COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

FACULTAD DE DERECHO

DERECHO DE DAÑOS EUROPEO E INTELIGENCIA ARTIFICIAL

Autor: Rafael Remigio Abad Esteban
5º Derecho y Business Analytics (E-3 Analytics)
Derecho de daños

Tutor: Íñigo Navarro Mendizábal

Madrid

Junio 2022

ÍNDICE

LISTADO DE ABREVIATURAS

CC: Código Civil

DRAE: Diccionario de la Real Academia Española

IA: Inteligencia Artificial

LCyU: Texto refundido de la Ley General para la Defensa de los Consumidores y usuarios y otras leyes complementarias

RGPD: Reglamento 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)

STJUE: Sentencia del Tribunal de Justicia de la Unión Europea

UE: Unión Europea

INTRODUCCIÓN

"*1. Un robot no hará daño a un ser humano ni, por inacción, permitirá que un ser humano sufra daño.*

2. Un robot debe cumplir las órdenes dadas por los seres humanos, a excepción de aquellas que entren en conflicto con la primera ley.

3. Un robot debe proteger su propia existencia en la medida en que esta protección no entre en conflicto con la primera o con la segunda ley."[1]

Las tres leyes de la robótica de Asimov fueron las primeras normas que hicieron patente una realidad: la necesidad de establecer leyes específicas para la relación entre el hombre y el robot.

Como afirma ANGUITA RÍOS[2], debemos ser sinceros y reconocer que, en materia de inteligencia artificial (IA), tenemos miedo a los robots y a los sistemas de IA, y a la vez no queremos renunciar a los innumerables beneficios que estos ofrecen. Por esta razón, resulta necesaria una regulación específica en torno a la IA y a los robots, especialmente en el terreno del derecho de daños. Asimov elaboró sus leyes para evitar que un robot pudiera causar daño a un ser humano, pero ¿qué sucede cuando no se logra evitar y se produce un daño? ¿quién responde? ¿cómo me defiende el ordenamiento jurídico de esta posibilidad de daño? ¿es posible que en algún momento un sistema de IA pueda responder por sus propios errores? ¿en qué se asemeja un robot a un animal en el terreno de la responsabilidad civil?

El derecho de daños ofrece un esquema de responsabilidad basado en dos elementos: la relación de causalidad (sistema objetivo) y la culpabilidad del sujeto por falta de diligencia (sistema subjetivo). Como se analizará en el trabajo, el examen de la responsabilidad de los robots y de los sistemas de IA conlleva necesariamente explorar nuevas alternativas, puesto que surgen variables a tomar en cuenta que no encajan en el esquema tradicional, tales como la automatización de procesos sin intervención humana o la multitud de fabricantes interdependientes entre ellos que dificulta separar las responsabilidades entre ellos.

---

[1] ASIMOV (1942), Círculo Vicioso. *Astounding science fiction March 1942.* p.13

[2] (2020). Inteligencia artificial y Derecho civil: líneas de pensamiento en materia de daños, *Revista Crítica de Derecho Inmobiliario*, N.º 781, p. 2541

Debido a esta nueva realidad y al rápido desarrollo tecnológico de los últimos años, la Unión Europea ha situado como prioridad una regulación en materia de IA que inspire confianza a las empresas para invertir y a los ciudadanos para utilizar los sistemas de IA, de tal manera que permita a la Unión liderar en este campo.[3]

Este trabajo brinda una perspectiva del panorama actual de responsabilidad civil en materia de IA a nivel europeo y analiza los cambios que ha sufrido el derecho de daños tradicional en esta materia, la evolución que va a sufrir asimismo durante los próximos años y estudia la protección que se ofrece a los ciudadanos europeos frente al tratamiento automatizado de datos personales, con los peligros que ello conlleva de vulneración de los derechos de protección de datos y no discriminación.

Respecto a los términos utilizados, se emplea un vocabulario perteneciente a esta materia, como sistemas de IA, robots o algoritmos. Conviene explicar a qué se hace referencia cuando se utiliza cada término, sabiendo que en algunos casos, normativa europea y textos doctrinales se separarán en cierta medida del concepto aquí ofrecido.

En primer lugar, un algoritmo es, según el DRAE, un conjunto ordenado y finito de operaciones que permite hallar la solución de un problema. Esta definición no da lugar a problemas de interpretación, pues a raíz de esta definición se entiende que los algoritmos son parte de los sistemas de IA. Sin embargo, este elemento adquiere gran importancia cuando se habla de los sesgos de los algoritmos, pues debido a diversas razones[4], un algoritmo puede presentar sesgos que afecten al funcionamiento del sistema de IA.

Por su parte, de la IA se encuentran distintas definiciones según la norma europea o según la obra doctrinal, mientras que el DRAE ofrece simplemente una definición sobre la disciplina científica[5]. A efectos de este trabajo, se puede utilizar como definición la ofrecida por el grupo independiente de expertos sobre IA: "programas informáticos (y posiblemente también equipos informáticos) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno mediante la adquisición de datos, la interpretación de los datos estructurados o no estructurados, el razonamiento sobre el conocimiento o el tratamiento de la

[3] La Resolución del Parlamento Europeo de 16 de febrero de 2017, en su Considerando V, afirma la importancia de una regulación en este sector para poder avanzar en la evolución tecnológica.
[4] BAEZA-YATES (2018), en su artículo *Bias on the Web*, realiza un análisis de las diferentes fuentes de sesgo que están presentes en todos los sistemas de IA, desde el sesgo procedente de errores en el código o de los datos de entrenamiento hasta del sesgo causado por el usuario que interacciona con el programa.
[5] "Disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico".

información, fruto de estos datos y la decisión de las mejores acciones que se llevarán a cabo para alcanzar el objetivo fijado". [6]

Finalmente, el robot es, según la DRAE, la "máquina o ingenio electrónico programable que es capaz de manipular objetos y realizar diversas operaciones". En base a esta definición, nos podemos encontrar con robots sin IA e IA que no formen parte de robots[7]. Sin embargo, cuando en este trabajo se mencione a los robots se estará haciendo referencia a aquellos que tengan dos particularidades: tienen un sistema de IA integrado dentro de ellos (por lo que se mencionará indistintamente al sistema de IA y al robot), y no necesariamente cumplen la condición de manipular objetos. La definición del DRAE no recoge aquellos robots que "manipulan" simplemente de manera *online*, por lo que, ante la mención de un robot, no se debe pensar únicamente en una máquina con forma cercana a la humanoide que desempeñe funciones físicas, sino como aquella máquina que, debido a los programas y a los sistemas informáticos que tiene integrados, es capaz de razonar matemáticamente y llegar a unos objetivos que se le introducen mediante el empleo de la IA.

[6] *Directrices éticas para una IA fiable*, p. 48

[7] NAVARRO (2021) La robótica y la Inteligencia Artificial en la nueva era de la Revolución Industrial 4.0. *La responsabilidad civil en tiempos de la IA y los robots*. p. 208.

CAPÍTULO I: EVOLUCIÓN NORMATIVA DE LA UE

La evolución normativa europea en materia de IA tiene su origen en la Cumbre Digital de Tallin de 29 de septiembre de 2017, convocada por la Presidencia estonia del Consejo y que reunió a los jefes de Estado y de Gobierno de los Estados miembros, junto con el presidente del Consejo Europeo y de la Comisión Europea. En dicha cumbre se debatió sobre la Agenda Digital, se discutió sobre distintos proyectos de innovación digital y se afirmó la necesidad de la Unión de adaptarse al progreso en materia de IA, tanto a nivel tecnológico como económico y legislativo.

Este encuentro supuso una llamada a los órganos legislativos de la Unión para que abordaran la principal preocupación del momento en lo que respecta a la Agenda Digital[8], a lo que respondieron a través de distintos documentos emitidos por diferentes organismos europeos, hasta llegar – a día de este trabajo – a la Propuesta de Reglamento del Parlamento Europeo y del Consejo de 21 de abril de 2021, por el que se establecen normas armonizadas en materia de Inteligencia Artificial (Ley de IA) y se modifican determinados actos legislativos de la Unión.

Debido a la multitud de organismos que han emitido dictámenes, recomendaciones y consejos, el objetivo de este capítulo no es analizar en profundidad toda la actividad legislativa de la Unión, sino ofrecer una perspectiva histórica de los últimos años respecto a esta materia. Por otra parte, carecería de sentido un análisis exhaustivo dado el gran dinamismo de esta materia, lo cual implica que la actividad legislativa está todavía en proceso y en ningún caso es definitiva. Por lo tanto, este capítulo trata de mostrar, a través de los documentos que se han considerado más relevantes, el camino seguido por la Unión hasta llegar a la Ley de IA.

1. RESOLUCIÓN DEL PARLAMENTO EUROPEO, DE 16 DE FEBRERO DE 2017, CON RECOMENDACIONES DESTINADAS A LA COMISIÓN SOBRE NORMAS DE DERECHO CIVIL SOBRE ROBÓTICA

Esta resolución del Parlamento Europeo se puede considerar el inicio del camino legislativo europeo sobre la IA. El reto legislativo de evitar la disparidad de normativas

[8] El 27 de abril de 2016 se había aprobado el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo 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 (RGPD). Este reglamento se había convertido en un referente mundial respecto de la protección de datos, por lo que la IA se convirtió en el siguiente elemento principal de la Agenda Digital.

en materia de IA comienza con una propuesta por parte del Parlamento a la Comisión para que legisle sobre los robots inteligentes. Al ser la primera aproximación, se incluyen una gran cantidad de ideas a ser desarrolladas, como por ejemplo el impacto que puede tener el desarrollo de los robots y de los sistemas de IA en diferentes sectores como la automoción, la medicina, el empleo y el medioambiente. En esta sección se recogen las aportaciones que se han considerado más relevantes para este trabajo.

En primer lugar, se reconoce la rápida evolución de los sistemas de IA, la tendencia de creación de robots autónomos con capacidad de aprendizaje y adaptación que interactúan por sí solos con los seres humanos, así como los retos jurídicos que presentan, tales como garantizar la no discriminación, la transparencia y la inteligibilidad de los procesos decisorios. Esta velocidad y estos nuevos retos hacen necesario un nuevo marco legislativo en el que se pueden apreciar dos piedras angulares: el respeto a los derechos fundamentales y el favorecimiento de la innovación.

Este segundo elemento refleja la vital importancia que la Unión otorga a la innovación tecnológica. La gran inversión económica que se planea realizar en los próximos años (más de 1.000 millones de euros en anuales en el período 2021-2027 en apoyo a la innovación tecnológica a través de los programas Europa Digital[9] y Horizonte Europa[10]) debe ir acompañada de un marco legislativo que proteja el libre mercado, no frene la innovación por parte de desarrolladores y fabricantes, genere seguridad jurídica respecto a la responsabilidad contractual y garantice un reconocimiento mutuo en el ámbito de los controles, certificaciones y trámites de seguridad.

