Universidad de Oviedo
*Universidá d'Uviéu*
*University of Oviedo*

# Centro Internacional de Postgrado

MASTER UNIVERSITARIO EN ABOGACÍA

# TRABAJO FIN DE MASTER

EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO INTERNACIONAL PRIVADO

Alumno: Ana María López Ormazabal

Convocatoria: Enero 2023

## RESUMEN

¿De qué hablamos cuando nos referimos a la Inteligencia Artificial? ¿Qué es un *"Smart Contract"*? ¿En qué consiste la Tecnología *"Blockchain"*? ¿Cuál es el impacto de todo ello en el ámbito del Derecho Internacional Privado? ¿Son suficientes y efectivas las normas existentes para abordar las cuestiones que de todo ello se derivan o, por el contrario, se necesita un nuevo marco legal para abordarlas? Si por algo se caracteriza el Derecho es por tratar de aportar soluciones a los problemas que se plantean en el día a día práctico de los distintos operadores jurídicos, así como de la propia doctrina jurídica. Sin embargo, sabido es que el primer paso para poder resolver un conflicto es la búsqueda misma del problema. Por ello, con este trabajo lo que me he propuesto es abordar las implicaciones de las interrogaciones antes anunciadas en el ámbito de este concreto sector del Derecho Privado desde un punto de vista crítico y teniendo presente el elemento de la novedad de la temática a tratar.

## ABSTRACT

What do we talk about when we talk about Artificial Intelligence? What is a *"Smart Contract"*? What does *"Blockchain Technology"* consist about*?* What kind of impact does it have in the Private International Law field? Are the existing regulations sufficient and effective to adress the issues arising from all this or is a new legal framework needed to deal with them? If the Law is characterized by something, it is by trying to provide solutions to the problems that arise in the practical day-to-day of the different legal operators, as well as the legal doctrine itself. However, it is known that the first step in resolving a conflict is the search for the problem itself. For this reason, with this research what I have proposed is to address the implications of the previously announced questions in the field of this specific sector of Private Law from a critical point of view and bearing in mind the element of novelty of the subject to be treated.

## ABREVIATURAS Y ACRÓNIMOS

Art ..... Artículo
CE ..... Constitución Española de 1978
Comunicaciones máquina a máquina ..... m2m
Dirección IP ..... Dirección del Protocolo de Internet
EM ..... Estado Miembro
Inteligencia Artificial ..... IA
Internet de las Cosas ..... IoT
LOPJ ..... Ley Orgánica del Poder Judicial
OCDE ..... Organización para la Cooperación y Desarrollo Económico
RGPD ..... Reglamento General de Protección de Datos
STJCE ..... Sentencia del Tribunal de Justicia de la Unión Europea
TJUE ..... Tribunal de Justicia de la Unión Europea
UE ..... Unión Europea
UNESCO ..... Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

# ÍNDICE

# 1.- INTRODUCCIÓN

La gran protagonista en la actualidad es la denominada "*Industria 4.0*", la cual está integrada por el Internet de las Cosas (IoT), las comunicaciones máquina a máquina (m2m), la robótica, el Big Data y, fundamentalmente, la Inteligencia Artificial (IA). El resultado de todo lo anterior se conoce como la Artificial Invention Age o Cuarta Revolución Industrial.

El objeto del presente trabajo no es otro que el análisis del impacto de esta tecnología en el Derecho, concretamente, en el Derecho Internacional Privado por la importancia que este novedoso tema está alcanzando y por las salidas profesionales que se están desarrollando en consecuencia en el mundo de la abogacía.

La metodología seguida a la hora de la realización de este estudio no ha sido otra que el planteamiento de los problemas principales en base a la distinta normativa y jurisprudencia existente.

Dichos problemas los he enunciado en cada uno de los apartados del trabajo, los cuales, a continuación, paso a analizar.

# 2.- APROXIMACIÓN A LA INTELIGENCIA ARTIFICIAL

## 2.1.- EL CONCEPTO DE INTELIGENCIA ARTIFICIAL

*"Hoy, quien programa, potencialmente legisla"*, decía Lawrence Lessing en su obra "The Code version 2.0". A mi juicio, no le falta razón alguna. El mundo de la programación ha traído de la mano a la famosa IA. El primer objetivo en este punto será el alcance de una definición de dicho término ya que, pese a que existen múltiples, ninguna de ellas es uniforme.

Remontándonos atrás en el tiempo, la primera vez que el término "Inteligencia Artificial" fue empleado, tuvo lugar en la conferencia realizada en Darmouth (USA) 1956 por John McCarthy, Marvin Minsky, Nathaniel Rochester y Claude Shannon, los cuales se refirieron a ella como *"la ciencia y la ingeniería de fabricar máquinas inteligentes, en especial máquinas inteligentes de computación"* y especificaron que destacan entre las características principales de la IA: la computación, el procesamiento del lenguaje natural, las redes neuronales, la teoría de la computación, la capacidad de mejora, la formación de abstracciones, la aleatoriedad y la creatividad.

Debemos partir de la idea de que la IA no posee la capacidad de comprender como si puede hacer un cerebro humano. Lo que si puede llevar a cabo es modificar su propio *status quo* y desarrollar acciones de forma automática. Por ello y, acuñando un poco más el término, señala Benedetta Capiello que el propio concepto se refiere más a la idea de automatización que a objetos específicos. Es decir, los algoritmos una vez que se incluyen en el *software* pueden ejecutar la acción. Pero ese resultado, al que podemos referirnos siguiendo la explicación de dicho autor como "salidas", depende de las "entradas", es decir, de las órdenes iniciales con las que se hayan programado a dicho algoritmo. Podríamos decir que se trata de un mecanismo de reglas encadenadas, o, lo que es lo mismo, que el algoritmo en sí no posee inteligencia. Es la encadenación de algoritmos la que produce IA.

A su vez, la consecución de la salida en función de la entrada depende de si el sistema se desarrolla siguiendo o bien un enfoque simbólico o bien un enfoque conexionista. En el caso de los algoritmos tradicionales o enfoques simbólicos las instrucciones se las da de forma anticipada el desarrollador al algoritmo, sin embargo, en el caso de los conexionistas, éstos aprenden las instrucciones mediante datos conocidos como datos de alineación.

Con base en la explicación anterior quizás pueda parecernos más precisa la definición aportada por el informe elaborado por el Parlamento Europeo sobre IA que se refiere a ésta como *"todo sistema basado en programas informáticos o incorporado en dispositivos físicos que muestra un comportamiento que simula la inteligencia, entre otras cosas, mediante la recopilación y el tratamiento de datos, el análisis y la interpretación de su entorno y la adopción de medidas, con cierto grado de autonomía, para lograr objetivos específicos".* A su vez, entiende por "autónomo", lo siguiente: *"todo sistema de IA que funciona interpretando determinados datos de entrada y utilizando un conjunto de instrucciones predeterminadas, sin limitarse a ellas, a pesar de que el comportamiento del sistema esté limitado y orientado a cumplir el objetivo que se le haya asignado y otras decisiones pertinentes de diseño tomadas por su desarrollador".*

Algunos autores, la definen como *"término que 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"*.

El primero de los problemas tanto jurídico-teórico como jurídico-práctico que plantea la falta de una definición universal no es otro que, siguiendo el razonamiento del profesor Antonio Merchán[1], la complejidad que supone alcanzar una legislación uniforme si ni siquiera hay una definición común de lo que se pretende regular.

De hecho, ni las propias instituciones se ponen de acuerdo en ofrecer una definición común.

