionaron del RGPD como es la limitación de la finalidad o la minimización de datos. El tratamiento de datos tiene que realizarse para el logro de un fin específico, y con la exactitud o transparencia requeridas.

En esta línea, si un individuo o ente hace uso de datos personales de terceros, debe siempre cerciorarse de que la procedencia de estos datos está amparada en una base legitimadora, realizando la correspondiente investigación y actuando de forma diligente.

Probablemente, la base jurídica más controvertida para la licitud del tratamiento de datos personales corresponde al apartado f) del artículo, que plantea la presencia de un interés legítimo que justifique el tratamiento. En el caso de que se demuestre que existe un interés superior de esta índole, no es necesario ni siquiera el consentimiento del titular, por lo que debe estar justificado y debe ser sometido a la evaluación pertinente. En general, la AEPD es muy restrictiva en cuanto al uso del interés legítimo como base legitimadora para el perfilado de clientes.

En el ámbito de la IA, es necesario realizar una distinción entre aquellos datos que se aportan con el objetivo de formar parte de un sistema de aprendizaje de un modelo y aquellos que se aportan con el propósito de acceder a un modelo ya creado. En el primer escenario, y asumiendo que los encargados del procesamiento de datos siguen un interés permitido por la ley, los titulares de los datos personales en principio no deberían sufrir graves consecuencias; pero si estos datos se usan para crear un perfil o deducir ciertos aspectos sobre el individuo, éste debería tener una posición privilegiada y debería respetarse su voluntad y consentimiento. (Servicio de Investigación del Parlamento Europeo, 2020)

Como en todo conflicto de intereses, la prueba de este interés legítimo es esencial para valorar el impacto y la presencia de algunos programas informáticos y aplicaciones. Es imperativo que los responsables del tratamiento de los datos evalúen de forma exhaustiva la afectación de los derechos del titular de los datos, y que implementen medidas de responsabilidad y para la protección de los mismos. Es por esto por lo que algunos sistemas de reconocimiento facial o vigilancia biométrica pueden verse perjudicados o incluso ser eliminados por proteger los intereses y la privacidad de los usuarios. Sin ir más lejos, muchas de estas se califican como "prácticas prohibidas" por la nueva ley de IA.

Las bases jurídicas tienen efectos irretroactivos en el caso en que dejaran de existir, es decir, el modelo en cuestión para cuyo funcionamiento se necesitó el acceso a datos personales, puede seguir existiendo y funcionando con normalidad siempre que se tengan en cuenta las peticiones de los usuarios relacionados con la privacidad de sus datos. Si por ejemplo se utilizaran datos para entrenar un algoritmo de IA que recomienda productos en un sitio web de compras, aunque el consentimiento de tratamiento de datos fuera retirado por parte del titular, el sitio web todavía podría seguir utilizando este algoritmo para recomendar productos a los usuarios. (Agencia Europea de Protección de Datos, 2020)

Se deben tener en consideración de igual forma los requisitos especiales para el tratamiento que se atribuyen a ciertas modalidades de datos como la identificación de la orientación sexual, por ejemplo, recogidos en el artículo 9 del reglamento.

4. GESTIÓN DE RIESGOS E IA

4.1 Protección de la nueva regulación y gestión de riesgos para derechos y libertades.

El nuevo Reglamento de la UE "IA Act" basa su estructura en un análisis de los riesgos que puede generar el uso de los sistemas de IA. Tiene una estructura clasificatoria de los sistemas basada en estos riesgos, según la cual se establece un nivel de intervención legal u otro. Lo que se busca con este sistema es la protección de los derechos fundamentales de los individuos incluidos en la Carta que pudieran verse afectados por las técnicas intrusivas de estos sistemas.

El Reglamento clasifica las prácticas en: prohibidas, de alto riesgo, de riesgos mínimo, y de propósito general como la IA generativa, según su uso. Lo esencial que se analiza es el uso del sistema, no el sistema en sí. En el caso por ejemplo de el piloto automático de un avión o el programa de entrenamiento para pilotos son sistemas de IA de alto riesgo, en cambio si utilizáramos ese mismo sistema a un videojuego de pilotaje, que no es un propósito serio, no sería un sistema de alto riesgo: el riesgo se mide por el uso que se da al sistema, no por sus prestaciones.

Además de esta división que se detalla a continuación, se establecen una serie de normas para la puesta en funcionamiento y comercialización de los sistemas y del mercado en la UE.

- Las prácticas prohibidas son aquellas de cuyo uso se deriva de un riesgo inaceptable. En el artículo 5 del título II del Reglamento se establece una lista de usos de IA que entran en esta categoría. Algunos ejemplos son la división de las personas por sus diferentes rasgos o ciertos sistemas de reconocimiento facial.
- Los sistemas generan un alto riesgo cuando de su uso se deriva una amenaza para los derechos fundamentales. Algunos de estos sistemas son los que se aplican a productos que se rigen por la ley de seguridad de productos de la UE, y otros que afectan a sectores como la educación, el empleo o la asistencia jurídica.
- Los sistemas que podríamos calificar como de riesgo medio o mínimo (dentro de los que englobo los de riesgo limitado y riesgo cero), son aquellos de los que no se derivan obligaciones por el uso de estos más que requisitos de trasparencia para evitar la generación de contenido ilegal o la manipulación de imágenes. Los de riesgo limitado tienen un

cierto grado de interacción con los humanos. Por otro lado, los de riesgo cero (que son prácticamente inexistentes) son aquellos de los que no se deriva obligación alguna ya que presentan un riesgo insignificante. De todas formas, se recomienda que estos sistemas sigan una serie de Códigos de Conducta establecidos.

- Más allá de esta organización de los sistemas según su uso, existe una excepción que se refiere a los modelos de inteligencia artificial de propósito general. Este tipo de tecnología ya no se debe incluir en las categorías mencionadas atendiendo al uso al que se destine, sino que, independientemente del fin al que se quiera dirigir, va a tener que someterse a una serie de condiciones y criterios por su sola naturaleza y propósito.

Además de esta clasificación, se establece un análisis de impacto del uso de sistemas en los derechos fundamentales de los usuarios que abordaremos más adelante.

a. Usos prohibidos

La lista de prácticas de IA basadas en el uso de sistemas que quedan prohibidas son las que se enuncian en el artículo 5 de la ley. Este artículo tiene gran relevancia porque establece un límite que no se puede sobrepasar para la protección de los usuarios en materia de IA. El uso de sistemas muy evolucionados podría sino dañar gravemente la privacidad y seguridad de los titulares de los datos.

No se permite la puesta en mercado o comercialización de sistemas que influyan inconscientemente en el comportamiento del consumidor o que conduzcan a error o a engaño, y como resultado afecten a su toma de decisiones y generen un daño importante en los derechos de un tercero o de esa misma persona. Tampoco podrán comercializarse los sistemas ya mencionados que utilizan datos biométricos para recoger datos personales relacionados con aspectos como la religión o la raza para establecer divisiones entre individuos, ni de los que a raíz de la clasificación de usuarios se derive un tratamiento discriminatorio.

En cuanto a los sistemas de identificación biométrica en tiempo real, que veremos más adelante, siempre que no se den las excepciones pertinentes relacionadas con la prevalencia de otros derechos fundamentales, también quedan prohibidos bajo el ámbito de esta ley.

Los sistemas que tengan el propósito específico de analizar el riesgo de la comisión de un delito, basados en la evaluación de características de un individuo, quedan prohibidos a menos que su uso respalde la evaluación humana basada en evidencia concreta de la actividad delictiva. Es decir, que se pueda probar con datos demostrables que la persona en cuestión está implicada en el delito que se discute.