De esta manera, afirma que el marco jurídico de derecho de daños ha caído en la obsolescencia. Se plantea el problema de quién debe responder de los daños causados por los robots autónomos, pues con el marco actual responderá el fabricante causante del daño (responsabilidad objetiva) o el usuario que pudo haber evitado el daño (responsabilidad subjetiva), pero el robot autónomo no puede ser jurídicamente responsable, al no poder determinarse el deudor de la indemnización, y no queda claro el papel de los agentes

[9] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el período 2021-2027. COM(2018) 434

[10] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea el Programa Marco de Investigación e Innovación «Horizonte Europa» y se establecen sus normas de participación y difusión. COM(2018) 435

intermedios entre el fabricante y el usuario (desarrollador del algoritmo, responsable del entrenamiento, importador del bien, etc.).

En atención a todos estos aspectos, estas son las principales solicitudes que transmite el Parlamento a la Comisión:

(i) La elaboración de una propuesta de definición europea común de "robot inteligente" y de sus subcategorías, teniendo en cuenta sus principales características: autonomía, interconectividad, capacidad de autoaprendizaje, soporte físico mínimo, capacidad de adaptación e inexistencia de vida en sentido biológico. Ligada a esta definición, se propone la creación de un sistema de clasificación de robots junto con un registro europeo de robots.

(ii) Proteger el libre mercado en lo que respecta al uso transfronterizo de robots, dando especial importancia al principio de reconocimiento mutuo, recordando que las certificaciones, autorizaciones y requerimientos burocráticos de controles realizados en un Estado miembro deben ser reconocidas en los Estados restantes.

(iii) Reforzar la inversión en investigación robótica.

(iv) Actualizar el marco normativo completándolo con directrices éticas. Se añade como anexo a la resolución una Carta sobre robótica que recoge principios que deben ser tenidos en cuenta a la hora de formular las propuestas legislativas. En esta actualización se debe tener presente de manera especial el principio de transparencia, resaltando la necesidad de poder entender en todo momento el proceso lógico que ha llevado al robot a tomar una decisión. En esta línea, se propone la inclusión de una "caja negra" en todos los robots avanzados para guardar un registro de los cálculos hechos y poder así comprender los pasos tomados en el proceso decisorio.

(v) Estudiar la posibilidad de designar una agencia europea para la robótica y la inteligencia artificial.

(vi) Respetar el RGPD, por lo que los nuevos proyectos normativos de la comisión y de los Estados miembros sean elaborados al amparo de este Reglamento.

(vii) En lo referente al nuevo proyecto normativo, priorizar las cuestiones relativas a la responsabilidad civil, debiendo ser el ámbito por el que se comience a legislar.

Respecto a esta última propuesta, se solicita a la Comisión que en el nuevo proyecto legislativo se exploren y analicen todas las posibles soluciones jurídicas. Dado que recoge algunas de estas nuevas posibilidades, es la sección más innovadora de la Resolución. Así, se propone establecer un régimen de seguro obligatorio para los distintos tipos de robots, utilizando como ejemplo el sistema de los automóviles. En esta línea, se debe crear un fondo de compensación que permita a los fabricantes y desarrolladores acogerse a un régimen de responsabilidad limitada. Este ha sido uno de los elementos más criticados, ya que hay autores que consideran que únicamente se está tratando de eximir de responsabilidad a los fabricantes y desarrolladores para favorecer la innovación[11].

Sin embargo, la mayor aportación de esta Resolución es la propuesta realizada al final del documento, donde se explora la posibilidad de "*crear a largo plazo una personalidad jurídica específica para los robots, de forma que como mínimo los robots autónomos más complejos puedan ser considerados personas electrónicas responsables de reparar los daños que puedan causar*". Es la primera vez que se sugiere en un texto normativo la posibilidad de dotar de personalidad jurídica a los robots. Esta idea ha dado a numerosas obras, ensayos y discusiones doctrinales que serán analizados más en profundidad en el Capítulo II.

2. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES DE 7 DE DICIEMBRE DE 2018. PLAN COORDINADO SOBRE LA INTELIGENCIA ARTIFICIAL.

El Plan Coordinado sobre la IA de la Comisión elaborado en 2018 – y actualizado en 2021 – supone una nueva llamada a la necesidad de un marco regulatorio concreto y actualizado sobre la IA.

Este Plan Coordinado tiene dos precedentes: en primer lugar, la firma de un compromiso de cooperación en el ámbito de la IA por parte de 24 Estados miembros y Noruega el 10 de abril de 2018. Por otra parte, la Comunicación de la Comisión "Inteligencia Artificial para Europa" del 25 de abril de 2018[12], en la cual se establece una estrategia en Europa para la IA fundamentada en la potenciación de la capacidad tecnológica e industrial de la UE en los sectores público y privado, en la preparación para

[11] SUÑÉ LLINAS, E. (2020) *Derecho e Inteligencia Artificial*. p. 117.
[12] COM(2018) 237

las transformaciones socioeconómicas futuras y en la garantía de establecer de un marco jurídico y ético apropiado, incluyendo una directriz de interpretación de las normas relativas a productos defectuosos.[13]

Entre las medidas del Plan Coordinado se recogen cerca de 70 propuestas centradas en la cooperación entre Estados miembros y la Comisión en materia de investigación, inversión, los datos, la introducción al mercado y la retención de talento. Todas estas medidas están orientadas a la maximización de las inversiones en IA y a la previsión de un marco en el que estas acciones pueden operar. Este plan refleja la real preocupación respecto a la baja inversión europea en IA en comparación con otros continentes como América del Norte y Asia.

Por esta razón, la Comisión solicita al Consejo que avale el plan propuesto, a los Estados miembros que implementen el Plan Coordinado y desarrollen sus respectivas estrategias nacionales, y a los colegisladores que adopten las figuras jurídicas necesarias para poder favorecer el mercado único.

3. LIBRO BLANCO, DE 19 DE FEBRERO DE 2020, SOBRE LA INTELIGENCIA ARTIFICIAL: UN ENFOQUE EUROPEO ORIENTADO A LA EXCELENCIA Y LA CONFIANZA

El Libro Blanco elaborado por la Comisión ofrece alternativas para facilitar el desarrollo de la IA en la Unión a través de un enfoque de coordinación en torno a las implicaciones éticas y económicas de la IA. Para ello, se fundamenta en el desarrollo de un ecosistema de excelencia, a través del aumento de cooperación internacional y una armonización de esfuerzos, y un ecosistema de confianza, mediante una elaboración de un marco jurídico apropiado.

En lo que respecta al marco jurídico, el Libro Blanco recoge las aportaciones anteriores elaboradas por la Comisión, tales como el Plan Coordinado de IA de 2018 – la primera acción que se anuncia en el Libro Blanco es la actualización del Plan Coordinado, la cual fue efectiva en 2021 – o las directrices éticas para una IA fiable realizadas por el

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

grupo de expertos de alto nivel sobre inteligencia artificial el 8 de abril de 2019. Estas últimas directrices sirvieron de gran inspiración al recoger los siguientes requisitos como presupuestos para el desarrollo de una IA que ofrezca seguridad y confianza: acción y supervisión humana, solidez técnica y seguridad, gestión de la privacidad y de los datos, transparencia, diversidad, no discriminación, equidad, bienestar social y medioambiental, rendición de cuentas.

En la creación de un ecosistema de confianza, se estudia la posibilidad de actualizar el marco actual frente a crear uno nuevo y se propone finalmente crear un marco jurídico específico para el uso de la IA. A raíz de este documento ya no se habla únicamente de una actualización del marco jurídico como en la Resolución del Parlamento de 16 de febrero de 2017, sino que se propone una legislación concreta. Por lo tanto, este Libro Blanco supone el precedente de la Ley de IA. Además de afirmar esta necesidad, se enumeran una serie de elementos imprescindibles que debe recoger el nuevo marco regulador:

(i) Determinación del ámbito de aplicación. Para ello, se debe concretar lo que se entiende por sistema de IA[14], sabiendo que debe ser una definición suficientemente flexible para adaptarse al progreso tecnológico.

(ii) Elaboración de la legislación teniendo en cuenta los peligros específicos de la IA: protección de los datos personales y la privacidad y la no discriminación, junto con el funcionamiento eficaz del régimen de responsabilidad civil.

(iii) Proposición de un enfoque basado en el riesgo para mantener el equilibrio entre la protección de los derechos fundamentales y la potenciación de la inversión.

(iv) Establecimiento de requisitos concretos para aquellos sistemas de riesgo elevado. Se enumeran una serie de características esenciales sobre las que se deben imponer determinadas obligaciones para lograr una seguridad jurídica efectiva y un auténtico respeto a los derechos fundamentales. Dichas características, a las que acompañan algunas propuestas de medidas, son: los datos de entrenamiento, la

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

conservación de registros y datos, el suministro de información, la solidez y exactitud, la supervisión humana y los casos de identificación biométrica.

(v) En materia de destinatarios, distribución de las obligaciones a lo largo de la cadena de producción, asignando responsabilidades a los agentes económicos que estén en mejor posición para evitar el posible riesgo[15]. Respecto al alcance geográfico, es imprescindible que el nuevo marco someta a aquellas personas físicas y jurídicas que ofrezcan productos o servicios que incorporen sistemas de IA dentro del territorio de la Unión, independientemente de su lugar de residencia. Solamente así se logrará una seguridad jurídica y una confianza real.

(vi) Respecto al control, se resalta la necesidad de establecer un control objetivo previo de conformidad como al que están sujetos otros productos comercializados en la UE. Este control podrá realizarse sobre los algoritmos y los datos (elementos esenciales de la IA según la Comisión[16]), teniendo en cuenta la capacidad de aprendizaje de los algoritmos y la indisponibilidad previa de toda la información utilizada en el entrenamiento. De la mano de este control, se aborda la necesidad de una estructura de gobernanza europea en materia de IA, la cual podría ser la responsable de realizar el control y debe estar en comunicación y cooperación con las autoridades nacionales.

4. PROPUESTA DE REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO, 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

La Ley de Inteligencia Artificial es la propuesta legislativa de la Comisión con la que se trata de crear un marco jurídico para la IA en todos los ámbitos, excluyendo únicamente el militar. A este Reglamento estarán sometidos todos los sujetos, públicos y privados, que ofrezcan y utilicen sistemas de IA que se encuentren en la Unión, independientemente de si residen en un tercer país distinto a un Estado miembro de la

[15] Uno de los elementos más problemáticos respecto del derecho de daños tradicional es la imputación de la responsabilidad por daños al fabricante del producto defectuoso. Esta conexión es insuficiente para aquellos sistemas de IA donde, además del fabricante, intervienen otros agentes como el desarrollador, el implementador o el distribuidor de servicios.
[16] COM(2020) 65 final p. 20

Unión,[17]. Esta Ley de Inteligencia Artificial sigue en gran medida las recomendaciones de los documentos explicados anteriormente, si bien realiza a su vez algunas aportaciones propias.