Así pues, mientras que para la Comisión Europea se utiliza el término IA para referirse a aquellos sistemas que se comportan de forma inteligente y son capaces de estudiar su entorno y actuar con el objetivo último de alcanzar fines específicos, para el Consejo de Europa el mismo término se corresponde con aquellas *"aplicaciones que, a menudo, mediante técnicas de optimización matemática, realizan una o más tareas como recopilar, combinar, limpiar, ordenar, clasificar e inferir datos, así como la selección, priorización, elaboración de recomendaciones y la toma de decisiones. Basándose en uno o más algoritmos para cumplir con sus requisitos en los entornos en los que se aplican, los sistemas algorítmicos automatizan las actividades de una manera que permite la creación de servicios adaptables a escala y en tiempo real"*.

La UNESCO define los sistemas de IA como *"tecnologías de procesamiento de la información que incorporan modelos y algoritmos que producen una capacidad para aprender y realizar tareas cognitivas, dando lugar a resultados como la predicción y la adopción de decisiones en entornos reales y virtuales. Los sistemas de IA están diseñados para funcionar con una cierta autonomía, mediante la modelización y representación del conocimiento y la explotación de datos y el cálculo de correlaciones".*

A su vez debemos tener presente que es realmente difícil definir algo que permanece en constante cambio. Es por ello que el Libro Blanco de la UE sobre IA que sigue las Directrices para una IA fiable del Grupo de Expertos de Alto Nivel, observa que *"en cualquier nuevo instrumento legal, la definición de la IA deberá ser lo*

[1] Antonio Merchán Murillo *"Identidad Digital Blockchain e Inteligencia Artidicial: aspectos jurídicos de presente y futuro a debate".* Vol 7. Núm 1 (2021). El jurista en la era Digital: Inteligencia Artificial, Robótica, Tecnologías Anexas y bioderecho.

*suficientemente flexible para adaptarse al progreso técnico y al mismo tiempo ser lo suficientemente precisa para proporcionar la seguridad jurídica necesaria"*.

Es por ello que se ha llegado a sugerir el uso del término *"toma de decisiones automatizadas"* en lugar del término IA ya que así se evitaría la ambigüedad de la definición.

A lo largo del presente estudio nos iremos aproximando a estos conceptos con objeto de hacer un planteamiento de los principales problemas que presentan y cuáles son sus consecuencias jurídicas.

## 2.2.- FINALIDAD Y ÁMBITO DE APLICACIÓN DE LA PROPUESTA DE REGLAMENTO POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL

El 21 de abril de 2021 la Comisión Europea presentaba la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial que, tal y como la propia Comisión lo ha presentado estaríamos ante *"el primer marco jurídico sobre la IA de la historia".* La finalidad de la nueva normativa en esta materia es triple.

En primer lugar, el desarrollo de la nueva legislación tiene por objeto aprovechar los potenciales beneficios y oportunidades que la IA puede generar no ya sólo a nivel europeo sino a nivel mundial.

En segundo lugar, protegerse frente a los peligros que esta tecnología puede generar. Así pues, ha sido la propia Comisión Europea la que ha puesto algunos ejemplos de éstos, siendo uno de ellos *"la opacidad de muchos algoritmos"*, la cual puede generar incertidumbre y dificultar la efectiva aplicación de la legislación en vigor sobre seguridad y derechos fundamentales. Con ello lo que se pretende es asegurar que el mercado interior de los sistemas de IA funciona adecuadamente, así como llevar a cabo una ponderación adecuada de beneficios y de riesgos. Y es que, si se dejase que cada autoridad nacional estableciese sus propias respuestas reglamentarias al respecto, se generaría un riesgo potencialmente superior de que dicho mercado se fragmentase.

En tercer lugar y, como último fin que podríamos considerar como el fundamento de los demás se encuentra la protección de los derechos fundamentales y la seguridad de los usuarios para generar confianza en el desarrollo y la adopción de este nuevo y prometedor ámbito, tratando de evitar la inseguridad jurídica para las empresas, así

como también la lenta adopción de la IA tanto por éstas como por ciudadanos, precisamente por una falta de confianza en aquélla.

Garantizando la seguridad de los usuarios existirá una mayor demanda de IA por parte de empresas y autoridades públicas y ello tendrá como consecuencia que los proveedores de IA podrán entrar en mercados mayores.

En lo que al ámbito de aplicación se refiere, puede resumirse en el siguiente:

El Reglamento tendrá un carácter horizontal puesto que no se aplicará a un número limitado de sectores, resultará aplicable a agentes ya sean estos públicos o privados y bien se encuentren dentro como fuera de la UE siempre que el sistema de IA se encuentre introducido en el mercado de la UE o su uso pueda afectar a personas tanto físicas como jurídicas que se encuentren en espacio de la UE. Es, de nuevo, la propia Comisión Europea la que pone algunos ejemplos a este respecto. En este sentido nos explica que puede afectar a proveedores, como, por ejemplo, "*un programador de una herramienta de evaluación de resúmenes curriculares*". También puede afectar a los usuarios de sistemas de IA de alto riesgo, como, por ejemplo, "*un banco que compre esa herramienta*". Tan importante es llegados a este punto conocer el ámbito de aplicación, como, su vertiente negativa, es decir, debemos saber quiénes quedan excluidos de la aplicación del Reglamento. Y es que este marco jurídico no se aplicará a los usos privados que no tengan el carácter de profesionales. A lo largo de esta exposición he mencionado lo que la normativa denomina "*riesgos*". Pues bien, debemos saber que la legislación se ha planteado en base al riesgo y ha establecido una clasificación que engloba cuatro niveles del mismo. Se trata de lo que algunos autores[2] denominan *"principio de gestión del riesgo",* que consiste en que cuanto mayor es el riesgo, más estricta debe ser la regulación que lo contemple. Antes de proceder a examinar estos cuatro estadios, la pregunta que nos puede surgir llegados a este punto es ¿de qué depende la clasificación del riesgo? Y la respuesta no es otra que de la función que lleve a cabo el sistema de IA y de su finalidad, así como de las modalidades específicas para las que se pueda usar ese concreto sistema. Pero, ¿existen criterios de clasificación? Sí. La propia Comisión pone de manifiesto algunos de ellos como, por ejemplo, el uso de la aplicación de IA y su finalidad prevista, el número de

[2] GARCÍA SAN JOSÉ, D. (2021). "Implicaciones jurídicas y bioéticas de la inteligencia artificial (IA). Especial consideración al marco normativo internacional". *CUADERNOS DE DERECHO TRANSNACIONAL*, *13*(1), 255-276. https://doi.org/10.20318/cdt.2021.5959

personas potencialmente afectadas, la dependencia en lo que al resultado se refiere, la irreversibilidad de los daños o cómo la legislación de la UE establece medidas eficaces para minimizar dichos riesgos de forma sustancial. Centrándonos ya en la clasificación propiamente dicha, la cual consta de cuatro categorías, a saber:

1) **Riesgo inadmisible.**
2) **Alto riesgo.**
3) **Riesgo limitado.**
4) **Riesgo mínimo.**