También, está terminantemente prohibido el uso de sistemas para crear bases de datos de reconocimiento facial mediante la agrupación de imágenes no selectiva, y la inferencia de emociones en los entornos mencionados menos por razones de seguridad o médicas.

Los sistemas de identificación biométrica a distancia en tiempo real se utilizarán para las excepciones del artículo 5.1 d) teniendo siempre en cuenta:

- La gravedad y la necesidad urgente de aplicar esta medida, sin la cual se generaría un agravio de mayor magnitud.
- La afectación de los derechos de los individuos implicados. Debe realizarse una evaluación de impacto de derechos fundamentales.
- La regulación nacional al respecto, que podrá imponer más restricciones o incluso desautorizar su uso. Cuando se adopten estas normas nacionales, deben ser notificadas a la Comisión.
- Las reglas procedimentales para su uso que incluyen la expedición de informes, la obtención de una autorización judicial o administrativa, y las reglas especiales de su registro en bases de datos correspondientes.
- El deber de notificar el uso en caso de fines policiales a la autoridad de supervisión en el mercado y la encargada de la protección de datos en el país en cuestión.

Es posible que el requisito de autorización administrativa o judicial se ponga en funcionamiento el sistema sin haber sido concedida. De todos modos, tendrá que solicitarse y en el caso de que se deniegue cesará el uso. La decisión de la autoridad competente sobre la concesión de la misma estará en todo caso basada en pruebas y fundamentos suficientemente justificados, y será vinculante.

La Comisión se compromete a expedir informes anuales sobre los sistemas biométricos discutidos en el artículo 5, basados en los informes formulados cada año por las autoridades nacionales. (Consejo de la Unión Europea, 2024)

b. **Sistemas de alto riesgo**

En el Título II del Reglamento sobre IA se analizan los sistemas de IA de alto riesgo. Primero se clasifican los diferentes casos que pueden incluirse bajo esta categoría. Más tarde se establecen una serie de requisitos para la gestión de riesgos y relacionados con la gobernanza de datos, la transparencia, la precisión y los procedimientos técnicos y administrativos que han de seguirse. También se incluyen en este título las obligaciones de los suministradores de estos sistemas para su comercialización y de las autoridades de notificación en cuestión con respecto a los organismos notificados. Todo esto se recoge en los artículos 6-34 de la nueva ley de IA.

Cuando se desarrolla un sistema de IA de "alto riesgo", se debe realizar una evaluación de conformidad y de cumplimiento de condiciones, más tarde se debe registrar el sistema en una base de datos de la UE y por último se establece una declaración de conformidad para su comercialización. En el caso en que se modifique sustancialmente el sistema deberán volver a realizarse la evaluación de conformidad y los siguientes pasos. (Lacort, 2024)

En esta categoría se incluyen todos aquellos sistemas que se tengan fines de seguridad y se incluyan en el Anexo II de la ley, como por ejemplo lo relacionado con las embarcaciones de recreo o de equipos radioeléctricos o sanitarios. También se incluyen los recogidos en el Anexo III como los usos de sistemas de identificación biométrica que no queden prohibidos, los de seguridad en infraestructuras, de educación, de empleo, de uso por las fuerzas de seguridad, los que tengan objetivos de asilo y control de fronteras, de fines para la administración de justicia y de acceso a servicios esenciales.

Los casos incluidos en el Anexo III no son siempre de alto riesgo. Existe una exención para todos aquellos sistemas de cuyo uso no se deriva un daño significativo para los derechos fundamentales, incluido el derecho a tomar decisiones no influenciadas.

- La limitación del propósito del sistema de IA que tiene un objetivo concreto.
- La mejora del cumplimiento de un objetivo ya satisfecho por otros métodos.
- El objetivo de los sistemas utilizados para identificar la forma en que individuos toman decisiones no puede incidir en estas decisiones ni reemplazarlas, a menos sin una revisión posterior por un humano.
- El fin del sistema es cualquier actividad realizada con motivos preparatorios antes de una evaluación determinada con el objetivo por ejemplo de la preparación de los datos o el análisis preliminar de la información

Si el programa de IA se utiliza para la creación de perfiles siempre se considerará como de alto riesgo.

Los proveedores de los sistemas son los encargados de probar que su producto en concreto cumple con todas las condiciones establecidas en la ley (concretamente en el Capítulo 2 del Título II). También son ellos los que deben probar que su sistema no cumple con las características de un sistema de alto riesgo a la hora de comercializarlo.

En cuanto a los requisitos de aplicación de estos sistemas, se basan en otra gestión de riesgos enunciada en el artículo 9. Tiene diferentes etapas: la localización de los riesgos que el sistema podría generar para las personas y sus derechos, el análisis de estos riesgos que puedan surgir si el sistema se aplica al fin previsto, el de otros riesgos adicionales que puedan generarse, y la implementación de medidas destinadas a mitigar estos riesgos.

Para la implementación de las medidas de mitigación del riesgo, se fijan una serie de garantías que deben cumplirse como la efectiva destrucción o limitación del riesgo localizado, siempre que sea posible técnicamente, el establecimiento de formas de control que no puedan desaparecer y la aportación de la información necesaria establecida en el artículo 13. (Consejo de la Unión Europea, 2024)

Más allá de este procedimiento de mitigación y gestión de riesgos generados por sistemas de IA de alto riesgo, se establecen en el Reglamento requisitos para la gobernanza de datos, la documentación necesaria, el mantenimiento en los registros, la supervisión humana y la exactitud y ciberseguridad.

La mayor parte de las obligaciones establecidas en el Reglamento son para los desarrolladores europeos de sistemas de IA de alto riesgo, que pretendan poner en circulación en el mercado un producto o sistema de esta índole, ya sea con sede dentro o fuera de la Unión. También se deben aplicar en aquellos casos en los que los sistemas se utilicen dentro de la UE, aunque el proveedor no tenga origen europeo.

En cuanto a los implantadores de estos sistemas, que no los que los desarrollan, se les exigirá también el cumplimiento de una serie de requisitos. Son los denominados "usuarios" que no se refieren al consumidor final de un producto que base su funcionamiento en IA, sino en aquellas personas que lo comercializan o implementan a nivel profesional. Incluye a aquellos de la UE y de países ajenos, cuando el sistema se utiliza dentro de la Unión. (Unión Europea, 2024)

En todo caso, la Comisión tiene la autoridad para hacer los cambios que considere en los requisitos establecidos para la regulación de la IA.

c. **Modelos de IA de propósito general**

Los modelos de IA de propósito general conocidos como GPAI son aquellos que son capaces de realizar una gran cantidad de tareas distintas independientemente de cómo se comercialicen y que pueden formar parte de numerosos sistemas distintos. Es decir que no sólo sirven para un uso en sí mismos, sino que se pueden integrar en otros sistemas para su funcionamiento. Un modelo no es lo mismo que un sistema, es una pieza que lo conforma. Un sistema GPAI puede estar basado en un modelo de esta naturaleza de propósito general o formar parte de otros

Pueden considerarse también o formar parte de sistemas de alto riesgo y sus proveedores deben cumplir una serie obligaciones como: (1) la redacción todos los documentos técnicos, que abarcan el procedimiento de preparación y evaluación y los resultados del análisis, (2) la elaboración de datos y documentos para entregar a futuros proveedores de sistemas que vayan a incluir estos modelos y sean esenciales para su comprensión y familiarización con él, (3) fijar un código de adecuación a la Directiva sobre derechos de

autor y (4) Elaborar y publicar una síntesis detallada sobre el material empleado en la capacitación del modelo. (Unión Europea, 2024)