En primer lugar, el Reglamento presenta una nueva definición de sistema de IA, estableciendo en su artículo 3 que se entiende por sistema de IA "el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa." Se puede apreciar cómo esta definición no es idéntica a la aportada por el grupo de expertos. Este hecho se explica en la recomendación del Libro Blanco por la que se propone aportar una definición general que pueda comprender múltiples sistemas, tanto presentes como futuros. De esta manera, el artículo 4 otorga a la Comisión facultades para ampliar la lista de sistemas integrados en el anexo I, de tal manera que el Reglamento no se quede obsoleto ante el progreso.

La Ley de Inteligencia Artificial asume un enfoque basado en el riesgo, tomando distintas medidas para los diferentes niveles de riesgo que un sistema de IA pueda presentar. Se señalan cuatro niveles con sus respectivas obligaciones:

(i) Riesgo inaceptable: prácticas prohibidas. Son aquellos riesgos que la Comisión considera inadmisibles por atentar contra los valores de la Unión. Los sistemas de IA que presenten este tipo de riesgos están prohibidos en todo el territorio de la Unión. Se incluyen en esta lista los sistemas de manipulación mediante técnicas subliminales que puedan causar perjuicios físicos o psíquicos, los sistemas de puntuación social por parte de las autoridades públicas y los sistemas de identificación biométrica remota en tiempo real con algunas excepciones, como la amenaza terrorista o la búsqueda de víctimas.

(ii) Riesgo alto: evaluación de conformidad. El concepto "alto riesgo" comprende una variedad de peligros que, si bien no son completamente inadmisibles, son potencialmente transgresores de los valores de la Unión y de la seguridad de los ciudadanos. Los sistemas que se consideran de alto riesgo están recogidos en un

[17] Se continúa la tendencia iniciada con el RGPD, que tiene el mismo ámbito de aplicación respecto de los datos personales.

anexo de la Ley de IA (sistemas utilizados en educación, empleo, identificación biométrica, infraestructuras públicas, administración de la justicia, etc), la cual puede ser revisada y ampliada por la modificación. También se incluyen con los sistemas que, según la legislación sectorial europea, sean utilizados como componentes de seguridad y estén sometidos a una evaluación de conformidad. Debido a la peligrosidad de estos sistemas, el Reglamento impone la obligación de someterlos a una evaluación de conformidad y gestión del riesgo con carácter previo a su comercialización. Los requisitos por cumplir se desprenden de las recomendaciones del Libro Blanco mencionadas *supra*: gobernanza de datos que garantice la calidad, documentación técnica detallada que aporte información sobre el sistema y la finalidad, actualización de registros, medidas de transparencia y supervisión humana que minimicen el riesgo, exigencias de alta precisión, solidez y ciberseguridad. No obstante, las obligaciones no cesan una vez superada la evaluación de conformidad previa, sino que se imponen obligaciones a los proveedores, distribuidores, importadores y a los usuarios durante toda la vida del producto. Dichas obligaciones incluyen la cooperación con autoridades, la información al fabricante o la elaboración de documentación técnica, entre otras.[18]

(iii) Riesgo limitado: obligación de transparencia. Los sistemas de IA que presentan este riesgo son aquellos que interactúa con los seres humanos y no se consideran especialmente peligrosos para la vida, salud o derechos de los ciudadanos (asistentes virtuales o *chatbots*). La principal obligación es la de transparencia con el usuario, asegurando el conocimiento por parte del usuario de estar interactuando con un sistema de IA.

(iv) Riesgo mínimo: sin obligaciones adicionales. Actualmente, la mayoría de los sistemas de IA presentes en la Unión se acogen a esta categoría. Son aquellos sistemas que presentan un riesgo mínimo o nulo para la seguridad de los ciudadanos (IA en videojuegos, filtros de correo basura o *spam*). Para este tipo de sistemas, el Reglamento no prescribe ninguna obligación adicional a las que ya tengan según sus respectivas leyes, si bien pueden – y recomienda para garantizar la confianza en los sistemas de IA – acogerse a códigos de conducta voluntarios,

[18] Artículo 16 en relación con el artículo 28

lo cual en la práctica significa cumplir de manera voluntaria los requisitos establecidos por los sistemas de alto riesgo.

En lo referente a la gobernanza, se crea un Comité Europeo de IA, formado por las autoridades nacionales competentes de supervisión y el Supervisor Europeo de Protección de Datos. El comité tiene funciones de coordinación y asistencia, junto con la emisión de dictámenes, recomendaciones y contribuciones, pero el control específico del cumplimiento de los requisitos de los sistemas de alto riesgo y de las obligaciones de transparencia queda en manos de las autoridades nacionales, las cuales serán designadas por cada Estado miembro.

Como se puede comprobar, la actual legislación supone una regulación que trata de inspirar confianza en la seguridad de los sistemas de IA. Por tanto, resulta una legislación dirigida a la industria, pero con el foco en el ciudadano. Para lograr esta percepción se ha preferido dejar a un lado la regulación específica de la responsabilidad civil, la cual será tratada en el siguiente capítulo analizando la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial.

Como toda nueva legislación, tiene sus detractores y sus defensores. Asimismo, mientras la Asociación de Consumidores Europeos (BEUC) ha sido muy crítica y la considera una regulación débil debido al alto número de excepciones en los que se permite los sistemas prohibidos, las industrias innovadoras consideran que tanto impedimento y control previo supone una traba para la investigación y el desarrollo en comparación con Estados Unidos o Asia.

No obstante, en líneas generales la Ley de Inteligencia Artificial ha seguido las líneas que se marcaron en la Cumbre Digital de Tallin de 2019, potenciar la innovación salvaguardando los derechos fundamentales de los ciudadanos europeos.

CAPÍTULO II: RESPONSABILIDAD CIVIL Y LOS SISTEMAS DE IA

1. DERECHO DE DAÑOS TRADICIONAL E IA

Como señalaba la Resolución del Parlamento Europeo de 16 de febrero de 2017, uno de los principales problemas de los nuevos sistemas de IA es el régimen de responsabilidad civil ante los daños que puedan ser causados por el funcionamiento de un sistema de IA. Para entender el problema debemos remontarnos al marco jurídico vigente de responsabilidad por productos defectuosos, la Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos.

Esta Directiva ofrece un marco de responsabilidad para el producto defectuoso que infringe un daño en un ciudadano, estableciendo un régimen de responsabilidad objetiva, el cual será explicado más adelante, que se ha mantenido vigente como instrumento de armonización durante más de 35 años. No obstante, Como ANGUITA RÍOS[19] defiende, las normas tradicionales de derecho de daños no sirven para aquellos sistemas de IA autónomos que pueden tomar decisiones propias. Se expone a continuación un resumen de las razones por las que este sistema ha devenido insuficiente.

En primer lugar, como NÚÑEZ ZORRILLA[20] afirma, las nuevas tecnologías traen consigo nuevos tipos de daños y, con ellos, nuevos derechos que se ven amenazados y se deben proteger. De esta manera, nos encontramos con actuaciones de los sistemas de IA que pueden causar daños que eran inimaginables hace 35 años, tales como los daños derivados del sesgo de un algoritmo correctamente programado pero incorrectamente entrenado, daños derivados de la evaluación de un sistema de IA hacia una persona que le niega determinadas prestaciones como un crédito bancario, o daños en la privacidad y en la protección de datos personales al ser tratados por un algoritmo sin contar con el consentimiento expreso de la víctima[21]. En esta misma línea, ABBOT[22], profesor de la universidad de UCLA, afirma que utilizar normas diseñadas para humanos para regular las conductas de las máquinas trae consigo consecuencias negativas e imprevistas en el momento en el que las máquinas comienzan a actuar como personas.

[19] *Op.cit.,* p. 2564
[20] (2019). *Inteligencia artificial y responsabilidad civil.* p. 9.
[21] Estos son algunos de los daños explicados por NAVARRO (2021), *Op.cit.*, pp. 218-221.
[22] (2020). The Reasonable Robot: Artificial Intelligence and the Law, *Cambridge University Press*. p. 3.

En segundo lugar, nos encontramos con una disociación de actividades que dificulta en gran medida identificar al fabricante concreto de la parte defectuosa del producto dañino. Podemos pensar en el ejemplo paradigmático del vehículo autónomo que tiene un accidente debido a un error en la detección del coche de delante. En ese proceso han intervenido el programador del *software*, el desarrollador de las actualizaciones, el proveedor de los datos de los satélites, etc. Otro ejemplo ilustrativo es el utilizado por el Grupo de Expertos en Responsabilidad y Nuevas Tecnologías[23], en el cual se compara un sistema de alarmas tradicional con uno moderno. Antiguamente, un sistema de alarmas podía fallar por un defecto en el cable en el detector de humo, por poner un ejemplo, lo cual llevaba a una fácil identificación del responsable. Sin embargo, un sistema moderno puede fallar asimismo por un error en el código del *firmware* o por su adaptación a los componentes del *hardware* y adicionalmente, si el sistema ha sido desarrollado por algoritmos de *deep learning* y *machine learning* que se basan en datos de múltiples fuentes externas para optimizar su funcionamiento, las posibles fuentes del daño se multiplican.

DÍAZ ALABART declara que *"todos esos daños pueden proceder de algún defecto en la fabricación o programación de los robots, de falta de información sobre su funcionamiento o información incorrecta de, inadecuación del tipo de robots a las tareas que serán asignados, o incluso del uso incorrecto de los mismos por el usuario"*[24]. Por tanto, en el campo de los daños causados por sistemas de IA nos solemos encontrar con una cadena de responsabilidades interdependientes unas de otras que conlleva una gran complicación a la hora de detectar el nexo causal entre el daño y el fallo en el sistema. En último término, esto implica una gran inseguridad para el consumidor que quiera reclamar una indemnización ante un daño, pues se encontrará en una situación de indefensión ante su incapacidad de identificar al sujeto culpable.

Estas razones hacen conveniente una ampliación del concepto de sujeto responsable, una actualización normativa en lo que se refiere al nexo causal y un estudio de posibles alternativas jurídicas a las tradicionales, tales como la personalidad jurídica de los robots.

[23] (2019) *Liability for artificial intelligence and other emerging digital technologies.* p. 20.
[24] (2018). *Robots y Responsabilidad civil*. Madrid: Reus. P. 55. Entiéndase el concepto robot utilizado por DÍAZ ALABART como máquina que integra un sistema de IA. Más adelante se explicará la diferencia entre los robots corpóreos y no corpóreos.