- Como anticipaba, en primer lugar, se encuentra el **"*Riesgo Inadmisible*"** el cual se regula en el Título II y, consiste, fundamentalmente, en que habrá un conjunto verdaderamente limitado de usos que pueden ser muy nocivos de la IA y que pueden contravenir los valores de la UE poniendo en riesgo a los derechos fundamentales. De nuevo la Comisión Europea nos pone varios ejemplos al respecto, pudiendo pensar en "*una puntuación social por parte de los Gobiernos, una explotación de los puntos débiles de los niños, el uso de técnicas subliminales, y salvo contadas excepciones, determinados sistemas de identificación biométrica remota en directo en espacios públicos con fines policiales*". Pues bien, lo que sucederá con este tipo de usos será que se prohibirá tanto su introducción en el mercado de la UE como su puesta en servicio y su propio uso.
- En segundo lugar, en el Título III, se encuentra la categoría de **"*Alto Riesgo*",** debiendo entenderse por el mismo a un número reducido de sistemas de IA que pueden impactar negativamente tanto en la seguridad de los ciudadanos como en los derechos fundamentales que les están atribuidos por la Carta de los Derechos Fundamentales de la UE. Este tipo de sistemas se permitirán en la UE, pero tendrán que cumplir una serie de requisitos que examinaremos posteriormente, así como someterse a una evaluación de conformidad previamente a ser introducidos en el mercado y con carácter previo a su puesta en servicio y uso. Para facilitar la delimitación de estos sistemas se ha adjuntado a la propuesta una lista que tiene la característica de ser adaptable en función de la evolución de los usos de la IA y que tendrá en cuenta las pruebas y los dictámenes de expertos y se mantendrá en consulta con los interesados. Esto pone de manifiesto que la UE quiere seguir un método

adecuado que pueda ayudar a detectar sistemas de IA de alto riesgo de una forma más sencilla contribuyendo a asegurar ese objetivo último. Algunos ejemplos de estos usos son: los componentes de seguridad de los productos que se encuentran en la legislación sectorial de la UE, que pertenecerán siempre a esta categoría si están sujetos a una evaluación de su conformidad por terceros en relación con esa legislación sectorial. Otro rasgo esencial de este tipo de riesgos es que en la normativa se hace una propuesta sobre requisitos obligatorios que éstos deben acatar y que engolaban lo referente a la calidad de los conjuntos de los datos que se utilizan, la documentación técnica y la obligación de registro (arts. 11 y 12), la transparencia y la divulgación de información a los usuarios (art. 13), la supervisión humana de la IA (art. 14), la solidez, la precisión y la ciberseguridad (art. 15). Como garantía adicional se establece la posibilidad conferida a las autoridades nacionales de poder acceder a aquella información que sea necesaria para poder descubrir si el uso de la IA cumplió o no la normativa en aquellos casos de infracción. Es importante destacar llegados a este punto que, a los proveedores de sistemas de IA de alto riesgo se les imponen una serie de obligaciones. De este modo, con carácter previo a la comercialización de estos sistemas en el mercado de la UE o de su puesta en servicio de cualquier otra forma, éstos deberán someterlos a una evaluación de conformidad lo cual permitirá hacer comprobar si su sistema cumple con los requisitos obligatorios de lo que se denomina "*una IA digna de confianza*". También se prevé que el sistema o su finalidad puedan sufrir un cambio sustancial, en cuyo caso, la evaluación deberá repetirse. En algunos casos deberá participar en este proceso un organismo notificado independiente. Siempre tendrán, así mismo, el elemento de alto riesgo, por un lado, los sistemas de IA que integren componentes de seguridad de productos que se observen en la legislación sectorial de la UE, así como los sistemas de identificación biométrica, en ambos casos, cuando necesiten una evaluación de conformidad por terceros. En lo relativo al momento posterior a la comercialización de sistemas de alto riesgo, se establecerán unas autoridades de vigilancia del mercado cuya misión principal será apoyar este seguimiento posterior, teniendo como recursos, entre otros, las auditorías o la posibilidad de ofrecer a los proveedores notificar

incidencias graves o supuestos de quebrantamiento de los derechos fundamentales.

- En tercer lugar, se establece la categoría de **"*Riesgo Limitado*"**, donde se encuentran algunos sistemas de IA con obligaciones particulares en materia de transparencia a los proveedores de los mismos y a los propios usuarios para evitar que puedan manipular los sistemas de IA. Éstos se regulan en el Título IV de la Propuesta. El ejemplo que ofrece la Comisión en este caso es "*cuando exista un riesgo claro de manipulación, por ejemplo, mediante el uso de robots conversacionales, los usuarios deben ser conscientes de que están interactuando con una máquina*".
- Finalmente, el último grado de esta categoría se corresponde con el **"*Riesgo mínimo*"**, que es aquél que engloba a los sistemas de IA que se pueden generar y utilizar con sujeción a la legislación vigente sin que se le impongan cargas jurídicas extra. Es decir, serán todos aquellos que no se incluyan en ninguna de las tres categorías que acabamos de analizar. La mayor parte de los sistemas que a día de hoy se utilizan en la UE se encuentran aquí clasificados, razón por la que, con carácter voluntario, aquellos que provean estos sistemas se pueden decantar por aplicar los requisitos de una IA de riesgo mayor y adherirse a códigos de conducta voluntarios con el objeto de asegurar una mayor confianza (Título IX). Los códigos de conducta voluntarios son, por tanto, aquellos mecanismos que permitirán a los proveedores de aplicaciones de alto riesgo asegurar la confianza de su sistema e implican una manifestación de *soft law* frente al *hard law* que hemos visto que se aplica a las otras modalidades de riesgos. La normativa se ha encargado también de asegurar el cumplimiento de todo lo anterior, siendo el elemento esencial en este punto, el papel que jugarán los EM ya que cada uno de ellos tendrá que establecer una o varias autoridades nacionales competentes para vigilar la aplicación y la ejecución, así como el propio mercado. Así mismo cada EM tendrá la obligación de establecer una autoridad nacional de supervisión, la cual llevará a cabo también la representación de dicho Estado ante el Comité Europeo de IA o también denominado "*European Artificial Intelligence Board*", el cual está integrado por representantes de alto nivel de las autoridades nacionales de supervisión competentes, el Supervisor Europeo de Protección de Datos y la Comisión. Su objetivo será conseguir una aplicación fluida, eficaz y

armonizada de este nuevo Reglamento sobre IA. Para ello, el Comité le realizará recomendaciones y dictámenes sobre sistemas de IA de alto riesgo y sobre todas aquellas cuestiones relativas a la aplicación eficaz y uniforme de la nueva normativa. Permitirá también la consulta por parte de las autoridades nacionales sobre conocimientos especializados en materia de IA. Además, también apoyará las actividades de normalización en la materia. Su función, por tanto, será, fundamentalmente, coordinar a las diferentes autoridades de control de los EM. Dispone el art. 63.4 de la Propuesta que en aquellos casos en los que los sistemas de IA sean empleados por entidades financieras la supervisión corresponderá a una autoridad de supervisión del propio ámbito financiero. Otra medida impuesta para asegurar el cumplimiento será que las importaciones de sistemas y aplicaciones de IA tendrán que cumplir la normativa, de modo que los importadores de estos sistemas tendrán que hacer una comprobación relativa a que el proveedor extranjero haya cubierto todo el procedimiento de evaluación de la conformidad necesaria y que cuente con la documentación técnica que exige el Reglamento. También se les impondrá a éstos la obligación de comprobar que su sistema lleve un marcado europeo de conformidad (CE) y se incluya la documentación e instrucciones de uso que se necesiten. No podemos dejar de mencionar el Nuevo Reglamento sobre máquinas debido a su estrecha relación con la IA ya que el mismo pretende que las máquinas contribuyan también a asegurar la seguridad de los usuarios y, por tanto, se aumente la innovación. Dentro de estas máquinas podemos mencionar, entre otras, robots, cortadoras de césped, impresoras 3D, máquinas de construcción… Son Reglamentos que se complementan ya que mientras el Reglamento sobre IA se ocupa de los riesgos para la seguridad de los sistemas de IA, el Reglamento sobre máquinas garantiza la integración segura del sistema de IA en la maquinaria para que no se ponga en riesgo la seguridad de la máquina. En conclusión, la idea a destacar fundamentalmente es que la UE pretende con todo ello convertirse en líder a nivel mundial en lo que al fomento de la IA digna de confianza se refiere. Teniendo en cuenta que la regulación de la IA es algo totalmente novedoso pretende fomentar la adopción de normas mundiales en armonía con el sistema multilateral en base a las normas y los valores que promulga. Por ello la UE pretende llevar a cabo asociaciones, coaliciones y alianzas con países como Japón, Estados Unidos o India, con la

OCDE y el G-20 o con organizaciones regionales como pueda ser el Consejo de Europa.