En el artículo 52 bis se definen los modelos de propósito general con riesgo sistémico, estableciendo una serie de condiciones. Se dice que se clasificarán como modelo con riesgo sistémico si:

"(a) tiene una gran capacidad de impacto evaluada sobre la base de herramientas técnicas y metodologías adecuadas, incluidos indicadores y puntos de referencia;

(b) basándose en una decisión de la Comisión, de oficio o tras una alerta cualificada de la comisión técnica científica, de que un modelo de IA de propósito general tiene capacidades o repercusiones equivalentes a las de la letra a)." (Consejo de la Unión Europea, 2024)

Realmente el criterio definidor de un modelo de propósito general con riesgo sistémico es la cantidad de operaciones en coma flotante que se necesitan para su formación, así se evalúa el impacto que tienen. Si para la creación del modelo y su entrenamiento utiliza una cantidad de 10 elevado a 25 FLOPS (operaciones), entonces se considera que son de riesgo sistémico. Los proveedores tienen el deber de notificarlo a la Comisión, o de probar que, aunque cumplan con estas condiciones, no generan este riesgo.

Las consecuencias principales de la clasificación de este tipo de modelos son un mayor número de obligaciones para los proveedores, derivadas del mayor riesgo que supone su comercialización. Estas implican la realización de evaluaciones y pruebas que intenten remitir el riesgo y hacer un seguimiento de los incidentes y reportarlos a la Oficina de IA.

La forma que tienen los modelos de demostrar que no generan riesgos adicionales y que cumplen con todo lo exigido es la adecuación a una serie de Códigos de Conducta establecidos. Recogidos en el artículo 69 de la ley, son fomentados por la Oficina de la IA y por los Estados Miembros. Algunas de las conductas recogidas son el análisis del impacto de la IA sobre personas vulnerables, o la facilitación de un diseño y lenguaje inclusivo y comprensible para los usuarios de estos sistemas, la preocupación por el impacto ambiental, la atención a las normas internacionales. (Consejo de la Unión Europea, 2024)

La IA generativa podría calificarse como modelo de propósito general desde una perspectiva material, y de acuerdo con la definición explicada, pero si nos concentramos en la división del riesgo según su uso, sería más del tipo de riesgo limitado o mínimo., y deberá atenerse a unas normas de transparencia que se explicarán a continuación.

d. **Transparencia para todos los usos**

Los requisitos de transparencia para los sistemas de IA, se encuentran de forma general recogidos en el artículo 52 del IA Act.

Los que desarrollen sistemas de riesgo mínimo cuyo fin es establecer una interactuación directa con el usuario deben adherirse a estas obligaciones de transparencia para que los usuarios sean conscientes de que están relacionándose con un sistema informático. Existen algunas excepciones relacionadas con la seguridad y la protección de derechos fundamentales.

Para los sistemas generativos de IA o que manipulen contenido multimedia, aquellos que los desplieguen deberán revelar si el contenido en cuestión ha sido creado efectivamente de forma artificial, con excepciones de seguridad, creativas o artísticas y publicitarias cuando afectan a un interés general. La etiquetación del contenido como una creación de IA es primordial.

Toda la información descrita anteriormente deberá transmitirse de forma comprensible e inequívoca en la primera etapa del uso del sistema.

Estas reglas se aplicarán sin perjuicio de todas las demás recogidas en la ley de IA y de los códigos o conductas que promueva la Oficina de la IA y la Comisión.

Un ejemplo de IA generativa que debe cumplir estas obligaciones son los Chat Bots o Chat GPT. Este caso concreto debe cumplir con la regulación relativa a los derechos de autor y cumplir con requisitos como establecer un diseño que evite la creación de información falsa o contenido ilegal, y expedir las listas de datos que se utilicen para el aprendizaje y entrenamiento del sistema cubiertos por los derechos de autor.

De todas formas, cada vez salen modelos de Chat GPT más avanzados, como es GPT 4, por lo que debe realizarse una evaluación del impacto del mismo y quizá considerarse como un modelo de propósito general con riesgo sistémico.

En el caso de los sistemas de alto riesgo, deben aplicarse una serie de obligaciones de transparencia más severas. Se recogen en el artículo 13 de la ley. Los sistemas de IA de alto riesgo tienen que ser transparentes para que los usuarios comprendan su funcionamiento y lo utilicen de manera adecuada y conforme a la ley. Además, los proveedores deben siempre adjuntar unas instrucciones completas y claras en formato digital o accesible para los usuarios y deben contener una serie de datos imprescindible como el fin y las características del sistema y el nombre de los responsables del sistema, entre otras.

4.2 Análisis de impacto de los derechos fundamentales.

La nueva ley de IA tiene como objetivo el desarrollo y regulación de modelos y sistemas a la vez que la protección de los derechos fundamentales de aquellos que vayan a utilizarlos. Por ende, todos los implementadores y suministradores de los sistemas de alto

riesgo (cuyo uso tienen una mayor incidencia en los derechos de los usuarios) deben asegurarse de realizar una evaluación del impacto de su uso en los derechos fundamentales.

Esta evaluación debe realizarse en todo caso antes de poner en circulación en el mercado los sistemas y deben complementarse con salvaguardas concretas para cerciorarse de que es efectivo el régimen de responsabilidad.

Para lograr cumplir con estos objetivos, es obligatorio que los sistemas proporcionen los datos e información necesaria que haga posible esta evaluación. Sólo así todas las autoridades externas encargadas de asegurar y supervisar el respeto de los derechos humanos podrán realizar una vigilancia efectiva.

En el IA Act, se regula la evaluación del impacto en el artículo 29 bis en el que se obliga a todos aquellos implementadores de sistemas de IA en los que se requiera (de alto riesgo con algunas excepciones), que realicen un análisis de los mismos incluyendo datos como:

- Los procedimientos en los que se utilizará el sistema para un fin concreto, la clasificación de usuarios a cuyo uso va dirigido.
- El tiempo y frecuencia con el que se prevé utilizarlos.
- El riesgo del daño que pudiera producirse a los usuarios.
- Una descripción de las disposiciones de supervisión adoptadas para mitigar la afección a los derechos recogidas en las instrucciones y todas las sanciones y medidas adoptables en el caso en que se hagan realidad estos riesgos, como mecanismos de denuncia.

Estos requisitos son susceptibles de modificaciones o actualizaciones si así se requiere, y si la evaluación ya se ha realizado siguiendo requisitos de la regulación de protección de datos se realizarán de forma conjunta. (Consejo de la Unión Europea, 2024)

Después de haber realizado este examen de impacto debe emitirse notificación a la autoridad correspondiente de vigilancia de mercado.

5. EN ESPECIAL: ESTUDIO DE LOS DATOS BIOMÉTRICOS Y SINTÉTICOS

A medida que avanza la tecnología, se extiende la desconfianza y la incertidumbre entre los usuarios, que cada vez confían menos en una simple contraseña para proteger su privacidad. Además, es posible que las contraseñas se olviden y sea necesario cambiarlas. Por ello, surgen los sistemas denominados de "identificación biométrica", que aplican la tecnología para reconocer a una persona basándose en sus rasgos físicos, psicológicos o de comportamiento únicos, como pueden ser las huellas dactilares o la forma de andar.