2. POSIBLES RESPONSABLES CIVILES

En este campo en el que puede resultar de gran complejidad determinar quién es el sujeto responsable de los daños causados por el sistema de IA, se propone a continuación los posibles responsables civiles de los daños del sistema de IA. A estos sujetos se les podrá imputar responsabilidad civil de diferentes maneras, como se explicará más adelante.

2.1. El fabricante

El fabricante se puede entender como aquella/s persona/s que interviene/n en la producción del bien o servicio que se ofrece directa o indirectamente al consumidor final. El derecho civil ha sido tradicionalmente estricto con esta figura, ya que se considera que tiene una posición de fuerza frente al consumidor, por lo que la legislación debe exigirle responsabilidad[25].

Resulta de gran utilidad para este caso la definición de productor que aporta la LCyU en su artículo 138, en la cual este concepto abarca al fabricante, al importador del producto en la Unión, así como al proveedor del producto al proveedor del servicio en caso de que no se pudiera identificar al productor original.

Por otra parte, ya se ha mencionado la multitud de fabricantes que pueden formar parte en la producción de un bien que tenga integrado un sistema de IA. Cada uno de los fabricantes parciales de los distintos elementos que forman parte de un producto es considerado fabricante y el usuario podrá dirigirse contra cualquiera de ellos, que responderán de manera solidaria por los daños del producto según la LCyU[26].

Cabe preguntarse en este contexto si el programador del algoritmo que aporta las instrucciones al sistema de IA se puede considerar como fabricante parcial o no. En este sentido, pueden tenerse en cuenta distintos elementos tales como si el algoritmo es exclusivo para ese tipo de producto o es algo general en el mercado, o la consideración del algoritmo como producto o servicio. A pesar de las diversas opiniones doctrinales, la opinión de este trabajo es que sí puede considerarse como fabricante, puesto que una programación incorrecta puede afectar sin duda alguna al funcionamiento del bien final,

[25] Sirva como ejemplo la Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (LCyU), donde se establece un amplio concepto de productor (arts. 5 y 138), se regulan las cláusulas abusivas (art. 82) y se regula de manera amplia los derechos y garantías del consumidor por garantizar su posición de debilidad frente al empresario (arts. 59-127 bis).
[26] LCyU, art. 132

provocando algún daño indemnizable. Más allá de acciones de responsabilidad internas entre fabricantes o controles de seguridad que se deban seguir, resulta conveniente – teniendo como prioridad la protección del consumidor final – integrar al desarrollador del algoritmo en la categoría de fabricante o productor.

2.2. El formador

Distinto del programador del algoritmo es aquel que entrena al sistema mediante el suministro de datos. Es comúnmente conocido que los modelos de *machine learning* que forman parte de los sistemas de IA basan su funcionamiento en la utilización de cantidades masivas de datos que les permiten explicar y predecir distintos fenómenos con gran precisión, por lo que el sujeto que aporta esos datos al sistema juega un papel esencial en el correcto funcionamiento del mismo, independientemente de encontrarnos ante modelos de aprendizaje supervisado (modelos de clasificación y regresión) o no supervisado (*clustering*).

El formador puede aportar diversas fuentes de datos que sirvan para entrenar al modelo y enseñarle a tomar sus propias decisiones en base a la información que ya ha recibido. Por lo tanto, cuanta mayor sea la capacidad de aprendizaje del modelo y mayor autonomía desarrolle después del aprendizaje, mayor será la responsabilidad del formador del sistema y menor será la del desarrollador. Esta distribución de responsabilidades encuentra su explicación en el hecho de que dos sistemas con el mismo código de programación pueden realizar actuaciones completamente distintas a raíz de su entrenamiento. Problemas que ya se han mencionado como la discriminación o la puntuación crediticia encuentran su origen en la formación del algoritmo por un suministro incorrecto de datos con mayor frecuencia que en la programación del mismo.

Se pueden utilizar dos ejemplos famosos para diferenciar la responsabilidad del desarrollador como fabricante y la del entrenador: El primero de ellos es el viral caso de Tay, el robot de IA programado por Microsoft para interactuar con usuarios de Twitter[27]. Tras su lanzamiento, en menos de 24 horas, Tay comenzó a emitir *tweets* racistas, de contenido sexual y defensores del holocausto. Tay fue diseñado para aprender de los *tweets* de todos los usuarios de Twitter, por lo que Microsoft retiró el programa debido a

[27] BBC Mundo, "Tay, la robot racista y xenófoba de Microsoft". *BBC,* 25 de marzo de 2016. (Disponible en: https://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb. Último acceso: 01/06/2022)

que no había diseñado a Tay para que detectar el contenido inapropiado de Twitter y lo ignorara. De esta manera, fue su aprendizaje en la interacción con determinados usuarios lo que lo llevó a emitir estos *tweets* altamente inapropiados.

El segundo caso es el famoso sistema de IA propiedad de IBM, Watson. El robot que se hizo famoso por ganar en un concurso de televisión estadounidense[28] es indiscutiblemente uno de los sistemas mejor programados del mundo y se ha utilizado en múltiples campos como en la división de consultoría de IBM, en medicina e incluso se ha utilizado como modelo para crear el programa Ross, que funciona como consultor jurídico[29]. Sin embargo, con el fin de que entendiera mejor el lenguaje humano, IBM decidió integrar en su información el *Urban Dictionary*, un diccionario de internet que incluye términos coloquiales y frases hechas en inglés. Como resultado, integró tan exitosamente la información que terminó respondiendo vulgarmente las consultas de los usuarios (a modo de ejemplo, ante algunas consultas su respuesta era simplemente: "*bullshit"*), por lo que IBM (en calidad de formador) decidió retirar la información del *Urban Dictionary* de la base de datos de Watson.

Como se puede apreciar, mientras el primer caso es un error en el desarrollo (fabricante), el segundo error trae causa en el incorrecto suministro de datos al modelo que formaba parte del sistema de IA. Si bien este caso concreto no implicó ninguna indemnización, es extrapolable a un caso en el que sí que se termine causando un daño a una persona.

2.3. El usuario

A pesar de estar analizando aquellos robots autónomos que son capaces de decidir por sí mismos en base a su código y los datos de entrenamiento, los sistemas de IA siempre deben estar sujetos a la acción y supervisión humana[30]. Por tanto, por pequeña que sea, siempre habrá una interacción entre el usuario y el sistema de IA. Cabe resaltar que el concepto clave aquí es el usuario, el cual se asemeja más a la figura del poseedor que a la del propietario.

---

[28] BEST, J., "IBM Watson: The inside story of how the Jeoparty-winning supercomputer was born, and what it wants to do next." *TechRepublic*. (Disponible en: https://www.techrepublic.com/article/ibm-watson-the-inside-story-of-how-the-jeopardy-winning-supercomputer-was-born-and-what-it-wants-to-do-next/. Último acceso: 03/06/2022)

[29] SUÑÉ LLINAS, E *Op.cit,* p. 89

[30] *Directrices éticas para una IA fiable*, p. 3

Actualmente no hay un régimen de responsabilidad civil para los usuarios de los sistemas de IA. En este contexto, salvando las diferencias, la responsabilidad del usuario podría asimilarse a la responsabilidad del dueño de un animal que recoge el art. 1905 CC, como plantea NAVARRO MENDIZÁBAL[31]. Se puede asemejar tanto en cuanto un sistema de IA actúa – en cierta medida – con cierta autonomía, pero bajo el control del usuario, quien tiene – o debe tener – la capacidad de que el sistema cese en sus acciones (apagar).

En esta línea, ANGUITA RÍOS[32] defiende que, ante un daño causado por un robot, el responsable directo es aquel que se sirve de él, es decir, quien ostenta su titularidad. De esta manera, el damnificado por el robot no deberá acudir al fabricante o al formador, tratando de dilucidar cuál fue el error que causó el daño, sino que se dirigirá directamente contra el usuario/titular, el cual más adelante tendrá acción contra el fabricante o contra el formador en un proceso aparte.

3. MODELOS DE IMPUTACIÓN DE RESPONSABILIDAD

De acuerdo con lo comentado previamente, la cuestión esencial en la responsabilidad civil es la determinación del sujeto responsable. De manera genérica, hay dos modelos diferentes de imputación de responsabilidad, según se atienda al daño y a su relación causal (objetivo) o al sujeto potencialmente responsable y a las medidas que podría haber tomado para disminuir el riesgo de daño (subjetivo).

3.1. Responsabilidad objetiva

La responsabilidad civil objetiva es el enfoque tradicional en el derecho de daños. En este sentido, la Directiva 85/374/CEE adopta este régimen de responsabilidad para la responsabilidad civil del fabricante de los daños causados por productos defectuosos.

Según este modelo, un sujeto será civilmente responsable si se prueban tres elementos: el daño, el defecto en el producto y la relación causal entre ambos. Este modelo es tradicionalmente utilizado debido a que brinda una mayor seguridad al damnificado, pues conoce claramente los elementos que debe probar. De esta manera, el fabricante será responsable salvo que exista alguna de las causas de exoneración.[33]

[31] *Op.cit.*, p. 235
[32] *Op.cit.*, P. 2567
[33] El art. 140 LCyU recoge las causas de exoneración del fabricante: el producto no estaba en circulación; es posible presumir que el defecto no existía cuando se puso en circulación el producto; el producto no había sido fabricado para su comercialización; el defecto se debió a que el producto se realizó siguiendo

Debido a que es favorable para el consumidor final, son numerosos los autores que defienden este modelo de responsabilidad para los sistemas de IA.[34] No obstante, se debe tener en cuenta que este modelo no resulta suficientemente adecuado para aquellos sistemas de IA que contienen algoritmos cuya opacidad y complejidad técnica impiden conocer el proceso decisorio del sistema de IA. Esta falta de transparencia dificulta al usuario probar el error o la relación causal entre el error y el daño sufrido.

Entre las posibles soluciones a este problema, encontramos en primer lugar la necesidad de incluir una "caja negra" en estos algoritmos, de tal manera que se puedan comprobar los diferentes pasos tomados por el sistema de IA a la hora de decidir.[35] Por otro lado, como GÓMEZ-REISCO[36] defiende, se puede establecer un régimen de solidaridad entre todos los fabricantes (con la posibilidad de extenderlo a los formadores), de tal manera que el consumidor o la persona dañada pueda dirigirse contra cualquiera de ellos, sin perjuicio de las correspondientes acciones de repetición que tengan entre ellos. De esta forma, se lograría una seguridad para el consumidor, quien no tendría que concretar el responsable del defecto específico que causó el daño, sino que le bastaría con hallar un defecto general del producto que ha derivado en el hecho dañino, debiendo los fabricantes repartirse la responsabilidad entre ellos.