En lo referente a la entrada en vigor y aplicación de esta norma, tendrá lugar a partir de abril de 2023.

A modo de conclusión final y enlazando con el epígrafe posterior, me gustaría hacer alusión a una cuestión pautada por el profesor Pedro A. De Miguel Asensio[3] que es la siguiente: a diferencia de lo que ocurre en el RGPD, esta Propuesta de Reglamento no dispone nada sobre los supuestos de indemnizaciones en aquellos casos en los que los sistemas de IA vulneren la normativa. Tal vez la razón sea que la Comisión prefiere reservar esta cuestión par el instrumento que, a continuación, pasamos a analizar.

## 2.3.- FINALIDAD Y ÁMBITO DE APLICACIÓN DE LA PROPUESTA DE REGLAMENTO EUROPEO SOBRE RESPONSABILIDAD CIVIL DERIVADA DE LA INTELIGENCIA ARTIFICIAL.

Para entender mejor los objetivos de la UE en este ámbito debemos partir de una idea base la cual es el principio que da lugar a toda la teoría de la responsabilidad civil que no es otro que el aforismo latino "*neminen laedere*" o la obligación de requilibrar la situación (generalmente mediante una compensación económica) cuando una parte le genera un daño a otra ya sea por acción o por omisión y con o sin culpa.

Desde los inicios de los sistemas de responsabilidad civil los diferentes ordenamientos jurídicos de los Estados han tratado la cuestión en base a su propio Derecho sustantivo de formas muy diversas pasando por diversas soluciones en función del momento histórico (desde sistemas de culpabilidad a sistemas de responsabilidad objetiva, por ejemplo).

¿Cuál es el actual objetivo? La armonización de las diferentes legislaciones sustantivas europeas en materia de responsabilidad extracontractual derivada de los sistemas de IA. En este punto es fundamental el papel que juega el Derecho Internacional Privado si tenemos presente que el problema fundamental será el surgimiento del denominado "*conflicto de leyes*" que tiene lugar cuando el supuesto del que se derive la

[3] P. A. DE MIGUEL ASENSIO "Propuesta de reglamento sobre Inteligencia Artificial" *La Ley Unión Europea*, número 92, mayo 2021.

responsabilidad mantenga relaciones relevantes con los derechos sustantivos de dos o más Estados.

El 20 de octubre de 2020 se aprobó por el Parlamento Europeo una Resolución en la que se establecían normas sobre Responsabilidad Civil, denominada "*Civil liabillity regime for artificial intelligence*", cuyo objetivo es la plena armonización y su instrumento el Reglamento mediante el cual se logre una legislación uniforme para todos los Estados Miembros, pero sin modificar completamente los regímenes de responsabilidad de la UE y de las legislaciones internas de cada Estado Miembro.

En un primer acercamiento al nuevo sistema de Responsabilidad Civil debemos tener presente su ámbito de aplicación espacial, a saber, en lo relativo al mismo dispone el artículo 2 del Reglamento que se aplicará en el territorio de la Unión Europea cuando una actividad física o virtual, dispositivo o proceso impulsado por un sistema de IA cause un daño a la vida, a la salud, a la integridad física, o, a los bienes de una persona física o jurídica. Por lo tanto, lo relevante en este punto es que el daño tenga lugar en territorio de la Unión Eurpea, siendo irrelevante que el productor o el fabricante sean ajenos al territorio de la Unión en este aspecto, o que la víctima no sea ciudadana de un Estado Miembro bastando con que se encuentre en alguna parte del territorio perteneciente a la Unión Europea. El eurodiputado alemán Axel Voss, comentó que el objetivo de la Propuesta al establecer este ámbito de aplicación espacial es generar confianza al proteger a los ciudadanos, sean o no éstos de la Unión Europea.

En lo que se refiere al ámbito de aplicación subjetivo, éste, engloba, fundamentalmente dos sujetos, a saber, el *"operador inicial"* y el *"operador final"*.

Antes de definir a estos dos sujetos debemos saber a qué se refiere el Reglamento con el término "*operador*", lo cual no es tarea sencilla. La responsabilidad del operador se deriva, ya sea éste inicial o final, de la creación o introducción de un peligro para los usuarios. El operador será, por tanto, el que controle el riesgo que se derive de los sistemas de Inteligencia Artificial y, si éstos causan daños, deberá responder por ello. Entrando ya en el análisis de los dos sujetos citados, siguiendo a la profesora Pilar Álvarez Olalla[4], podemos definir al "*Operador Final*" como la *"persona física o*

[4] ÁLVAREZ OLALLA, M. P. (2021). "Propuesta de Reglamento en materia de responsabilidad civil por el uso de inteligencia artificial, del Parlamento Europeo, de 20 de octubre de 2020". *Revista CESCO De Derecho De Consumo*, (38), 1-10.

*jurídica que ejerce un grado de control sobre un riesgo asociado a la operación y el funcionamiento de un sistema de IA, y que se beneficia de su funcionamiento".* Y al "*Operador Inicial*" como *"persona física o jurídica que define, de forma continuada, las características de la tecnología, proporciona unos datos y un servicio de apoyo final de base esencial y, por tanto, ejerce también un grado de control sobre el riesgo asociado a la operación y el funcionamiento del sistema (suministrando programas informáticos, suministrando datos de tráfico en un sistema de navegación, o suministrando programas de entrenamiento en un reloj inteligente, por ej.). Todo ello siendo ejercicio del control cualquier acción del operador que influya en el funcionamiento del sistema de IA".* Así mismo debemos tener presente que si el "operador inicial", a su vez, es productor conforme a la Directiva de productos defectuosos, la Propuesta dispone que se le aplique con carácter preferente dicha Directiva.

Finalmente debe tenerse en cuenta el sistema de responsabilidad subjetiva introducido por la Propuesta en el sentido de que si el usuario es "*operador final*" podrá ser responsable, pero, de lo contrario, sólo respondería por uso negligente o doloso frente a terceros.

La pregunta que nos puede surgir llegados a este punto es ¿qué pasa si los daños son causados por un tercero? En dicha tesitura, se aplicaría la normativa sobre responsabilidad subjetiva de cada Estado Miembro.

Respecto al concepto de "*dañado*", sería la persona física o jurídica que sufre el daño.

Centrándonos ya en lo que al sistema de responsabilidad civil establecido por la propuesta se refiere debemos saber, en primer lugar, que se trata de un sistema imperativo dado que operador y dañado no pueden realizar pacto en contrario y si lo hicieren el mismo sería nulo de pleno derecho. En segundo lugar, se establecen dos grandes tipos de responsabilidad en función de dos grandes tipos de sistemas de riesgo. El art. 3 de la Propuesta consagra lo que denomina "*Sistemas de Alto Riesgo*", para los cuales establece un sistema de Responsabilidad Objetiva en el art. 4.1, según el cual cualquier operador de este tipo de sistemas responderá objetivamente de los daños que cause la actividad bien física o bien virtual de los dispositivos o procesos gobernados por dicho sistema, con lo que la prueba de haber operado conforme a las reglas de la debida diligencia o que el daño fue consecuencia de la propia autonomía del sistema

de IA no serán causa de exoneración de dicha responsabilidad, a diferencia de la fuerza mayor y la culpa exclusiva de la víctima.

Estos sistemas son aquellos *"sistemas de inteligencia artificial que funcionan de forma autónoma con un potencial significativo para causar daños o perjuicios a una o más personas de manera aleatoria, quizás desconocidas e indeterminadas, y que exceden de lo que cabe esperar razonablemente. El potencial será significativo teniendo en cuenta la relación entre la gravedad del posible daño o perjuicio, el grado de autonomía en la toma de decisiones, la probabilidad de que el riesgo se materialice y el modo y contexto en que se utiliza el sistema de IA".* Dispone el art. 4.5 que este sistema de responsabilidad imperará sobre los que tenga establecidos cada Estado Miembro.