Estos datos también sirven para otros usos, como por ejemplo el control de accesos.

El artículo 9.1 del RGPD clasifica a los datos de identificación biométrica que se utilizan para la identificación de un individuo como prohibidos, siempre que no se cumplan las condiciones del apartado de 2 del mismo artículo.

Habiendo realizado un juicio de proporcionalidad y de necesidad para el uso de estos datos biométricos, se examinan las excepciones por las que es justificable su utilización del 9.2. Se incluyen motivos como la persecución de un interés público esencial o la protección de intereses vitales del titular, pero quizá el más relevante sea la aportación del consentimiento previo del interesado para el tratamiento de sus datos, siempre que éste no quede desvirtuado por el derecho de la Unión. (RGPD, 2016).

La Agencia Española de Protección de Datos ha publicado una guía sobre el tratamiento de datos biométricos para el control de accesos que es muy restrictiva. Según la guía, en general no cabe el uso de datos biométricos para control de accesos dado que, si existe una alternativa viable al uso de datos biométricos, entonces el juicio de necesidad no se supera, y por tanto el tratamiento no es lícito. Si en cambio no existe una alternativa viable, entonces el consentimiento no es lícito y no sirve para levantar la prohibición del 9.2. Esta guía tan restrictiva ha sido criticada por la doctrina.

Pero los datos biométricos no sólo son relevantes a efectos de protección de datos. El considerando 7 a) del IA Act distingue entre los datos biométricos usados para verificación (incluida la autenticación) con base en el consentimiento del interesado que no serían objeto del IA Act sino del RGPD, y por otro lado la identificación mediante estos datos de personas que no han prestado consentimiento alguno, cuestión que no sólo afecta al RGPD, sino también al AI Act.

Es importante realizar una observación presente en la nueva ley de IA (IA Act), que distingue varios conceptos:

- La identificación a través de datos biométricos, que es meramente esta identificación de la persona por sus características
- La verificación biométrica. Esta última implica corroborar que, efectivamente, estos datos pertenecen al afectado, para proporcionarle acceso a un servicio o lugar, por ejemplo, para entrar en una oficina gracias a una huella dactilar o para desbloquear un smartphone mediante el reconocimiento facial. (Grupo Ático 34, 2023)
- La categorización biométrica es ir un paso más allá. Consiste en clasificar a los individuos en diferentes grupos, basándose en un criterio que se guía por los datos obtenidos.
- Los sistemas de identificación biométrica remota no necesitan de la participación del titular de los datos, sino que los recolectan y comparan con una base de datos existente para, en un contexto más amplio, lograr determinar la identidad del individuo. Un ejemplo fácil de esto es el reconocimiento facial utilizado en aeropuertos. Las cámaras capturan el rostro del sujeto y lo comparan con una base de datos de imágenes biométricas de personas que podrían presentar una amenaza o que se les tiene prohibido volar. (Consejo de la Unión Europea, 2024)

En el artículo 5 de esta ley se incluyen las "prácticas prohibidas" para sistemas de IA de identificación biométrica.

La categorización por datos biométricos para deducir algunos aspectos mencionados en la ley como la raza o la afiliación política del individuo no está permitida, para evitar resultados discriminatorios, salvo que se hayan obtenido los datos por una vía legal. La categorización a través de datos biométricos que no quede por tanto prohibida por este reglamento se considerará como "de alto riesgo".

En esta misma línea, se prohíben los usos que impliquen la atribución de un individuo a un grupo por sus actitudes o rasgos deducidos o reales, en el caso en que de esta agrupación resulte un tratamiento discriminatorio.

En cuanto a los sistemas de identificación remota que hemos mencionado, la regla general es que en lugares de acceso público y en tiempo real no se permita utilizarlos, pero hay algunas excepciones que justifican estos métodos. En una lucha por la privacidad de los sujetos afectados debemos tener en cuenta aspectos de mucha gravedad que obligan a tomar estas medidas excepcionales. Se recogen en el artículo 5.1 d) del IA Act y son: *(i) La búsqueda específica de* ***víctimas de secuestro, tráfico***

de personas y explotación sexual *de seres humanos, así como la búsqueda de personas desaparecidas; (ii)* ***La prevención de una amenaza específica, sustancial e inminente para la vida*** *o la seguridad física de personas naturales o una amenaza genuina y presente o una amenaza previsible de un ataque terrorista; (iii)* ***La localización o identificación de una persona sospechosa de haber cometido un delito penal****, con fines de conducción de una investigación penal, enjuiciamiento o ejecución de una pena penal por delitos, mencionados en el Anexo IIa y punibles en el Estado miembro correspondiente con una pena de prisión o una orden de detención por un período máximo de* ***al menos cuatro años****. (*Consejo de la Unión Europea, 2024)

Las excepciones del uso de sistemas de identificación remota recién mencionadas hacen plantearse hasta qué punto la protección de datos personales, que es un derecho fundamental, puede ser ignorada. Debido a la colisión de derechos como el derecho a la vida y el de protección de datos, aunque puede resultar evidente, debemos realizar un juicio de ponderación que evalúe la necesidad de aplicación de un derecho u otro y la proporcionalidad; o una ponderación entre ambos derechos.

La ley concreta que es primordial tener en cuenta la gravedad y la proporción de los daños que vayan a causarse y la consecuencia para los derechos fundamentales de todos aquellos que estén involucrados.

Reflexionamos sobre estas situaciones con un ejemplo: La utilización de cámaras de vigilancia para encontrar a una niña recién desaparecida, cuya investigación muestra indicios de involucrar el crimen de trata de blancas y explotación sexual. Existe una amenaza a la integridad física de las personas, y poniendo los dos derechos en una balanza, está claro que es necesario proteger la integridad física de la niña. Si realizáramos la prueba de proporcionalidad pertinente, nos daríamos cuenta de que:

- La violación del derecho de protección de datos tiene **un fin legítimo**: proteger a una niña cuya vida o cuyo cuerpo está siendo amenazado.
- La medida aplicada de utilizar este tipo de sistemas de reconocimiento es **idónea** o adecuada ya que la instalación de cámaras es una forma eficaz de lograr el fin para el que se establece. De esta forma, existe la posibilidad de que se capture en vídeo a la niña desaparecida.
- Analizando si es **necesaria** la adopción de esta medida, observamos que es la menos restrictiva que puede utilizarse. La que resulta menos gravosa es respecto del derecho fundamental de la protección de datos.

- Poniendo ambos derechos en una balanza y analizando **la proporcionalidad** de la medida aplicada, concluimos que existe un equilibrio entre los beneficios que obtenemos al aplicar esta medida (prevenir un riesgo que podría afectar a la integridad física de alguien) y el daño que se ocasiona a la privacidad de los individuos que se sometan a este sistema. (Baquerizo, 2009)

Además, existen numerosos procedimientos formales y salvaguardias que protegen la privacidad de los sujetos. En primer lugar, y teniendo en cuenta lo establecido en la Directiva 2016/680, es necesario obtener una autorización judicial para el uso de sistemas de identificación remota posterior (no de tiempo real). Los datos recogidos no se divulgarán en ningún caso al público, quedando únicamente archivados por la autoridad competente. Aquellos que tengan acceso a estos sistemas deberán, en todo caso, presentar una serie de informes que justifiquen la utilización de los mismos. En el IA Act se aclara que, siguiendo estas pautas generales, los Estados podrán aplicar legislación más estricta si así lo desean.

De todos modos, es evidente que todas aquellas excepciones a la prohibición del uso de este tipo de sistemas se clasificarán como sistemas de "alto riesgo".