3.2. Responsabilidad subjetiva: gestión de riesgos

El modelo de gestión de riesgos traslada su foco del nexo causal entre daño y defecto a la conducta del sujeto responsable, analizando el nivel de diligencia empleado a la hora de fabricar el producto para poder determinar su grado de culpabilidad. Es el criterio al que se acoge el Código Civil, el cual en sus artículos 1101 y 1902 exige la existencia de culpabilidad para la posible imputación de responsabilidad.

Este sistema presenta la ventaja de focalizarse en aquellos eventos que son potencialmente peligrosos, prestando atención a los sucesos que pueden desembocar en un resultado no deseado. De esta forma, los fabricantes de partes menos peligrosas quedan libres de la responsabilidad solidaria mencionada anteriormente, ya que resulta más fácil

normas imperativas; el estado de los conocimientos científicos y técnicos existentes en el momento de la comercialización del producto no permitían detectar los defectos.

[34] ANGUITA RÍOS, *Op.cit.*, p. 2574

[35] Una de las medidas de la Propuesta del Parlamento Europeo de 16 de febrero de 2017

[36] (2018). *Los robots y la responsabilidad civil extracontractual en Derecho de los robots. p*. 125

probar que su elemento no tiene riesgo de producir el daño en vez de demostrar que otro elemento efectivamente causó el daño.

Sin embargo, como consecuencia de lo afirmado, el principal problema de este sistema reside en la dificultad probatoria, puesto que el damnificado debe probar que el responsable (fabricante, formador o usuario) no fue suficientemente diligente como para poder prever el fallo que produjo el daño.

Puesto que la responsabilidad subjetiva impone unos deberes de conducta adicionales, a los fabricantes y el proveedor les bastará demostrar que tomaron medidas para evitar la aparición de los potenciales riesgos para evitar la imputación de responsabilidad. Para ello, los fabricantes deberán realizar una evaluación previa de los posibles riesgos del producto y evaluar si los riesgos que presenta son los que un consumidor ordinario podría esperar del producto (este es el *consumer expectation test* que se contrapone al *risk-utility* test que realiza una ponderación de riesgos y beneficios del producto[37]). Mediante la realización de esta evaluación de riesgos y la toma de medidas para evitarlos, el fabricante o formador[38] habrá actuado diligentemente, por lo que un futuro daño del producto no le será imputable incluso existiendo nexo causal.

3.3. Modelo híbrido: Resolución del Parlamento Europeo sobre un régimen de responsabilidad civil en materia de IA

Dada la importancia de establecer un régimen de responsabilidad civil para los sistemas de IA, el Parlamento ha emitido una resolución por la cual propone a la Comisión un reglamento de responsabilidad en materia de IA. Los tres pilares en los que se fundamenta esta propuesta de reglamento son: la necesidad de actualizar y no sustituir el régimen vigente de responsabilidad; un enfoque híbrido basado en el riesgo; y la ausencia de personalidad jurídica de los robots.

Como se ha podido comprobar en el capítulo anterior, desde una resolución del Parlamento hasta la elaboración de un reglamento definitivo por la Comisión pasan meses o años de dictámenes, consultas e informes que llevan a una versión definitiva distinta en numerosos aspectos de la propuesta inicial. Esta realidad se agudiza en este caso, ya que

[37] NAVARRO (2021) *Op.cit.,*. p. 231

[38] Nótese que se hace referencia a la responsabilidad del fabricante y el formador y no del usuario. Esto es así porque no existe una regulación específica sobre la responsabilidad del usuario en materia de IA, si bien puede extenderse a este lo dicho en ese capítulo respecto de los fabricantes y formadores como lo dicho respecto de conducta diligente o el nexo causal entre la conducta del usuario y el daño a un tercero.

el Parlamento subraya la necesidad de que cualquier regulación futura de responsabilidad en materia de IA debe someterse a la consulta de los Estados miembros y a un debate público de los distintos sectores afectados[39]. Como consecuencia, la versión preliminar estará sujeta a numerosos cambios hasta que la versión definitiva vea la luz. No obstante, en lugar de un análisis exhaustivo de la Resolución analizando todos sus elementos, resulta de gran interés analizar el enfoque híbrido basado en el riesgo, pues es de esperar que el enfoque del reglamento definitivo sea similar.

En primer lugar, el Parlamento reconoce la necesidad de actualizar la Directiva para adaptarla al mundo digital, sin ser necesaria una revisión completa del sistema de responsabilidad civil. En esta línea, declara que el reglamento de responsabilidad en materia de IA será un complemento a la Directiva, estableciendo un orden de prelación entre ambos.[40]

Respecto al régimen de responsabilidad, el Parlamento propone al "operador" como sujeto civilmente responsable. El operador es todo aquel sujeto que pueda haber ejercido un grado de control sobre un riesgo del sistema de IA, entendiendo como control cualquier tipo de influencia en el comportamiento del sistema que pueda conllevar un riesgo. Estableciendo la posibilidad de que haya múltiples operadores, esta categoría incluye a todos los sujetos potencialmente responsables mencionados en el apartado anterior, pues incluye al fabricante, al formador ("*afirma que por «operador inicial» debe entenderse la persona física o jurídica que […], proporciona datos*"[41]) y al usuario (*"Si un usuario, es decir, la persona que utiliza el sistema de IA, está involucrado en el incidente que causa el daño, solo debe ser considerado responsable en virtud del presente Reglamento si el usuario también tiene la condición de operador*"[42]).

A partir del concepto de operador, el Parlamento propone un enfoque de responsabilidad híbrido que se fundamenta en el riesgo. De esta manera, se distinguen dos regímenes de responsabilidad según el sistema de IA de que se trate: modelo objetivo para los sistemas de IA de alto riesgo y modelo subjetivo para los sistemas restantes.

---

[39] Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial, p.4.

[40] El considerando 10 de la Propuesta de Reglamento establece que, cuando un fabricante tenga la consideración común de "operador inicial" a efectos del Reglamento y "productor" a efectos de la Directiva, debe prevalecer esta última, salvo que el fabricante sea el único operador, momento en el cual prevalecerá el Reglamento

[41] *Ibid*, p. 8

[42] *Ibid*, p. 18

Según la propuesta, debido al peligro que presentan los sistemas de IA de alto riesgo, es razonable establecer un régimen de responsabilidad objetiva para todos los operadores de este tipo de sistemas. De esta manera, solamente la fuerza mayor será causa de exoneración de responsabilidad para estos sujetos, no bastando la simple muestra de diligencia para no responder por los daños causados en los que se demuestre el nexo causal entre el daño y el control ejercido por el operador.

Por otra parte, para los sistemas restantes se atribuye un régimen de responsabilidad subjetiva, pero se incluye un matiz relevante: la presunción *iuris tantum* de culpabilidad del operador. Por lo tanto, se invierte la carga de la prueba para los daños producidos por sistemas de IA, siendo el operador quien debe probar su falta de culpabilidad, demostrando que desempeñó un comportamiento diligente ante el riesgo que implicaba su actuación.

Se puede apreciar cómo el Parlamento respeta el equilibrio entre la potenciación de la innovación en materia de IA y la seguridad de los ciudadanos respecto a estos sistemas. Mediante este enfoque híbrido, se prioriza la seguridad ciudadana en los sistemas que más daño puedan causar, mientras que en aquellos en los que se considera que el riesgo es aceptable, se promocionan la inversión y la innovación mediante el modelo subjetivo que permite evitar el pago de indemnizaciones mediante la prueba de diligencia.

Puesto que el factor determinante para la atribución de responsabilidad es el tipo de sistema que produce el daño, resulta esencial para el Parlamento establecer requisitos objetivos para determinar si un sistema de IA es de alto riesgo, así como un anexo detallado donde se enumeren los sistemas considerados como tales, anexo que debe poder ser revisado. En la práctica, lo más probable es que se utilice como referencia el listado de sistemas de alto riesgo que recoge la Ley de IA.

Como último elemento destacado de la propuesta, se menciona en reiteradas ocasiones la falta de personalidad jurídica de los sistemas de IA. Cabe recordar que es el propio Parlamento quien abre la puerta a una personalidad jurídica de los robots en su Resolución de 16 de febrero de 2017[43]. Sin embargo, tras años de recomendaciones, dictámenes y numerosos tratados doctrinales cambia el rumbo en esta materia, negando – de momento – la personalidad jurídica de robots y sistemas de IA.

[43] *Op.cit.*, p.17

Este asunto ha dado lugar a una gran variedad de artículos de revistas, capítulos de libros y discusiones doctrinales en los que se ha debatido sobre la posibilidad de personificar jurídicamente a los sistemas de IA. Entre los que se muestran a favor de establecer esta nueva categoría jurídica hay diversidad tanto en el término –la Resolución del Parlamento Europeo de 16 de febrero de 2017 propone una persona electrónica, mientras que ERCILLA GARCÍA[44] habla de una persona ciber-física– como en la forma de articularse.

De esta manera, NÚÑEZ ZORRILLA[45] defiende la creación de una nueva categoría de "cosa personificada", completamente distinta de los seres humanos. En otra línea distinta, NAVARRO MENDIZÁBAL se acerca más a la futura persona jurídica propia del robot, afirmando que "*es completamente factible que según avance el nivel de sofisticación de los robots pueda llegarse a un estatuto jurídico del robot"*[46]. Sin embargo, como explica a lo largo del capítulo, este estatuto jurídico deberá ir ligado a una serie de derechos y obligaciones que puedan ser ejercitados por el propio robot. En la actualidad, el ordenamiento jurídico reconoce situaciones jurídicas con una naturaleza distinta a las de las personas que son reguladas, tales como el medioambiente –sin tener personalidad jurídica, hay numeras normas que lo protegen – o los animales – están protegidos también por una gran variedad de normas, pero no tienen personalidad jurídica en sí a pesar de tener autonomía y capacidad de decisión –, por lo que en el ordenamiento actual los robots pueden ser regulados de una forma propia, pero sin llegar a tener una personalidad jurídica similar a la de los hombres.

Sin embargo, la mayor parte de la doctrina está en contra de esta personificación jurídica de los robots y sistemas de IA[47]. La razón principal la expone SUÑÉ LLINAS[48], catedrático de Derecho Informático y de Filosofía Jurídica y Política por la Universidad Complutense de Madrid, cuando expone que dotar de personalidad jurídica a los sistemas

[44] (2018). Aproximación a una persona jurídica específica para los robots. *Revista Aranzadi de Derecho y nuevas tecnologías,* núm. 47, p.8

[45] (2018) Los nuevos retos de la Unión Europea en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial. *Revista española de Derecho europeo,* núm. 66, p. 14.