La lista de daños indemnizables a consecuencia del uso de Sistemas de Alto Riesgo queda reducida a la siguiente:

- Daño corporal. Consiste fundamentalmente en lo relativo al daño emergente y el lucro cesante a consecuencia o bien del fallecimiento o bien de los daños que se generen a la salud y a la integridad física, siendo su límite máximo indemnizable de dos millones de euros.
- Daños materiales y morales que determinen daño económico calculado con la media de sus ingresos. El límite en este caso será de un millón de euros. Es importante recalcar que estos límites funcionarán también cuando sean varios los perjudicados, de manera que a cada uno no se otorgará dicha cantidad, sino que se repartirá entre todos ellos de forma proporcional al daño que hayan sufrido.

La Propuesta diseña un plazo de prescripción de treinta años, que empezará a computarse a partir de la fecha de producción del daño si se da fallecimiento o daño a la salud.

Sin embargo, para los daños materiales o morales con perjuicio económico indemnizables se diseña un plazo de prescripción de diez años desde que se causó el menoscabo a los bienes o el perjuicio económico o treinta años desde la operación de IA que generó el daño. Se deberá optar de entre estos dos, por el plazo de anterior vencimiento. Por su parte el art. 7.3 deja a salvo la suspensión e interrupción de dichos plazos que pueda estar prevista en cada legislación interna. El art. 4.4 establece la

obligación para todo operador de Sistema de Alto Riesgo de contratar un seguro de responsabilidad civil. Como ya adelantábamos, respecto a todos aquellos sistemas que no tengan la cualidad de Alto Riesgo, se aplica tal y como dispone el art. 8.1 un sistema de responsabilidad subjetiva "*respecto de todo daño o perjuicio causado por la actividad física o virtual del sistema*". Además, concreta el punto dos que no se responderá cuando "*se pueda demostrar que no tuvo culpa en el daño o perjuicio causado*".

Para poder exonerarse tendrán que cumplirse los siguientes requisitos concretos:

- El sistema de IA se activó sin conocimiento del operador cuando éste ya había adoptado todas las medidas razónales para que no se activase.
- El operador actuó con la diligencia exigible ya que:
    - O seleccionó un sistema de IA adecuado y debidamente certificado.
    - O puso en funcionamiento el sistema de forma correcta e informó al productor de posibles irregularidades.
    - O controló las actividades y mantuvo la fiabilidad operativa instalando las oportunas actualizaciones.

En este tipo de sistemas en lo que se refiere tanto a los límites máximos indemnizables como a los plazos de prescripción, la Propuesta opta por remitirlo a cada legislación interna.

## 2.4.- LAS PROPUESTAS DE DIRECTIVAS EN EL ÁMBITO DE RESPONSABILIDAD CIVIL DERIVADA DE LA INTELIGENCIA ARTIFICIAL

### 2.4.1.- La Propuesta de Directiva sobre responsabilidad por los daños causados por productos defectuosos

Esta Directiva, de 28 de septiembre de 2022 va ser la que sustituya a la Directiva 85/374 sobre Productos Defectuosos, que incorpora algunos elementos en relación con la Inteligencia Artificial, como pueda ser, la ampliación de la responsabilidad a los productores de sistemas de IA.

La propia Comisión hace referencia a la necesidad de que las reglas sobre responsabilidad civil por productos defectuosos sean actualizadas en base a que se deben modernizar y reforzar las normas ya establecidas, teniendo en cuenta que la anterior Directiva de responsabilidad por productos defectuosos (PLD) se remonta

a 1985, y, no cubre categorías de productos que surgen de las nuevas tecnologías digitales, como los productos inteligentes y la inteligencia artificial (IA). Así pues, la Comisión considera que con la revisión de esta normativa se garantizará que las nuevas normas de responsabilidad por productos defectuosos se adapten a la nueva tipología de productos en pro tanto de las empresas como de los consumidores.

Ahora bien, ¿qué tipo de productos estarán cubiertos por la nueva norma? La variedad abarcada implica tanto desde simples sillas de jardín hasta medicamentos contra el cáncer y, especifica que se incluirán expresamente actualizaciones de software ya que éstas, así como productos que incluyan IA, en caso de resultar defectuosos, pueden causar daños. La Comisión ejemplifica algunos productos en los que podrían detectarse estos errores, como, por ejemplo, robots de limpieza o, incluso, aplicaciones médicas de salud incorporadas en teléfonos inteligentes. La nueva normativa asegura la posibilidad de reclamar compensación si surgen este tipo de daños.

¿Qué se podría reclamar en estos casos según la nueva normativa? La norma hace referencia a que el perjudicado podrá reclamar el daño causado incluyendo éste la lesión personal, las lesiones a bienes de su propiedad, e, incluso, la pérdida de datos.

Hasta ahora hemos visto la vinculación de la norma con lo que se refiere a los daños en el ámbito de la Unión Europea, pero, ¿quién responde por los productos defectuosos fuera del espacio de la Unión?

Hasta ahora lo que permitía la normativa era que el perjudicado reclamase al importador del producto fabricado fuera de la UE. Sin embargo, la actual cadena de valor mundial permite la compra de productos directa fuera de dicho espacio, es decir, sin importador. Por ello, la nueva normativa, permitirá al perjudicado reclamar al representante del fabricante fuera de la UE. Así las cosas, el Reglamento de Vigilancia del Mercado junto con el Reglamento General de Seguridad de los Productos que será próximamente revisado, harán que exista una persona responsable con sede en la UE a la que sea posible reclamar una compensación. ¿Cómo se materializa entonces la reclamación al representante del fabricante fuera de la UE? Sencillamente cuando éste no facilite la identificación del responsable con sede en la UE.

Por último y, analizando más en profundidad la relación de esta nueva Directiva con la propuesta de Reglamento sobre IA, sabemos, que dicha propuesta consagra normas para garantizar que los sistemas de IA cumplan con altos requisitos de seguridad. Pues bien, esta nueva directiva, clarifica que todos los requisitos de seguridad obligatorios deben tenerse en cuenta por el tribunal que vaya a determinar si el producto se considera o no defectuoso. Así mismo, deja claro que tanto el software como los sistemas que incluyen IA se consideran productos. De esta manera si un producto con IA produce un daño, ya sea personal, material o de pérdida de datos la persona perjudicada puede reclamar el daño causado.

A modo de conclusión final la nueva norma garantiza junto con las comentadas anteriormente y la que a continuación paso a explicar que las víctimas se beneficien de la misma protección cuando resulten perjudicadas por productos de IA o cuando sufran daños en cualquier otro tipo de situación.

### 2.4.2.- La propuesta de Directiva sobre responsabilidad civil en materia de IA.

Esta nueva Directiva moderniza el marco de responsabilidad civil de la UE ya que, por primera vez, se introducen reglas específicas para daños causados por sistemas de IA.

De nuevo lo que se consigue es que una víctima que sufra un daño causado por un sistema de IA pueda obtener la reparación del mismo al igual que podría obtenerla si hubiera sufrido daños en cualquier otro tipo de circunstancia.

Para ello la Directiva introduce dos mecanismos principales:

**1)** La denominada "presunción de causalidad" que evitará que el perjudicado deba explicar de forma detallada todo lo relativo a la producción del daño. Es decir, si el perjudicado puede demostrar que el responsable no cumplió una determinada obligación y que existe un vínculo causal entre ello y la producción del daño, el tribunal podrá apreciar que ese incumplimiento ocasionó el daño. Se trata de una presunción iuris tantum ya que el responsable podrá refutarla, por ejemplo, probando que una causa distinta provocó el daño.