También se clasificarán como de alto riesgo los usos de sistemas para el reconocimiento de emociones que no queden prohibidos por el nuevo reglamento (aquellos implementados motivos médicos y de seguridad). En los ámbitos de trabajo y de educación restantes este tipo de usos queda prohibido por el artículo 5. De la misma forma, si el scraping o recolección de datos sin autorización para la creación de bases de datos es también ilegal.

En cuanto a los sistemas de mera verificación, que implican el mero acceso a un servicio por la comprobación de la identidad de una persona, como los de control de acceso, no se clasifican como de alto riesgo al ser utilizados únicamente para un fin práctico y específico y contando con el consentimiento del titular de los datos.

Los datos sintéticos son aquellos generados por la inteligencia artificial, y recogidos en el artículo 10 del nuevo IA Act, que son difíciles de distinguir de los reales. El gran número de datos de disponibles de estas características hace que sea cada vez más difícil fiarse de lo proporcionado por la IA, ya que se pone en duda el hecho de que hayan sido manipulados, cambiados o extorsionados y que tengan como resultado la desinformación o el engaño del que los recibe.

Es por esto por lo que, urge el desarrollo de nuevos métodos y procedimientos para buscar la procedencia de los datos. La detección de estos datos es un trabajo farragoso. Es lícito, por tanto, solicitar a los suministradores de estos sistemas que integren mecanismos que hagan posible su identificación en los propios sistemas, que

la máquina en cuestión sea capaz de discernir los datos reales de los creados de forma virtual, a través de la IA.

En el artículo 52 de la nueva ley se especifican las obligaciones de los proveedores de IA que creen datos sintéticos sean del tipo que sean (de texto, visuales o auditivos). Algunas de los requisitos para ellos con respecto de los datos sintéticos son:

- Que, como ya especificamos antes, sea detectable su procedencia y generación por la propia máquina y se generen con un formato legible por el sistema.
- Que el output generado sea lo más confiable y exacto posible. Se tienen en cuenta algunos obstáculos o dificultades técnicas que pueden experimentar estos sistemas en este sentido, incluyendo los elevados costes de estos programas y la complejidad del contenido generado.

El último requisito para los proveedores no se suplementará en todos los casos. En aquellos sistemas cuya utilización esté aprobada legalmente para la investigación, proceso y resolución de un delito no es necesario realizar estas comprobaciones. Tampoco en el caso en que los sistemas hayan realizado cambios en los datos originalmente proporcionados, pero que no sean significativos ni alteren el sentido de estos. (Consejo de la Unión Europea, 2024).

6. RÉGIMEN SANCIONADOR Y RESPONSABILIDAD E INTELIGENCIA ARTIFICIAL

6.1 Sanciones derivadas de los daños por IA en el RGPD y en el IA Act.

Como toda infracción legal tiene una consecuencia, es imperativo analizar la responsabilidad que se deriva de un uso intrusivo de los sistemas de IA o que afecta a derechos fundamentales, como el de la protección de datos.

Con respecto al régimen sancionador recogido en el Reglamento General de Protección de Datos y en la nueva ley de inteligencia artificial, se aplicarán las siguientes multas en diferentes situaciones:

- En el Artículo 83 del RGPD, se establecen las condiciones generales para la imposición de multas administrativas, que se aplican ad casum y deben ser proporcionadas y eficaces. Se tendrán en cuenta los factores enumerados en el apartado 2 del artículo como la naturaleza o duración de la infracción, la negligencia o la adhesión a códigos de conducta.
  En los apartados 4, 5 y 6se establecen las cuantías que deberán ser soportadas por el infractor:
  - La multa será de 10 millones de euros como máximo o en una empresa del 2% del volumen de negocio de la misma si se ha producido una infracción relativa al incumplimiento de las obligaciones recogidas en la ley,
  - La cuantía será de hasta 20 millones o de un 4% del volumen de negocios de una empresa si se infringen principios o derechos enunciados en la ley, incluyendo los casos de incumplimiento de las resoluciones de la autoridad de control.

Para los casos a los que no se les apliquen multas administrativas, se deja a elección libre de los Estados Miembros la imposición de sanciones proporcionadas a la infracción, debiendo comunicarlas a la Comisión al formularlas.

- En el IA Act se recogen las sanciones en el título X, en concreto en los artículos 71 y 72. En el artículo 71 se establece la imposición libre de los Estados Miembros de sanciones y medidas coercitivas necesarias que también deben notificarse posteriormente a la comisión. También se mencionan en su apartado 6 las condiciones y circunstancias que hay que tener en cuenta para la aplicación de la sanción dentro de los siguientes límites:
  - Se establece una multa de hasta 35 millones de euros o del 7% del volumen total de negocios si es una empresa para las prácticas de uso prohibidas.

- Para todas las prácticas que no sean prohibidas la multa será de hasta 15 millones de euros o de hasta el 3% del volumen de negocios anual.
- En el caso de falta de información o de proporción de datos engañosos o falsos, se aplicarán multas administrativas de hasta 7.5 millones de euros o del 1% del volumen de negocios de una empresa.

En los artículos 72 y 72 bis se establece el régimen de multas en casos especiales como las aplicables a las instituciones de la unión o a los proveedores de modelos de IA de propósito general.

6.2 Proyectos de directiva de responsabilidad por daños causados por IA (primer borrador del PE y el actual de la comisión) y de modificación de la responsabilidad por productos defectuosos.

La UE está elaborando una Directiva para abordar la responsabilidad extracontractual en materia de IA. El gran problema que se plantea es la complicación a la hora de establecer un culpable, de identificar quién o qué ha sido el que ha originado el daño en cuestión.

Tanto el Parlamento como la Comisión han publicado propuestas para la elaboración de esta directiva.

En primer lugar, la propuesta del Parlamento Europeo sobre responsabilidad civil en 2020 en materia de inteligencia artificial plantea dos sistemas de responsabilidad: (Torre de Silva, 2024)

- Para los sistemas de alto riesgo:
  El establecimiento de una responsabilidad objetiva para todos los sistemas de alto riesgo además la imposición de un seguro de responsabilidad civil incluidos en el artículo 4 de la ley se realizará tras identificar a estos sistemas de cuyo uso se deriva un riesgo mayor.
  Además, en el artículo 5 se especifica que deberán disminuirse las indemnizaciones y sin embargo prolongarse el plazo establecido para la prescripción (Son 10 años en el caso de daños materiales y 30 si son personales). Se especifica además que los operadores no pueden evitar esta responsabilidad justificando que fueron diligentes o que el daño causado no fue directamente originado por su sistema. Únicamente podrán eludir esta responsabilidad, en los casos de fuerza mayor. (Parlamento Europeo, 2020)
- Para todos los demás sistemas que no sean de riesgo alto:
    a. La responsabilidad del operador se basa en la culpa, en una responsabilidad subjetiva, especificada en el artículo 8. En estos casos es el operador quien debe probar que no fue culpable, alegando una de

las causas expuestas en la ley. En caso de que el daño sea realizado por un tercero, y este no pueda abonar el importe, el operador quedará obligado subsidiariamente a pagar la indemnización correspondiente.
Es importante aclarar qué entendemos por operador. En las definiciones de esta propuesta del Parlamento se aclara que son todos aquellos operadores finales que tienen un "*grado de control sobre un riesgo asociado a la operación y funcionamiento del sistema de IA"* y todos los operadores iniciales que promueven y proporcionan el servicio aportando tecnología e información claves, y que por tanto también tienen una afección con respecto al riesgo.

b. Para los co-operadores, es decir, cuando hay más de un operador del sistema de IA, la responsabilidad es un poco distinta. Se establece en el artículo 11 de la ley, y es solidaria.