[46] *Op.cit.*, p. 227

[47] Junto con los autores mencionados, un ejemplo de gran oposición a la creación de cualquier tipo de personalidad jurídica para los robots es la *Carta abierta a la Comisión Europea sobre Inteligencia Artificial*, firmada actualmente por 285 expertos en la materia de 14 Estados miembros diferentes. En dicha carta se afirma que la creación de esta categoría se basa en una sobreestimación de las aptitudes reales de los sistemas de IA y que no hay ninguna categoría jurídica actual a la que asemejar la nueva. La carta se puede consultar en: http://www.robotics-openletter.eu/

[48] *Op.cit.*, p. 117.

de IA es simplemente un medio para poder imputarles la responsabilidad civil, exonerando de responsabilidad a los fabricantes y desarrolladores a través del nuevo responsable ficticio. No obstante, no niega la posibilidad futura donde se regulen realmente unos derechos y obligaciones, pero dadas las características actuales de los sistemas de IA, dotarles de personalidad jurídica sería únicamente un medio para los fabricantes de eludir responder por sus errores[49]. Con este mismo razonamiento, ANGUITA RÍOS[50] defiende que estaríamos ante una categoría jurídica creada con una finalidad evidentemente instrumental, añadiendo que la posibilidad de un seguro obligatorio no suple la función de patrimonio con el que responder.

En vista de lo anterior, el pronóstico general – tanto desde la doctrina como desde la legislación – es que estamos lejos de una personalización jurídica de los robots y de los sistemas de IA, ya que otorgar personalidad jurídica a un sistema de IA no puede ir únicamente encaminado a la imputación de responsabilidad. Como defiende BALKIN,[51] profesor de Derecho Constitucional en la Facultad de Derecho de Yale, para poder hablar de la persona electrónica (o cualquier otra denominación), debemos tratar a los sistemas como entidades autoconscientes titulares de derechos y obligaciones, y todavía nos encontramos lejos de esa situación.

[49] Esta postura es compartida incluso por autores que admiten la posibilidad de una regulación futura, como es NAVARRO MENDIZÁBAL.
[50] *Op.cit.*, p. 2560
[51] (2015). "The Path of Robotics Law". *California Law Review, Forthcoming Yale Law School*, 2015, Vol. 6, p. 46.

CAPÍTULO III: PROTECCIÓN ANTE LAS DECISIONES AUTOMATIZADAS: LA ELABORACIÓN DE PERFILES

1. LOS RIESGOS DE LAS DECISIONES AUTOMATIZADAS

Una de las principales preocupaciones de los organismos reguladores en materia de IA es lograr una confianza real en estos sistemas por parte de los ciudadanos europeos[52]. Esta confianza opera en una doble vía: confianza en la tecnología – baja probabilidad de fallo – y confianza en el ordenamiento jurídico – protección ante un posible daño y posibilidad de ser indemnizado en caso de sufrirlo –. En lo referente a esta segunda confianza, la posibilidad de ser indemnizado se ha tratado ya en los capítulos anteriores, explicando las propuestas realizadas sobre la responsabilidad civil de los sistemas de IA. Sin embargo, la sociedad necesita sentirse protegida también *ex ante*, con la seguridad de que el Estado (o la Unión) toma las medidas necesarias para no solamente resarcir el daño, sino también evitarlo.

Es este razonamiento el que lleva a sancionar a un conductor cuando conduce sin cinturón o bajo los efectos del alcohol, sin la necesidad de haber producido ningún daño, simplemente por el peligro que supone para la vida, propia y ajena. Llevándonos este concepto a los sistemas de IA, el tratamiento automatizado de datos personales genera un miedo especial debido a tres factores: la ignorancia sobre el funcionamiento de estos complejos sistemas, el desconocimiento sobre los mecanismos de protección jurídicos que poseemos y la conciencia de que las grandes empresas fuerzan permanentemente los límites legales y éticos para adquirir la mayor información posible para mejorar sus modelos de predicción[53].

Dentro de los principales daños que se puede sufrir como consecuencia de una decisión automatizada, la doctrina y la legislación se han centrado en dos derechos especialmente vulnerables: la protección de datos y la no discriminación. La Resolución del Parlamento Europeo de 16 de febrero de 2017[54] y la Ley de IA[55] reconocen estos dos derechos como merecedores de especial protección en materia de IA. Por su parte, los

[52] Véase el propio título del Libro Blanco sobre IA de la Comisión de 19 de febrero de 2020: un enfoque europeo orientado a la excelencia y la confianza.
[53] MANHEIM y KAPLAN (2018), Artificial Intelligence: Risks to Privacy and Democracy. 21 Yale Journal of Law and Technology 106 (2019), Loyola Law School, Los Angeles Legal Studies Research Paper No. 2018-37. P.14
[54] *Op.cit.*, p.8
[55] *Op.cit.*, Expositivo 3.5, p. 12

profesores de la Universidad Loyola Marymount, MANHEIM y KAPLAN[56], explican los riesgos que presenta el desarrollo de la IA, identificando como especial amenaza los ataques a la privacidad y protección de datos, así como la discriminación por los algoritmos de los sistemas.

El derecho a la protección de datos es el derecho que tiene toda persona física por el cual puede para disponer y controlar sus datos de carácter personal, pudiendo decidir cuáles proporcionar a terceros, así como conocer quién posee esos datos y para qué, y oponerse a esa posesión o tratamiento[57]. Las facultades que se desprenden de este derecho son los derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y de no ser objeto de decisiones individualizadas.[58] Por tanto, este derecho será violado cuando se disponga de los datos personales de una persona física sin su consentimiento o sus causas recogidas por el RGPD.[59] Por su parte, el derecho a la no discriminación viene recogido en el artículo 14 de la Constitución Española, prohibiéndose cualquier discriminación por razones personales tales como el nacimiento, la raza, el sexo o la religión.

Si bien el riesgo de que estos daños sean atacados está siempre patente, aumenta en la medida que un sistema de IA desarrolla su automatización y autoaprendizaje, puesto que los robots carecen de una ética o conciencia de legalidad más allá de los límites que se le indique en el código que no deben traspasar[60].

En el caso de la no discriminación, recuerda BURNS[61] en una conferencia en el MIT sobre la IA el caso en el que el algoritmo de clasificación de Google Photos, después de su aprendizaje automático, clasificó a dos afroamericanos como gorilas. Por parte de la protección de datos, el caso de Cambridge Analytica que terminó influyendo en las elecciones americanas hizo visible el control que tienen empresas como Facebook sobre nuestros datos y, por tanto, sobre nuestro comportamiento[62]. En este caso particular

[56] *Op.cit*., p.4
[57] Diccionario panhispánico del español jurídico
[58] AEPD (2021). *Ejerce tus derechos*
[59] Además de las causas de legitimidad del tratamiento, el RGPD recoge requisitos sobre la finalidad del tratamiento y las garantías, así como sobre formalidades que deben cumplirse.
[60] Este es uno de los argumentos que utiliza SUÑÉ LLINAS para oponerse a la creación de una personalidad jurídica a los robots que se ha explicado en el capítulo anterior
[61] (2018): *El estado actual de la IA no es bien entendido por el público.*
[62] WOOLLACOTT, E. "Facebook Fined $645,150 Over Cambridge Analytica Scandal - And Is Told It's Getting Off Lightly", Forbes, 25 de octubre de 2018. (Disponible en: https://www.forbes.com/sites/emmawoollacott/2018/10/25/facebook-fined-645150-over-cambridge-analytica-scandal-and-is-told-its-getting-off-lightly/?sh=319d7b392c34. Último acceso: 09/06/2022)

Facebook fue sancionada por su conducta irregular, pero no resulta difícil imaginar un sistema de IA al que se le introduce un objetivo de maximizar beneficios y, teniendo capacidad de decisión, termina ofreciendo datos personales al mejor postor.

A pesar de ser dos tipos de daños distintos, tienen en común un factor, el tratamiento automatizado de datos personales aumenta su riesgo. Bien sea porque todo sistema cuenta con sesgos que pueden llevar a discriminación[63] o por la falta de conciencia de legalidad de un algoritmo, una mayor automatización de los sistemas incrementa el peligro de que ambos derechos sean vulnerados.

2. PROTECCIÓN ANTE EL TRATAMIENTO AUTOMATIZADO: ELABORACIÓN DE PERFILES

El tratamiento automatizado de datos tiene especial utilidad en la elaboración de perfiles. El artículo 4.4 del RGPD define la elaboración de perfiles como "*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física"*.

Por tanto, la elaboración de perfiles consiste en utilizar los algoritmos de los sistemas de IA, junto con la información que aportan las personas a internet (búsquedas, creación de usuarios de redes sociales, publicaciones, entre otros) y de esta manera categorizarlas y agruparlas, parametrizando sus comportamientos y pudiendo predecir sus acciones futuras. Esta elaboración de perfiles es tan esencial debido a que la principal fuente de ingresos de las mayores plataformas de internet es la publicidad[64] y esta labor de predicción permite adaptar la publicidad de manera más personalizada.

La manera en la que se gestionan los datos personales o los efectos de categorizar y agrupar de tal manera que haya productos que solamente se ofrezcan a personas con determinadas características hacen factible una publicidad que discrimine y/o vulnere la protección de datos. Frente a este peligro, el marco de protección europeo actual es principalmente el RGPD, apoyado por la nueva Ley de Servicios Digitales (DSA), cuya

[63] BAEZA-YATES (2018), "Bias on the Web", *Communications of the ACM*. Vol. 61. p. 54.
[64] A modo de ejemplo, Facebook ingresó en 2020 28.007 millones de dólares. El 97,08% de estos ingresos procedían de publicidad. Más información en: https://cincodias.elpais.com/cincodias/2021/01/27/companias/1611782581_730013.html

propuesta presentó la Comisión el 15 de febrero de 2020 y ha logrado un consenso con el Parlamento Europeo en 2022, por lo que está a la espera de aprobación formal para ser efectiva en la Unión[65].

2.1. RGPD

El RGPD protege a los ciudadanos europeos del tratamiento automatizado de sus datos personales mediante el artículo 22, que tiene la siguiente redacción:

"Artículo 22 Decisiones individuales automatizadas, incluida la elaboración de perfiles.

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado."

[65] Comunicado de prensa del Consejo de la UE (2022): Ley de Servicios Digitales: acuerdo provisional del Consejo y el Parlamento Europeo para hacer de internet un espacio más seguro para los ciudadanos europeos. https://www.consilium.europa.eu/es/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/

Este artículo configura la principal protección frente al riesgo de vulneración de los derechos de protección de datos y privacidad por parte de los sistemas de IA autónomos, mediante la prohibición de la elaboración de perfiles por decisiones únicamente automatizadas que produzcan efectos jurídicos. Estos elementos han sido objeto de discusión doctrinal, como explica CERRILLO I MARTÍNEZ[66], pues la redacción del artículo permite distintas interpretaciones.