**2)** El acceso a la información de empresas o proveedores en los casos de IA catalogadas como sistemas de alto riesgo. Es decir, en este sentido, la propia Comisión pone algunos ejemplos, a saber, si un daño se produce porque un operador de drones que entrega paquetes no respeta las instrucciones de uso del dron las

víctimas podrán acceder a las pruebas de una forma sencilla solicitando al tribunal que ordene la divulgación de información sobre sistemas de IA de alto riesgo. Ello permitirá tal y como explica la Comisión que la víctima identifique a la persona que podría ser considerada responsable y determinar qué fue lo que falló.

¿Cuál es la relación entre esta Directiva y la que acabamos de analizar anteriormente?

La norma que hemos analizado con anterioridad se aplicará a las reclamaciones contra el fabricante por los daños que ocasionen productos defectuosos tales como pérdidas de vidas, daños a la salud, daños a la propiedad o pérdidas de datos. Se limita a reclamaciones que puedan hacer los particulares.

La nueva Directiva de responsabilidad de IA reforma de forma específica los regímenes nacionales de responsabilidad que se basan en la culpa y se aplicará a reclamaciones contra cualquier persona y las reclamaciones podrán hacerlas tanto personas físicas como personas jurídicas.

Por último, ¿cómo se relaciona esta nueva Directiva con la Propuesta de Reglamento sobre IA de 2021? Pues bien, las dos normas se aplican en distintos momentos, pero se refuerzan mutuamente. Es decir, las directivas no reemplazan a los reglamentos, sino que están destinadas a convivir. Mientras que la Ley de AI tiene como objetivo prevenir daños, la Directiva de responsabilidad de AI establece una red de seguridad para la compensación en caso de daños. La Directiva de responsabilidad de IA utiliza las mismas definiciones que la Ley de IA, mantiene la distinción entre IA de alto riesgo/no alto riesgo, reconoce los requisitos de documentación y transparencia de la Ley de IA al hacerlos operativos para la responsabilidad a través del derecho a la divulgación de información e incentiva a los proveedores/usuarios de sistemas de IA a cumplir con sus obligaciones en virtud de la Ley de IA. La Directiva se aplicará a los daños causados por los sistemas de IA, independientemente de si son de alto riesgo o no de acuerdo con la Ley de IA.

En la actualidad no se están introduciendo por la Comisión en estas propuestas de Directivas normas específicas de Derecho Internacional Privado. Pese a ello podríamos llegar a plantearnos si los elementos que introduce y armoniza, como, por ejemplo, el acceso a la información o la prueba de la causalidad se pueden aplicar imperativamente. Si tenemos presente el art. 16 del Reglamento Roma II estas cuestiones serían de aplicación.

Debemos tener presente que cuando estas normas entren en vigor se aplicarán si la norma material concreta que se trate, por ejemplo, el Convenio de la Haya del 71 o el Convenio de la Haya del 73 nos lleva al Derecho material de un determinado Estado Miembro, pues la nueva normativa no desplaza a las normas materiales que ya existían en el marco normativo.

## 3.- EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO INTERNACIONAL PRIVADO DE DAÑOS

Tal y como habíamos anticipado en la introducción de nuestro estudio disponemos de dos tipos de algoritmos que conforman los sistemas de IA, a saber, simbólicos y conexionistas. En esa mecánica de funcionamiento es importante precisar que el desarrollador no desempeña el papel de decirle al algoritmo cómo tiene que comportarse, sino que su misión es enseñarle a aprender utilizando los datos que estén a su disposición y las reglas de probabilidad. Lo que hace el algoritmo a partir de ahí es analizar los ejemplos y decidir distinguir en función de diversos factores unos de otros. Es precisamente esa probabilidad y esa capacidad de decisión del algoritmo lo que rompe la relación de causalidad entre la acción humana, en este caso, el desarrollador del algoritmo y el daño que resulta del funcionamiento del mismo. En definitiva, el software de IA se diseña para que realice una sola función que, con el tiempo, debe mejorar. Pero precisamente en dicha mejora se encuentra el riesgo, pues cualquier mejora supone un cambio en la actividad de aprendizaje y todo cambio supone un riesgo. Siguiendo a Benedetta Capiello[5], existe una imposibilidad técnica, conocida como el fenómeno "*humano fuera del circuito*" o "*problema de la caja negra*" que implica que ni si quiera el desarrollador del algoritmo pueda entender cómo el programa que procesa la información mediante el aprendizaje llegue a una solución particular y no a otra. En conclusión, se están comercializando sistemas de IA que permanecen al margen del control humano. Una posible solución en la que ya se encuentra trabajando actualmente el ejército estadounidense es obtener un sistema híbrido de algoritmos (simbólicos y conexionistas) para superar este problema al que nos hemos referido como "*imposibilidad técnica*", siendo el objetivo de este sistema que los usuarios del mismo puedan entender cómo el algoritmo ha llegado a una conclusión determinada y no a otra.

[5] BENEDETTA CAPIELLO, *AI-systems and non-contractual liability*. *A european private international law analysis.* Giappichelli. 2022.

¿Cuál es la consecuencia jurídica de todo este planteamiento? Si el algoritmo se retroalimenta de su propio aprendizaje hasta el punto que el desarrollador ni si quiera puede comprender cómo el algoritmo toma decisiones, se rompe, como he anticipado, la relación de causalidad, principio fundamental de nuestro actual sistema de responsabilidad civil.

Esa rotura de responsabilidad genera una brecha que sufre la actual legislación y, consecuentemente, el propio usuario del sistema.

Sabido es que la ley debe adaptarse a la realidad cambiante para hacer frente a las nuevas problemáticas que surgen cada día.

Lo que a partir de ahora me propongo analizar es si la velocidad abismal del desarrollo tecnológico unida a la lentitud legislativa está generando un vacío normativo que se debería abordar aportando nuevas normas desde el ámbito del Derecho supranacional o, si, por el contrario, bastaría con darle un nuevo enfoque a la regulación ya existente en la materia.

### 3.1.- INTELIGENCIA ARTIFICIAL Y NORMATIVA SOBRE DAÑOS TRANSFRONTERIZOS

En 1942 Isaac Asimov creó lo que se conoce como las "*leyes de la robótica*" y las enunció del modo que se expone a continuación:

1) Un robot no dañará a un ser humano o, por inacción, permitirá que un humano sufra daño.

2) Un robot obedecerá las órdenes que le sean dadas por los seres humanos, excepto si esas órdenes entran en conflicto con la Primera Ley.

3) Un robot protegerá su propia existencia siempre que dicha protección no entre en conflicto con la Primera o Segunda Ley.

Aunque en un principio pudiera parecernos esto algo más propio de la ciencia ficción que del mundo real, lo cierto es que, con el auge y los avances que se están produciendo en IA cada día está más cerca de la realidad que de la ficción. Tal vez a ninguno de nosotros se nos pudiera ocurrir pensar que unos robots de una gran empresa tienen que ser desconectados por crear un idioma propio que los humanos no son capaces de entender.

Pues bien, esto fue lo que le sucedió a Facebook cuando, el equipo de desarrollo de IA tuvo que desconectar a dos de sus bots los cuáles habían sido desarrollados para que fueran capaces de negociar, cuando, dejaron de emplear el lenguaje con el que habían sido programados y desarrollaron uno propio.

Todos estos sucesos pueden generar daños tanto a objetos como a personas que pueden rebasar fronteras. El Parlamento Europeo, consciente de esta problemática, llegó incluso a proponer en su Resolución de 16 de febrero de 2017 en la que establecía recomendaciones destinadas a la Comisión sobre normas de Derecho civil en relación con la robótica, la creación de una personalidad jurídica específica para los sistemas de IA.

Lo que ahora analizaré es la normativa existente en materia de daños transfronterizos que sería la aplicable para este tipo de supuestos.

Partimos de que se trata de daños de naturaleza extracontractual y comenzamos analizando la competencia judicial internacional.