Más tarde, en 2022 se publicó la propuesta de la Comisión, que es la vigente actualmente con una serie de cambios. También realiza una división entre sistemas de alto riesgo y los demás. Hace más hincapié en la importancia de la determinación de la culpa, y se basa en demandas civiles presentadas por los que sufren el daño.

- Para los sistemas de alto riesgo, en el artículo 3 se determina la información y las pruebas que debe presentar el demandante para la determinación de la culpa y del nexo causal. Los tribunales pueden obligar al demandante a revelar estas pruebas, o a que demuestre que ha hecho todo lo posible para la obtención de las mismas. En el caso de que no se entregue la información, se presume culpable.
  De todas formas, se producirá una presunción de culpabilidad y nexo causal entre las acciones del demandado y los daños producidos por el sistema de IA si se cumplen las condiciones del artículo 4 de la propuesta. Estas están relacionadas con la falta de diligencia del demandado, la suficiente probabilidad de que los resultados de IA perjudiciales estén relacionados con la culpa y con que la información directa de salida del sistema sea la causante del perjuicio.
- Para todos los demás sistemas, se presume que hay un nexo causal y por tanto culpa del demandado, únicamente si el Tribunal en cuestión considera que la prueba es "extremadamente difícil" (por ejemplo, el daño causado por un error del piloto automático de un avión) También en casos en los que no haya accesibilidad a un número suficiente de pruebas y cuando el demandado no quiera explicar el funcionamiento del sistema o lo haya utilizado para actividades de fuera del ámbito profesional. (Pina, 2022)

Todas las medidas expuestas se utilizan para proteger y facilitar la defensión del perjudicado, ya que en casos de daños producidos por sistemas de esta índole es a veces complicado probar quién ha cometido el acto.

La propuesta de la Comisión debe ser aprobada por los demás órganos de la UE y cuando se publique y entre en vigor será traspuesta a todos los estados miembros.

Además de esta ley de responsabilidad extracontractual, es necesario mencionar que la Comisión Europea ha presentado una propuesta de Directiva sobre responsabilidad por productos defectuosos para abordar los desafíos surgidos en la era digital.

Esta propuesta busca actualizar el régimen de responsabilidad por productos defectuosos de la UE, considerando la creciente complejidad de los productos y las características únicas de la economía circular y las cadenas de valor globales.

Amplía el ámbito de aplicación para incluir productos como el software, incluyendo los sistemas de IA, y los archivos de fabricación digital, así como los servicios digitales necesarios para su funcionamiento. La propuesta establece disposiciones específicas para los sistemas de IA, haciéndoles responsables durante todo su ciclo de vida, incluso en actualizaciones de software y en casos de discriminación por IA en procesos de contratación. Se dirige a quiénes pueden ser responsables de los productos defectuosos, incluyendo fabricantes, importadores, prestadores de servicios y distribuidores. Además, amplía la definición de daño para incluir pérdidas materiales y alteración de datos. Esta propuesta busca reforzar los requisitos de seguridad de los productos en el mercado interior de la UE, protegiendo así a los consumidores. Aunque la Directiva está pendiente de aprobación, refleja el compromiso de la UE en abordar los riesgos asociados con la IA mientras fomenta la innovación tecnológica. (Ramírez, 2024).

6.3 Tutela judicial de los derechos fundamentales

Otra vía para imponer el cumplimento de la ley, en cuanto a la protección de los derechos en el ámbito de la IA es la tutela judicial de los derechos fundamentales.

Además de la posibilidad de imponer sanciones administrativas a los causantes del perjuicio y de hacerles responsables de los daños, que tendrán que compensar, se puede optar por la opción tradicional de acudir a la vía judicial para la defensa de los derechos.

Como hemos podido observar, los derechos que pueden verse afectados por el uso de sistemas de IA son el derecho de protección de datos recogido en el artículo 8 de CDFUE, el de respeto a la vida privada y familiar del artículo 7 de CDFUE, el respeto al principio de no discriminación (por ejemplo por la categorización de datos con sesgos de raza o religión) y por tanto al artículo 14 de la CE, e incluso al artículo

17 de la CE con relación con la libertad y la seguridad, al requerirse un consentimiento informado a los usuarios que apostan sus datos personales para el funcionamiento de estos sistemas.

El procedimiento se basaría en la interposición de una demanda, y si se agotan los recursos ordinarios y persisten las alegaciones de violación de derechos fundamentales, la parte afectada podría llegar a presentar un recurso de amparo ante el TC o una instancia similar. Este recurso busca proteger los derechos fundamentales consagrados en la Constitución del país.

En el ámbito internacional, se pueden llegar a presentar demandas ante el Tribunal Europeo de Derechos Humanos o la Corte Internacional de Justicia tras haber agotado la vía judicial previa.

Si el recurso de amparo tiene éxito, el tribunal constitucional puede declarar nula la decisión impugnada y restablecer los derechos vulnerados. Esto puede implicar la revisión de todo el proceso judicial y tener repercusiones en las partes involucradas, así como en la interpretación y aplicación de la ley.

7. CONCLUSIONES

La inteligencia artificial (IA) ha emergido como una fuerza transformadora en diversos ámbitos de la sociedad, prometiendo avances significativos en la eficiencia, la innovación y la calidad de vida. Sin embargo, este rápido progreso también plantea una serie de desafíos y riesgos, especialmente en lo que respecta a la protección de los derechos fundamentales.

A medida que la IA se integra cada vez más en nuestras vidas, desde sistemas de recomendación hasta sistemas de toma de decisiones en sectores como la salud y la justicia, es crucial examinar de cerca cómo estos avances tecnológicos pueden afectar nuestros derechos.

Tras realizarse un análisis sobre la evolución de la IA y definir los conceptos y principales riesgos que pueden derivarse de su uso, como la afectación de derechos de protección de datos, de la vida privada y familiar, de igualdad y no discriminación o de libertad o seguridad, se realiza en esta tesis un análisis sobre la respuesta internacional de algunos países ante tal amenaza.

Habiendo analizado la "Exeutive Order" de EEUU o la "Declaración de Bletchey" del Reino Unido, y comparándolas con la legislación nueva sobre protección de derechos fundamentales en el ámbito de la IA en Europa (IA Act), he llegado a la conclusión de que la regulación europea es quizá la que estará llamada a convertirse en un canon global o modelo de regulación predominante en el mundo al igual que sucedió con el RGPD. Esto es, ya que los límites establecidos en el IA Act se deberán aplicar a todo aquel que quiera operar con estos sistemas en Europa, y debido a que es hasta ahora la más exigente y por tanto si un operador cumple con ella, debería ser compatible con todas las demás.

La respuesta Comunitaria a los desafíos que presenta la IA se basa en la aplicación de normativa ya vigente para la protección de estos derechos y en el lanzamiento de tres nuevos proyectos que van a resultar claves para la protección de los titulares de los datos. Podemos encontrar muchas leyes que ya abordaban la protección de estos derechos como el RGPD en materia de protección de datos, la ley de responsabilidad por daños causados por productos defectuosos de 1985 o la Ley de Gobernanza de Datos.

En cuanto a los nuevos proyectos, los más relevantes son: el proyecto de directiva sobre responsabilidad civil derivada del uso de sistemas de IA y el proyecto de modificación de directiva sobre responsabilidad por daños provocados a raíz de productos defectuosos y el IA Act.