En primer lugar, cabe reflexionar sobre si se está ante una prohibición o ante un derecho de oposición del usuario, quien se tiene que negar explícitamente a que sus datos sean tratados por decisiones automatizadas. Debido a la redacción del artículo, ambas opciones son comprensibles. De hecho, mientras GIL GONZÁLEZ[67] opina que supone un derecho de oposición solamente ejercitable a opción del interesado, el Grupo de Trabajo del artículo 29 ha interpretado que constituye una prohibición, independientemente de cualquier actuación por parte del interesado.[68]

Una vez establecida la prohibición, no toda elaboración de perfiles está prohibida, sino que hay tres presupuestos de aplicación para que aplique: decisión individual, únicamente automatizada y que cause al individuo efectos jurídicos o le afecte significativamente de modo similar.

El primer elemento esencial es ser una elaboración individualizada, de tal manera que pueda afectar a un individuo concreto (quien puede ser discriminado por razón de sexo, raza, creencias religiosas, etc.). Como señalan los profesores de las universidades de Newcastle y University College London, EDWARDS Y VEALE[69], el RGPD habla siempre de individuos y no de tratamiento de datos de grupos o discriminación de grupos. Sin embargo, una decisión automatizada individual no implica que sea única, por lo que se puede comprender que el tratamiento automatizado de datos individuales repetido en numerosos sujetos, constituyendo estos un grupo, se encuentra bajo el amparo de este artículo.

---

[66] (2020). *Retos jurídicos de la Inteligencia. Artificial.*

[67] (2017) Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional. *Revista española de la transparencia, nº5 Segundo Semestre 2017. p. 177*

[68] (2018) *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*. p. 21. El Grupo de Trabajo del artículo 29 ha sido sustituido por el Comité Europeo de Protección de Datos a raíz del RGPD.

[69] (2018). Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'*? IEEE Security & Privacy*, 2018, Vol. 16. Nº 3, p. 51,

Respecto a que la decisión sea "únicamente" automatizada, destaca CERRILLO I MARTÍNEZ[70] cómo se trata de evitar este artículo mediante una apariencia formal de intervención humana. Para que un tratamiento quede excluido de la aplicación de este artículo no basta con una mera supervisión, sino con una intervención real en el proceso decisorio, no estando en manos del algoritmo la elaboración del perfil, sino tomando parte un ser humano a la hora de categorizar.

En cuanto al efecto jurídico o la afectación similar, el RGPD ofrece dos conceptos de insuficiente claridad para poder determinar cuándo es aplicable esta prohibición. A pesar de los ejemplos que ofrece en el considerando 71[71], no resulta evidente cuándo una decisión afecta "significativamente" a un sujeto. Puede deducirse que aquellos casos en los que la decisión tenga impacto en la situación financiera o laboral del interesado estaremos ante un efecto significativo. No obstante, el efecto concreto dependerá de las características de cada individuo, como afirman MENDOZA y BYGRAVE[72], por lo que se deberá hacer un estudio *ad casum* sobre la significación o relevancia del efecto.

Una vez determinados los presupuestos de aplicación, una elaboración de perfil puede estar excluida de la prohibición si se da alguna de las causas del artículo 22.2: es necesario para la celebración de un contrato, está amparado bajo leyes estatales o europeas, o el interesado ha dado su consentimiento expreso. En el caso de que se trate de datos especialmente sensibles (datos relativos a la raza, salud, orientación sexual, ideología, etc.), solamente se levantará la prohibición si el interesado presta su consentimiento expreso o si hay una razón de interés público que lo permita.

Sin embargo, la exención de la prohibición no implica una desprotección total para el ciudadano europeo, pues el RGPD impone la obligación al responsable del tratamiento de tomar medidas para salvaguardar los intereses legítimos del interesado, señalando como intereses mínimos a respetar los derechos a obtener intervención humana, a poder opinar sobre el tratamiento y a impugnar la decisión automatizada. Estos intereses legítimos han sido objeto de interpretación y discusión doctrinal, en especial si dentro de este concepto jurídico indeterminado se incluye el derecho a la explicación y el contenido de este.

---

[70] *Op.cit.*, p. 4

[71] Brinda como ejemplos la denegación automática de créditos *online* y los servicios de contratación electrónica.

[72] (2017)., The Right Not to Be Subject to Automated Decisions Based on Profiling. *University of Oslo Faculty of Law Research Paper* No. 2017-20, p. 12.

Respecto a si el artículo 22.3 reconoce implícitamente el derecho a la explicación, la duda surge debido a que este derecho está reconocido en el considerando 71. No obstante, como recuerda el TJUE[73], un considerando tiene carácter de norma, sino que sirve como herramienta de interpretación de las normas. Partiendo de esta afirmación, hay autores como los profesores de las facultades de derecho de UCLA y UWA, SELBST y POWLES[74] que defienden que hacer una interpretación sistemática de los artículos 13, 14 y 15 (derechos de información) junto con el considerando 71 y el artículo 22.3 implica reconocer el derecho de explicación como incorporado implícitamente en el artículo 22.3. En cambio, los profesores de Oxford WATCHER et al.[75] afirman que la omisión del derecho a la explicación en el artículo 22.3 es intencionada, por lo que niegan el reconocimiento de este derecho.

Finalmente, en cuanto al contenido concreto del derecho a la explicación, la finalidad de este derecho es la comprensión del interesado de cómo han sido tratados sus datos personales. Esta comprensión presenta varias dificultades, puesto que una explicación que consista en mostrar el código chocaría con la propiedad intelectual y el secreto comercial del responsable del tratamiento, además de no lograr – probablemente – la comprensión del interesado, debido a su falta de conocimientos algorítmicos.

Por tanto, la explicación debe consistir en que el interesado entienda el proceso decisorio del algoritmo respecto de sus datos, sin necesidad de revelar información respecto del código o del sistema de IA. De esta manera, como explica PALMA ORTIGOSA[76], el responsable del tratamiento debe explicar, en la medida de lo posible, el funcionamiento del programa informático, aportando información útil para el interesado – como por ejemplo los factores que más han influido en la elaboración del perfil – que le permita comprender el proceso y pueda así ejercer el resto de los derechos que le reconoce el RGPD en su artículo 22.3.

[73] STJUE (Sala Tercera) de 13 de julio de 1989, Asunto 215/88. (FJ 31).
[74] (2017): "Meaningful information and the right to explanation". *International Data Privacy Law, 2017*, Vol. 7, No. 4, pág.236.
[75] (2017) *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation* International Data Privacy Law, 2017. p. 80.
[76] (2019). Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos. *Revista General de Derecho Administrativo*. Nº 50 Enero 2019 p. 28

2.2. DSA

En palabras de MONJAS GONZÁLEZ[77], la DSA supone "*definir un marco horizontal de derechos y obligaciones para los prestadores de servicios de intermediación (intermediarios), especialmente las plataformas en línea, que proporcione certeza jurídica a las empresas y refuerce la protección de los ciudadanos y sus derechos*."

La DSA supone otro avance en el camino regulatorio de la UE para proteger a los ciudadanos europeos mientras se favorece la innovación. Esta propuesta de Reglamento, igual que el RGPD o la Ley de IA, obliga a todo aquel que preste servicios digitales de intermediación en territorio de la Unión, independientemente de su residencia, favoreciendo así una mayor confianza.

En lo que afecta al tratamiento automatizado de datos y a la elaboración de perfiles, la DSA impone, en su artículo 29, a las plataformas de muy gran tamaño (VLOP) la obligación de exponer de manera "clara, accesible y fácil de comprender" los parámetros y atributos que han sido utilizados a la hora de realizar la recomendación.

Adicionalmente, el texto incluye que las VLOP deben ofrecer distintos tipos de sistemas de recomendación a elección del destinatario, debiendo ser, al menos uno de ellos, una opción que no incluya una elaboración de perfiles. De esta manera, se protege en mayor medida al ciudadano europeo frente al tratamiento de sus datos personales de manera automatizada por parte de las grandes plataformas.

[77] (2022). Relevancia del reglamento de ley de servicios digitales para las autoridades reguladoras del audiovisual. *Información Comercial Española, ICE: Revista de economía*, Nº 925, p. 54

CONCLUSIONES

La evolución del panorama normativo europeo en materia de IA durante los últimos años es digna de reconocimiento. Se ha considerado realmente una prioridad en la agenda de los organismos regulatorios y se han puesto los medios para conseguir un marco que favorezca la inversión en IA y que simultáneamente inspire confianza y seguridad a los ciudadanos europeos.

No obstante, el camino no está terminado. No solamente porque la mayoría de reglamentos están en fase de propuesta, sino porque para lograr esa confianza resulta necesario concretar los requisitos de transparencia de los sistemas de IA. Si bien se ha logrado – en opinión de este trabajo – un sistema de responsabilidad civil mediante el enfoque híbrido basado en el riesgo que permite al ciudadano europeo saber a quién dirigirse ante un posible daño, son todavía de gran desconocimiento los daños concretos que pueden causar un tratamiento automatizado, o manual pero inadecuado, de los datos personales.

En numerosos documentos consultados para la realización de este trabajo se menciona en repetidas ocasiones la necesidad de transparencia, pero rara vez se concretan medios para lograr esa transparencia. Hay diversas propuestas en el aire, tales como la inclusión de una "caja negra" en los algoritmos que recoja los cálculos matemáticos realizados[78] o el nombramiento de auditores de algoritmos que puedan preservar el secreto a la vez que comprobar el respeto de los intereses legítimos[79], pero falta todavía algún estándar de transparencia o requisitos comunes a todos los sistemas que permitan saber de manera cierta a los fabricantes qué información deben mostrar y a los ciudadanos qué pueden llegar a conocer.

Este es el último paso que dar para lograr una confianza real en los sistemas de IA: una transparencia que permita al ciudadano conocer el tratamiento que se realiza de sus datos personales, siendo consciente de los factores que más influyen a la hora de realizar perfiles para así poder él mismo controlar – en cierta medida – el uso que se hace de su información.

[78] Resolución del Parlamento Europeo, de 16 de febrero de 2017… *Op.cit.,* p.8
[79] CERRILLO I MARTÍNEZ, *op.cit.,* p. 14

Sería interesante una futura investigación que ahonde en el problema de la falta de transparencia de los sistemas de IA, especialmente en aquellos que cuentan con algoritmos opacos como las redes neuronales, pues si bien la dificultad de mostrar el tratamiento de datos sin perder ventajas comerciales es evidente, resulta indispensable para el ciudadano saber que sus datos no son tratados de manera inexplicable, sino que detrás de los anuncios y las recomendaciones que recibe hay un razonamiento lógico comprensible que respeta los límites legales y no infringe sus derechos.

BIBLIOGRAFÍA

LEGISLACIÓN

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan Coordinado sobre la inteligencia artificial. COM(2018) 795.

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Inteligencia artificial para Europa. COM(2018) 237

Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos.

Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza. COM(2020) 65

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE. 2020/0361(COD)

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el período 2021-2027. 2018/0227(COD)

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea el Programa Marco de Investigación e Innovación «Horizonte Europa» y se establecen sus normas de participación y difusión. 2018/0224(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. 2021/0106(COD)

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

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)

Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)).

Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia artificial. (2020/2014(INL))

JURISPRUDENCIA

Sentencia del Tribunal de Justicia de la Unión Europea (Sala Tercera) de 13 de julio de 1989, Asunto 215/88. https://eur-lex.europa.eu/resource.html?uri=cellar:bff0427d-b75d-46bf-8015-7eeddf6f9ca8.0008.06/DOC_2&format=PDF

OBRAS DOCTRINALES

ABBOTT, R. B., "The Reasonable Robot: Artificial Intelligence and the Law" (Excerpt) *Cambridge University Press.* (2020).

ANGUITA RÍOS, R.., "Inteligencia artificial y Derecho civil: líneas de pensamiento en materia de daños", *Revista Crítica de Derecho Inmobiliario,* N.º 781 (2020), pp. 2541 - 2581.

BAEZA-YATES, R., Bias on the Web. *Communications of the ACM* . Volume 61. 2018. Pp. 54–61

BALKIN, J. M., "The Path of Robotics Law". *California Law Review, Forthcoming Yale Law School*, 2015, Vol. 6, pp. 45-61.

CERRILLO I MARTÍNEZ, A., [et al.], ANGLÉS JUANPERE, B., & PEGUERA POCH, M., *Retos jurídicos de la Inteligencia Artificial* (1ª ed.). 2020. Navarra: Aranzadi.

DÍAZ ALABART, S. (2018). *Robots y Responsabilidad civil*. Madrid: Reus.

ERCILLA GARCÍA, J. (2018). *Normas de Derecho civil y robótica. Robots inteligentes, personalidad jurídica, responsabilidad civil y regulación*. Pamplona: Aranzadi Thomson Reuters.

ERCILLA GARCÍA, J. (2018). Aproximación a una persona jurídica específica para los robots. *Revista Aranzadi de Derecho y nuevas tecnologías,* núm. 47. Pamplona: Aranzadi Thomson Reuters

EDWARDS, L. & VEALE, M., "Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'?" *IEEE Security & Privacy,* vol. 16. Nº. 3, 2018, pp. 46-54.

GARCÍA GARCÍA, S. (2022), Una aproximación a la futura regulación de la inteligencia artificial en la Unión Europea, *Revista de Estudios Europeos,* volumen 79, enero-junio 2022. pp. 304-323.

GIL GONZÁLEZ, E., "Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional". *Revista española de la transparencia,* nº5 Segundo Semestre 2017. pp. 165-179.

GÓMEZ-RIESCO TABERNERO DE PAZ, J., BARRIO ANDRÉS, M. (Dir.) (2018). *Los robots y la responsabilidad civil extracontractual en Derecho de los robots*, La Ley Wolters Kluwer, Madrid.

MANHEIM, K. M., & KAPLAN, L., "Artificial Intelligence: Risks to Privacy and Democracy". *21 Yale Journal of Law and Technology 106*, vol. 21, 2019, pp. 106-189.

MENDOZA, I. & BYGRAVE, L.A., "The Right Not to Be Subject to Automated Decisions Based on Profiling". *University of Oslo Faculty of Law Research Paper* No. 2017-20. pp.1-23.

MONJAS GONZÁLEZ, S., "Relevancia del reglamento de ley de servicios digitales para las autoridades reguladoras del audiovisual". *Información Comercial Española, ICE: Revista de economía*, Nº 925, 2022 pp. 53-65.

NAVARRO MENDIZÁBAL, I. (2021). *La responsabilidad civil en tiempos de IA y los Robots* en LLEDÓ YAGÜE, F., BENÍTEZ ORTÚZAR, I., & MONJE

BALMASEDA, O. (dirs.) La Robótica y la inteligencia artificial en la nueva revolución industrial 4.0. Madrid: Dykinson, pp. 197-238.

NÚÑEZ ZORRILLA, M.C. (2019). *Inteligencia artificial y responsabilidad civil.* Madrid: Reus.

NÚÑEZ ZORRILLA, M.C. (2018) Los nuevos retos de la Unión Europea en la regulación de la responsabilidad civil por los daños causados por la inteligencia artificial. *Revista española de Derecho europeo,* núm. 66. pp. 1-38.

PALMA ORTIGOSA, A. "Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos." *Revista General de Derecho Administrativo.* Nº 50 Enero 2019.

SELBST, A. D & POWLES, J.,: "Meaningful information and the right to explanation". *International Data Privacy Law*, Vol. 7, No. 4, 2017, pp. 233-242.

SUÑÉ LLINÁS, E (2020). *Derecho e Inteligencia Artificial.* Tirant lo Blanc, Ciudad de México

WACHTER, S., MITTELSTADT, B. & FLORIDI, L.*, "*Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law,* 2017.

RECURSOS DE INTERNET

AEPD (2021). *Ejerce tus derechos.* https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos

ASIMOV, I. (1942), Círculo Vicioso. *Astounding science fiction, March 1942.* https://inteligenciaeducativa.net/descargas/runaround.pdf

ASOCIACIÓN DE CONSUMIDORES EUROPEOS (2021). EU proposal for artificial intelligence law is weak on consumer protection. *BEUC.* https://www.beuc.eu/publications/eu-proposal-artificial-intelligence-law-weak-consumer-protection/html

BAYÓN, A. & JIMÉNEZ, M. "Facebook gana 24.000 millones en 2020, un 58% más, y valida su apuesta por el 'ecommerce'". *Cinco Días. El País Economía*, 27 de enero de 2021. (Disponible en*:* https://cincodias.elpais.com/cincodias/2021/01/27/companias/1611782581_7300

13.html#:~:text=El%20beneficio%20de%20la%20compa%C3%B1%C3%ADa,)%2C%20un%2058%25%20m%C3%A1s. Última consulta: 05/06/2022)

BBC Mundo, "Tay, la robot racista y xenófoba de Microsoft". *BBC*, 25 de marzo de 2016. (Disponible en: https://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb. Último acceso: 01/06/2022)

BEST, J., "IBM Watson: The inside story of how the Jeoparty-winning supercomputer was born, and what it wants to do next." *TechRepublic*. (Disponible en: https://www.techrepublic.com/article/ibm-watson-the-inside-story-of-how-the-jeopardy-winning-supercomputer-was-born-and-what-it-wants-to-do-next/. Último acceso: 03/06/2022)

BURNS, E., "El estado actual de la IA no es bien entendido por el público". *Tech Target.* (Disponible en: https://www.techtarget.com/searchenterpriseai/opinion/Current-state-of-AI-is-poorly-understood-by-the-public. Último acceso: 03/06/2022)

COMISIÓN EUROPEA, DIRECCIÓN GENERAL DE REDES DE COMUNICACIÓN, CONTENIDO Y TECNOLOGÍAS, "Directrices éticas para una IA fiable," Oficina de Publicaciones. (Disponible en: https://data.europa.eu/doi/10.2759/14078. Último acceso: 02/06/2022)

COMISIÓN EUROPEA, DIRECCIÓN GENERAL DE JUSTICIA Y CONSUMIDORES, "Liability for artificial intelligence and other emerging digital technologies", *Publications Office.* (Disponible en: https://data.europa.eu/doi/10.2838/573689. Último acceso: 01/06/2022)

COMISIÓN EUROPEA. *Normas sobre la inteligencia artificial: preguntas y respuestas*. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/qanda_21_1683. Último acceso: 22/05/2022

CONSEJO DE LA UNIÓN EUROPEA, "Ley de Servicios Digitales: acuerdo provisional del Consejo y el Parlamento Europeo para hacer de internet un espacio más seguro para los ciudadanos europeos". *Comunicados de prensa del Consejo de la UE*. (Disponible en: https://www.consilium.europa.eu/es/press/press-

releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space/. Último acceso: 07/06/2022)

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 (2018), *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*. Adoptadas el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018.

LÓPEZ BARAJAS, G., "Una regulación europea de la Inteligencia Artificial adecuada y sin fronteras". *Telefónica blog,* 2021. (Disponible en: https://www.telefonica.com/es/sala-comunicacion/blog/una-regulacion-europea-de-la-inteligencia-artificial-adecuada-y-sin-fronteras/. Último acceso: 23/05/2022)

LÓPEZ BARAJAS, G., PIAZZA, A. & SASTRE, A., "Claves de la nueva regulación europea de Inteligencia Artificial". *Telefónica blog,* 2021. (Disponible en:. https://www.telefonica.com/es/sala-comunicacion/blog/claves-de-la-nueva-regulacion-europea-de-inteligencia-artificial/. Último acceso: 21/05/2022)

MADRICAL, A.C., "IBM'S Watson Memorized the Entire 'Urban Dictionary', Then His Overlords Had to Delete It." *The Atlantic,* 2013. Disponible en: https://www.theatlantic.com/technology/archive/2013/01/ibms-watson-memorized-the-entire-urban-dictionary-then-his-overlords-had-to-delete-it/267047/. Último acceso: 01/06/2022)

MORGADO, C. & ESTEBAN, A., "Propuesta de reglamento de la UE sobre inteligencia artificial". *Cuatrecasas: Blog de Propiedad Intelectual y Tecnologías,* 2021. (Disponible en: https://www.cuatrecasas.com/es/spain/articulo/propuesta-reglamento-ue-inteligencia-artificial. Último acceso: 27/05/2022)

MURILLO, J. (2020) "What should be taken into account if Artificial Intelligence is to be regulate?" *Finextra,* 2021. (Disponible en: https://www.finextra.com/the-long-read/62/what-should-be-taken-into-account-if-artificial-intelligence-is-to-be-regulated . Último acceso: 20/05/2022)

ORTEGA, A. "Hacia un régimen europeo de control de la Inteligencia Artificial". *Real Instituto Elcano.* (Disponible en: https://www.realinstitutoelcano.org/analisis/hacia-un-regimen-europeo-de-control-de-la-inteligencia-artificial/. Último acceso: 29/05/2022).

SENDÍN, J., Decisiones individuales automatizadas y elaboración de perfiles. *Sistemius*. (Disponible en: https://www.sistemius.com/decisiones-individuales-automatizadas-elaboracion-perfiles/ . Último acceso: 30/05/2022)

WOOLLACOTT, E. "Facebook Fined $645,150 Over Cambridge Analytica Scandal - And Is Told It's Getting Off Lightly", *Forbes*, 25 de octubre de 2018. (Disponible en: https://www.forbes.com/sites/emmawoollacott/2018/10/25/facebook-fined-645150-over-cambridge-analytica-scandal-and-is-told-its-getting-off-lightly/?sh=319d7b392c34. Último acceso: 09/06/2022)