La perspectiva que me gustaría adoptar y que de hecho adoptaré a lo largo de este análisis consiste, además, en realizar este análisis con un objetivo claro, concluir si la normativa existente a día de hoy es suficiente para hacer frente a la nueva realidad tecnológica y, en caso negativo, si basta con una modificación de la misma o si, por el contrario, se necesitan nuevas leyes para hacer frente a las nuevas realidades.

### 3.1.1.- Competencia Judicial Internacional

Debemos proceder al análisis de la jurisdicción competente, a saber, los tres instrumentos a considerar son:

1) Reglamento UE 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Bruselas I Bis).

2) Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Lugano el 30 de octubre de 2007 (Convenio de Lugano).

3) Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ).

Por su mayor aplicación práctica nos centraremos en el primero de ellos bastando saber que se aplican en base a la cláusula de compatibilidad introducida en el art.

64 del Convenio, que se aplicará si se cumplen los requisitos exigidos en dicha norma y, en caso de no ser así, se aplicaría el Reglamento y si no acudiríamos residualmente a la Ley estatal (LOPJ).

Tal y como dispone el Reglamento Bruselas I Bis en caso de darse una responsabilidad extracontractual serían competentes los siguientes órganos jurisdiccionales:

- Los órganos jurisdiccionales a los que las partes se hubieran sometido de forma expresa o tácita (arts. 25 y 26).
- Los órganos jurisdiccionales del lugar donde el demandado tenga su domicilio (art. 4).
- Los órganos jurisdiccionales del lugar donde se produzca el hecho dañoso (art. 7).

En este sentido debemos hacer no obstante una consideración para la cual debemos tener presente la STJCE de 30 de noviembre de 1976, as. 21/76, Mines de Potasse d´Alsace. En este tipo de supuestos lo que ocurre es que el hecho generador del daño se produce en un país mientras que el resultado dañoso se manifiesta en otro país diferente. En la mencionada sentencia sentaba el TJUE la tesis de la "*ubicuidad*", en virtud de la cual, podrá plantearse la demanda en cualquiera de los dos países, concediéndosele así el denominado por algunos autores, entre los que podemos citar a P. De Miguel Asensio, J.B. Fuentes Mañas… "*Optio fori"*[6].

Pongamos un breve ejemplo al efecto. Pensemos en una máquina que, utilizando IA, emite unos vertidos en Francia y, que, dichos vertidos, causan daños en diversas plantaciones localizadas en Alemania.

En dicho supuesto, los damnificados, a su elección, podrían presentar la demanda tanto en Francia como en Alemania.

¿Cuál es el problema que plantea la teoría de la ubicuidad en relación con los sistemas de IA? En el ejemplo propuesto estamos hablando de lugares concretos, esto es,

[6] P.A. DE MIGUEL ASENSIO, DERECHO PRIVADO DE INTERNET, 4A ED., CIVITAS, MADRID, 2011, PP. 185-204; J.B. FUENTES MAÑAS, «DETERMINACIÓN DE LA COMPETENCIA JUDICIAL INTERNACIONAL EN LOS 'ILÍCITOS A DISTANCIA' SOBRE DERECHOS DE AUTOR EN INTERNET», RCEA, 2003, PP. 119-147.

físicos. Pero la IA plantea un nuevo espacio, un espacio virtual o un *"ciberespacio"*. Si no se puede localizar ni la producción ni el resultado dañoso, ¿dónde debe presentarse la demanda?

Además, también debemos tener presente que puede producirse un daño múltiple, también conocidos como "*daños multilocalizados*" que son aquellos que se encuentran en varios lugares y, como hemos anunciado, ya no sólo físicos sino también virtuales.

El debate en estos supuestos radica en torno a la teoría aplicable.

Esto es, o bien el denominado "*principio del mosaico*" que fue desarrollado por el TJCE en la famosa "*decisión Shevill*" o bien la solución prevista en la "*decisión eDate*". También se ha planteado la posible aplicación simultánea de ambas teorías.

La doctrina alemana se ha referido al citado principio del mosaico como "*Mosaikbetrachtung"*, que en nuestro idioma se traduce como *"vista de mosaico"*. A partir de su desarrollo por el TJCE en la mencionada sentencia, el Tribunal ha tratado esta teoría en otras muchas decisiones, entre las que podemos citar las siguientes: STJCE 30 noviembre 1976, 21/76, *Mines de Potasse*; STJCE 26 marzo 1992, C-261/90, *Dresdner Bank [II]*; STJCE 27 septiembre 1988, 189/87, *Kalfelis*; STJCE 11 enero 1990, C-220/88, *Dumez*; STJCE 7 marzo 1995, C-68/93, *Shevill*; STJCE 19 septiembre 1995, C-364/93, *Marinari*; STJCE 27 octubre 1998, C-351/96, *Réunion*; STJCE 17 septiembre 2002, C-334/00, *Tacconi*; STJCE 1 octubre 2002, C-167/00, *Henkel*; STJCE 5 febrero 2004, C-18/02, *Torline*; STJCE 10 junio 2004, C-168/02, *Kronhofer*.

La idea que podemos extraer de toda esta jurisprudencia es que el objetivo y, de ahí el nombre que se le ha otorgado, es completar un mosaico, es decir, la competencia internacional que ostenta el tribunal del EM en cuyo territorio se ha producido el daño, en base al art. 7.2 del Reglamento Bruselas I Bis sólo alcanzaría a aquella responsabilidad que se derive de los daños producidos en su territorio. Sin embargo, el damnificado deberá presentar demandas en el resto de EM en los que haya sufrido los daños para ver efectivamente reparados los mismos.

Como mencionaba, esta teoría se relaciona con la famosa tesis de la ubicuidad. Que no se trata de otra cosa sino de la respuesta a la pregunta ¿Qué sucede, además, en el

caso de los ilícitos a distancia o cuándo el hecho dañoso se produce en lugar diferente del que se verifica el daño?

La ubicuidad de esta situación ha generado el surgimiento de la conocida como "op*tio fori*", que se recoge en el mencionado precepto y que consiste en que el demandante optará por plantear su demanda o bien en el foro del hecho causal o bien en el foro de verificación de los daños.

Analizada la doctrina sentada en la decisión Shevill, pasamos ahora a observar lo recogido en la decisión eDate, pues aporta el elemento crucial cuando de daños causados por sistemas de IA se trata.

El problema fundamental es como ya anuncié que, aunque el daño se materializa en un espacio físico, el lugar donde haya podido tener lugar el fallo que da lugar al accidente es un espacio que potencialmente, puede todo el territorio mundial, es decir, el ciberespacio es universal. Entonces, en este tipo de supuestos se podría demandar en el lugar donde se produce el daño físico o en el lugar dónde hubiera tenido lugar el error en el sistema de IA, por ejemplo, ubicado en un determinado servidor. Como podemos observar, el nuevo parámetro que añade la IA con respecto a lo que veníamos acostumbrados es, fundamentalmente, el ***proceso de electronificación***. Ello lleva aparejada la creación de la identidad electrónica que, a su vez, nos lleva a la residencia electrónica como posible criterio de conexión a la hora de determinar tanto la competencia como el segundo de los aspectos que analizaremos, esto es, la ley aplicable. Y es que para poder determinar la residencia electrónica es imprescindible esa identidad electrónica a la que nos referimos. La residencia electrónica debe ser un criterio de conexión a tener en cuenta.

### 3.1.2.- Ley aplicable

Analizada la competencia llegamos al segundo gran bloque, que no es otro que el de la ley aplicable.

Por su importancia práctica nos centraremos en el Reglamento (CE) 864/2007 del Parlamento Europeo y del Consejo de 11 de julio de 2007 relativo a la ley aplicable a las obligaciones extracontractuales (Reglamento Roma II).

Dado que se trata de un reglamento de carácter universal tal y como establece en su artículo tercero se aplica siempre con independencia de que la ley designada no sea la de un Estado Miembro.