El IA Act es, como hemos visto, el primer proyecto detallado de legislación de IA en el mundo y fue aprobada el pasado 13 de marzo de 2024 por el Parlamento Europeo. Es un resultado de un proceso muy deliberado y de numerosas conversaciones entre las diferentes instituciones de la UE y se basa en una gestión de riesgos de los sistemas de IA basado en su uso. Conforma un conjunto de reglas armonizadas por la que se van a regir todos los Estados Miembros en materia de IA, y los que interaccionen con ellos.

Adentrándonos en el primer pilar de este ensayo, la protección de datos, nos damos cuenta de que la legislación más importante que se toma como referencia es el RGPD. Remitiéndonos al IA Act, se especifica que las condiciones establecidas en el RGPD deben ser cumplidas en todo caso, por lo se realiza un estudio en profundidad de las condiciones y requisitos establecidos en esta ley.

Refiriéndonos siempre a datos personales, se especifica en el Reglamento la necesidad de que exista un consentimiento informado y granulado de la aportación de estos datos, que la información que proporcionen los titulares de los mismos tenga derecho a ser rectificada, y que la inferencia a través de ella para crear perfiles sea prudente. Vemos que sin el consentimiento no se puede entender el derecho a la protección de datos.

Se realiza un estudio detallado de los principios de protección de datos relacionándolos con la IA. Estos son la transparencia (importante intentar clarificar el objetivo del tratamiento de los datos, y que sean accesibles y certeros), la limitación de la finalidad (que los datos aportados cumplan con un fin específico, en la IA la reutilización de datos se puede evaluar analizando aspectos como la proximidad de objetivos o su impacto), la minimización de los datos (deben ser limitados al objetivo que se quiere cumplir, en la IA se exige si afecta a un individuo y no a un grupo), la exactitud (precisión de los datos), la limitación del plazo de conservación de los datos y la confidencialidad e integridad de los datos (que sean imparciales y secretos, es importante en sistemas de IA que almacenan muchos datos que necesitan de prácticas como la encriptación).

Por otro lado, en cuanto a la base legal legitimadora del tratamiento de los datos, se recogen en el artículo 6 del RGPD las condiciones para que sea lícito (incluyen la aportación del consentimiento o el logro de un interés legítimo). Estas bases jurídicas tienen un efecto irretroactivo en el caso en que dejen de existir.

Una vez cubierta la protección de datos personales por remisión al RGPD se analiza la nueva ley de gestión de riesgos para la afectación de los demás derechos fundamentales que pueden quedar influidos por los usos de la IA. Así, se realiza en este ensayo un estudio del IA Act que divide a los usos los sistemas de IA siguiendo

un esquema piramidal en: prácticas prohibidas, sistemas cuyo uso genera un alto riesgo, aquellos de riesgo limitado y cero, y los modelos de IA de propósito general

Los usos prohibidos se enuncian en el artículo 5 y son una lista de prácticas no aceptadas que tiene como objetivo proteger los derechos fundamentales, incluyen algunas como la categorización de los individuos según sus rasgos o la creación de bases de datos de reconocimiento facial. Los sistemas de alto riesgo son sometidos a una serie de requisitos muy restrictivos y a unas condiciones de adecuación a principios como la transparencia o la precisión de los datos, luego se registran el sistema en una base de datos y requieren de una declaración de conformidad para su comercialización. Se incluyen los casos especificados en los Anexos II y III de la ley, como la creación de perfiles, y se especifican medidas para mitigar los riesgos que generan.

Los modelos de IA de propósito general son por su parte los que tienen la capacidad de realizar muchas tareas diferentes independientemente de cómo se comercialicen y que pueden formar parte de sistemas distintos. También se definen los GPAI con riesgo sistémico que quedan sometidos a un mayor número de obligaciones para los proveedores de los sistemas. La IA generativa podría considerarse de esta categoría si analizamos la definición de GPAI, pero según su uso es más de riesgo limitado.

El requisito de transparencia es común a todas las categorías, pero en diferente proporción. La IA generativa como Chat GPT, debe revelar en todo caso si el contenido ha sido creado de forma artificial o no. Unos requisitos más estrictos se aplican a los sistemas de alto riesgo.

Al tener como objetivo la protección de los derechos fundamentales, se incluye en el IA Act en su artículo 29, un requisito de evaluación del impacto de los mismos.

Me ha parecido importante señalar el caso de los datos biométricos. La identificación biométrica que se utiliza para la localización de un individuo está prohibida menos cuando se cumplen una serie de condiciones. Por ejemplo, los sistemas de identificación remota como de reconocimiento facial en lugares públicos están prohibidos, menos en los casos mencionados como la búsqueda de víctimas de un secuestro. Aunque se permita la utilización de estos sistemas en ciertos casos, existen numerosas salvaguardias legales que protegen la privacidad del sujeto. Esto es por la intrusividad que se deriva del no consentimiento de las personas afectadas. Por otra parte, los proveedores de sistemas que creen datos sintéticos deben dejar claro que la procedencia de los mismos es la IA.

Para finalizar, al haber realizado un seguimiento y examen de las leyes que salvaguardan los derechos fundamentales en relación con el uso de la IA, y los límites que se establecen a su utilización, es imperativo especificar las consecuencias que se

derivan de una infracción de estos derechos. Si del uso de un sistema se deriva una lesión de los mismos, se pueden optar por tres vías para imponer el cumplimiento de la ley: aplicar sanciones administrativas o multas recogidas tanto en el IA Act como en el RGPD, responder por los daños causados o impugnar la lesión por vía judicial.

En cuanto a la responsabilidad, existe un problema para estos sistemas de IA en el nexo causal y existencia o no de culpa, al final, es muy difícil probar la culpabilidad del proveedor de un sistema complejo de IA, por lo que se necesita establecer unas medidas de protección para el sujeto afectado. Es por ello por lo que surgen las dos nuevas directivas mencionadas en materia de responsabilidad por daños causados por la IA y por productos defectuosos. La tercera opción es la vía de la tutela judicial de los derechos fundamentales. Mediante la interposición de una demanda hasta llegar al recurso de amparo si es necesario, se pueden impugnar los derechos ante el TC y otros tribunales internacionales que velan por el cumplimiento de estos derechos fundamentales y de los derechos humanos en general.

Hemos podido observar cómo existe legislación ya vigente aplicable a estos problemas, y a su vez proyectos nuevos que van a ayudar a establecer un marco jurídico completo que sirva como guía para esta tecnología emergente que está cada vez más presente.

En conclusión, y tras haber realizado un estudio exhaustivo sobre el tema, considero completamente necesaria la regulación relacionada con el uso de IA. Cada vez la tecnología tiene más influencia en el mundo actual y si no se establecen una serie de límites, pueden llegar a desvirtuarse la dignidad y los derechos fundamentales de las personas.

8. BIBLIOGRAFÍA

1. Legislación

- Propuesta de Reglamento del Parlamento Europeo y del Consejo 2021/0106 (COD), de 21 de abril de 2021, por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (DOCE COM (2021) 206 final).
- Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (versión refundida).
- Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), Comisión Europea, Bruselas, 28 de septiembre de 2022 (COM (2022) 496 final)
- Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la responsabilidad por productos defectuosos, Comisión Europea, Bruselas, 28 de septiembre de 2022 (COM (2022) 495 final, 2022/0302 (COD)).
- Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión - Análisis del texto final de compromiso con vistas a un acuerdo. (Consejo de la Unión Europea, de 26 de enero de 2024). Documento 5662/24. Interinstitucional File: 2021/0106(COD) No. Cion doc.: 8115/21
- Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). Publicado en: «DOUE» núm. 152, de 3 de junio de 2022, páginas 1 a 44 (44 págs.). Unión Europea. Referencia: DOUE-L-2022-80835.
- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Publicado en: «DOUE» núm. 119, de 4 de mayo de 2016, páginas 1 a 88 (88 págs.). Unión Europea. Referencia: DOUE-L-2016-80807.

- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Artículo 6.
- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Artículo 4.
- 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Artículo 9.
- Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Gobierno de los Estados Unidos. (30 de octubre de 2023).
- Países asistentes a la Cumbre sobre Seguridad de la IA. (1 y 2 de noviembre de 2023). "*Declaración de Bletchley*." Documento de política. Publicado el 1 de noviembre de 2023.

2. <u>Jurisprudencia</u>

- Boucher, P. (2020). STUDY *Panel for the Future of Science and Technology. European Parliamentary Research Service. Scientific Foresight Unit* (STOA). PE 641.547.
- Sentencia del Tribunal del Distrito de la Haya Rb. Den Haag (Países Bajos). núm 18/388, de 5 de febrero C/09/550982/HA ZA (Identificador de jurisprudencia europea: ECLI:NL:RBDHA:2020:865.)

3. <u>Obras doctrinales</u>

- Recio Gayo, M. (2023). LA LEY Inteligencia Artificial (IA): *"¿Qué es y cuáles son los principios para que sea confiable?"*. Derecho Digital e Innovación, Nº 17, julio-septiembre 2023. Editorial LA LEY.
- EY. (2023). "*The Artificial Intelligence (AI) global regulatory landscape: Policy trends and considerations to build confidence in AI*."
- Martínez Rodríguez, L. (2021, 15 de mayo). *"El marco legal de la Inteligencia Artificial: datos y herramientas.*" Ensayo presentado como requisito parcial para obtener el título de Grado en Derecho y en Administración y Dirección de Empresas, Facultad de Derecho, Universidad Autónoma de Madrid.

- Servicio de Investigación del Parlamento Europeo (2023). "*BRIEFING: EU Legislation in Progress.*" Autor: Tambiama Madiega; Research Service. PE 698.792. Disponible en: 1 Artificial intelligence act (europa.eu)
- Parlamento Europeo. Panel para el Futuro de la Ciencia y la Tecnología. (2020, June). *"The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*." Servicio de Investigación del Parlamento Europeo, Unidad de Prospectiva Científica (STOA). Disponible en: (IMPORTANTE COMO IMPACTA LA GDPR EN LA INTELIGENCIA ARTIFICAL.pdf)
- Agencia Europea de Protección de Datos. (2020, febrero). *"Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción."* Disponible en: (adecuacion-rgpd-ia (1).pdf)
- Baquerizo Minuche, J. (2009, junio). *"COLISIÓN de derechos fundamentales y juicio de ponderación."* Disponible en: (1-colision-derechos.pdf (revistajuridicaonline.com))
- Torre de Silva, J. (2024). *"El Reglamento de IA y la European Data Act"* [Diapositivas de PowerPoint]. CMS Albiñana y Suarez de Lezo. Disponible en: (24-03-04 Master EPJ IA (1).pdf)

4. Recursos de internet

- Tableau. (s.f.). "*Tipos de inteligencia artificial*." Recuperado de (https://www.tableau.com/es-mx/data-insights/ai/tipos-de-inteligencia-artificial)
- Noticias Parlamento Europeo. (14 de junio de 2023). *"Ley de IA de la UE: primera normativa sobre inteligencia artificial."* Parlamento Europeo. Recuperado de (Ley de IA de la UE: primera normativa sobre inteligencia artificial | Noticias | Parlamento Europeo (europa.eu)).
- Portal de Administración Electrónica del Gobierno de España. (11 de diciembre de 2023). *"Ley de Inteligencia Artificial: el Consejo y el Parlamento Europeo llegan a un acuerdo sobre las primeras normas para regular la IA en el mundo*." Recuperado de (PAe - Ley de inteligencia artificial: el Consejo de Europa y el Parlamento Europeo llegan a un acuerdo sobre las primeras normas en el mundo para regular la Inteligencia Artificial (AI) (administracionelectronica.gob.es)).
- Pehlivan, C. N. (27 de diciembre de 2023). *"Los retos de armonizar la inteligencia artificial con los derechos fundamentales."* Tribuna. Pedro del Rosal. El Confidencial. Recuperado de (https://blogs.elconfidencial.com/juridico/tribuna/2023-12-27/retos-armonizar-inteligencia-artificial-derechos-fundamentales_3801180/).
- Instituto Hermes. (2020, 18 de febrero). *"Primera sentencia europea que declara ilegal un algoritmo de evaluación de características personales de los*

ciudadanos." Recuperado de (https://institutohermes.org/2020/02/18/primera-sentencia-europea-que-declara-ilegal-un-algoritmo-de-evaluacion-de-caracteristicas-personales-de-los-ciudadanos/)

- Wolters Kluwer. (2020, 13 de febrero). *"Primera sentencia europea que declara ilegal un algoritmo de evaluación de características personales de los ciudadanos."* La Ley. Disponible en: (diariolaley - Documento (laleynext.es))
- Comisión Europea. (2018, 7 de diciembre). Comunicado de prensa: *"Los Estados miembros y la Comisión colaborarán para impulsar la inteligencia artificial "fabricada en Europa"."* Bruselas. Recuperado de (Los Estados miembros y la Comisión colaborarán para impulsar la inteligencia artificial «fabricada en Europa»).

- Grupo Atico34. (2023, 24 de abril). "*Identificación biométrica ¿Qué es y cómo funciona?"* Recuperado de: (https://protecciondatos-lopd.com/empresas/identificacion-biometrica/).
- Lacort, J. (2024, March 13). "*Del Riesgo mínimo Al Riesgo inaceptable: Así define la UE los cuatro niveles de los sistemas de ia en su nueva ley."* Xataka. Recuperado de: (https://www.xataka.com/legislacion-y-derechos/riesgo-minimo-al-riesgo-inaceptable-asi-define-ue-cuatro-niveles-sistemas-ia-su-nueva-ley).
- Unión Europea. (2024). "*Resumen de alto nivel de la Ley de Inteligencia Artificial."* Disponible en: (Resumen de alto nivel de la Ley de Inteligencia Artificial | Ley de Inteligencia Artificial de la UE (artificialintelligenceact.eu)).
- Parlamento Europeo. (2024, 13 de marzo). *"Ley de IA de la UE: primera normativa sobre inteligencia artificial."* Disponible en: (Ley de IA de la UE: primera normativa sobre inteligencia artificial | Temas | Parlamento Europeo (europa.eu)).
- Ramírez Barrio, A. (06 de febrero de 2024). *"Protección del consumidor e inteligencia artificial: claves de la propuesta de Directiva sobre productos defectuosos."* Publicado por El Derecho. Disponible en: (Protección del consumidor e IA: Directiva sobre productos defectuosos (elderecho.com)).
- Pina, C. (05 de octubre de 2022). *"Inteligencia artificial (IA): así es la Propuesta de Directiva para adaptar las normas de responsabilidad extracontractual."* Publicado por Garrigues. Disponible en: (Inteligencia artificial (IA): así es la Propuesta de Directiva para adaptar las normas de responsabilidad extracontractual | Garrigues Digital).