Los puntos de conexión que establece esta norma son los siguientes:

En primer lugar, se aplicará, aunque en condiciones muy limitadas, la ley que las partes elijan (art. 14). Si las partes no eligen ley, es decir, en defecto de elección de ley, se aplicará la ley de residencia habitual común de las partes en el momento de producción del daño (art. 4.2).

Dispone el art. 4.1 el criterio de la lex loci en virtud del cual, en defecto de aplicación de los dos criterios analizados anteriormente, se aplicará la Ley del país en el que se produzca el daño, siendo irrelevante tanto el país donde se haya producido el hecho generador del daño como el país o países donde se manifiesten las consecuencias indirectas del hecho dañoso. En este sentido, respecto a los daños plurilocalizados, vuelve a entrar en juego la tesis del mosaico, es decir, que los daños cuya verificación tenga lugar en el territorio de un EM se regirán únicamente por la ley de dicho Estado. En este caso, para completar ese mosaico, si los daños se producen en varios Estados a cada daño se aplicará la ley del EM donde se verifiquen.

Como excepción a tener en cuenta, establece el art. 4.3 del Reglamento que, en caso de que las partes no hayan elegido ley y de las circunstancias se desprende que el daño manifiesta vínculos más estrechos con un país diferente del resultante de aplicar los criterios anteriores, se aplicará la ley del país con los vínculos más estrechos.

Los arts. 15 a 20 complementan lo anterior disponiendo el ámbito de la ley aplicable.

El art. 20 regula los supuestos de responsabilidad múltiple estableciendo que cuando sean varios los responsables y pague uno de ellos, podrá reclamar lo que le corresponda al resto en virtud de la ley aplicable a la obligación extracontractual que el deudor posea frente al acreedor. Respecto al reenvío, mencionar que queda excluido según lo dispuesto en el art. 24.

Hay dos supuestos específicos de responsabilidad extracontractual que, aunque no quedan fuera del ámbito de aplicación del Reglamento Roma II en base la cuestión de compatibilidad de instrumentos dispuesta en el art. 28 de la citada norma, poseen igualmente una normativa específica que considero merecedora de una especial atención por lo que, a continuación, procedo a examinarla, no sin antes hacer una breve conclusión sobre la estrategia a seguir en relación con la analizada teoría del mosaico.

Como letrada, si un cliente se presentase en mi despacho porque ha sufrido un daño plurilocalizado en el espacio cibernético trataría de diseñar una estrategia de actuación en base a dos cuestiones claves: los daños sufridos y el lugar donde los ha experimentado.

Intentaría adecuar mi demanda en base a la conocida como home litigation que, consiste, fundamentalmente en que, si el mayor porcentaje de daños pueden relacionarse con su EM, pongamos que en este caso sería España y ese porcentaje de daños sería un 90%, descartaría ese porcentaje de menor entidad para concentrar mi demanda en España, teniendo la competencia la jurisdicción de mi país (de ahí que se denomine a esta estrategia home litigation), consiguiendo que el pleito se dirima conforme a mi Derecho (el Derecho español) y reclamando por ese gran y mayor porcentaje de los daños sufridos a lo cual se refiere el profesor Javier Carrascosa González con el nombre de "the bulk of the damage" . Todo ello conforma lo que la doctrina denomina "demanda inteligente" ya que, aunque actuando así el mosaico no se completa, la actuación compone la mayor parte de dicho mosaico y el litigante ahorrará una cantidad económica sustancial de gastos y costes.

### 3.2.- INTELIGENCIA ARTIFICIAL Y ACCIDENTES DE CIRCULACIÓN POR CARRETERA

Llegados a este punto debemos tener presente la existencia del Convenio de La Haya de 4 de mayo de 1971 sobre la Ley aplicable en materia de accidentes de circulación por carretera (en vigor para España desde el 21 de noviembre de 1987). Ya conocemos esta normativa, por tanto, lo que vamos a cuestionarnos es lo siguiente ¿Qué pasa cuando es la Inteligencia Artificial la que va al volante? Es decir, hablamos de sistemas de IA aplicados a sistemas automatizados, o, lo que es lo mismo, qué sucede en los casos de accidentes de circulación por carretera cuando el vehículo es autónomo.

La primera pregunta en este sentido es ¿Qué es un vehículo autónomo? Es un elemento de transporte que prescinde del factor humano en su manejo dado que lleva integrado un sistema de transporte inteligente. El sistema operativo que se implanta

en el vehículo realiza una comunicación constante con elementos externos al mismo y adapta sus decisiones a la información que recibe, supliendo así al conductor[7].

El problema principal se centra en tratar de encontrar los criterios que definan tanto la competencia judicial internacional de los jueces como la ley aplicable cuando el accidente lo causa un sistema de IA ya que este sistema no se encuentra en un territorio físico concreto, sino que se ubica en el ciberespacio. En otras palabras, aunque el lugar dónde se produce el accidente es un espacio físico concreto, y sigue siendo un foro a efectos de la normativa existente, debemos introducir la cuestión de que el fallo del sistema que produce el accidente puede haber tenido lugar en cualquier lugar en función de la ubicación del servidor, de la señal digital, de su base de datos o incluso de la dirección IP.

A mi juicio y, completando la explicación iniciada en el apartado anterior, pese a haber analizado las distintas tesis desarrolladas por el TJUE, el punto de conexión, es decir, el criterio territorial se queda corto, pues no sólo se puede aplicar un criterio de un espacio físico o geográfico (es decir, el del lugar concreto donde se produce el accidente de coche) sino que también debemos tener en cuenta el espacio virtual a los efectos de tener presente dónde se produce el fallo del sistema de IA que causa ese accidente.

Tal vez la solución se base en desarrollar nuevos criterios conectados con esta nueva realidad a través de la suscripción de nuevos convenios internacionales. Modificar la normativa tradicional adaptándola a la tecnología.

Precisamente, como nuevos puntos de conexión podrían proponerse, a modo ejemplificativo, el del lugar de la dirección IP del sistema que causó el daño, el de la ubicación del servidor, el del repetidor que hubiera generado la última señal digital…

Este apartado enlaza con el siguiente de los puntos a tratar en el trabajo en base a una cuestión fundamental que yo misma me planteo que no es otra que un problema de calificación el cual es que en este tipo de supuestos ¿nos encontramos ante un caso de responsabilidad por daños en accidente de tráfico o, por el contrario, el vehículo autónomo puede considerarse un producto defectuoso y hay que tener en cuenta la aplicabilidad de la normativa por productos defectuoso?

---

[7] Juan Torraba Díaz. *Los vehículos autónomos y la responsabilidad del fabricante*. Revista de Responsabilidad Civil y Seguro. Año 55, núm. 2, febrero 2019.

## 3.3.- INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD POR PRODUCTOS DEFECTUOSOS

Como llevamos analizando a lo largo de todo nuestro estudio en la actualidad los algoritmos de IA se encuentran en multitud de productos tanto de uso cotidiano, como pudiera ser, por ejemplo, una aspiradora, como productos de alta precisión utilizados en el ámbito médico, o, incluso, en medicaciones para tratar el cáncer.

Pero ¿qué pasa si el uso de los mismos es defectuoso o negligente y causa daños a sus usuarios? ¿Qué pasa, además, si esos daños poseen un carácter transfronterizo?

A mi juicio se necesita una legislación uniforme en la comunidad internacional que garantice un enfoque uniforme en el tratamiento de esta cuestión para evitar el riesgo (que podría considerarse un daño secundario en caso de tener lugar) de que un mismo producto de IA que genere un daño no responda igual en función del país en el que se encuentre y la normativa a la que esté sometido.

Hasta que dicha legislación uniforme no se logre, siguiendo las palabras del profesor Antonio Merchán en el III Foro Europeo de Derecho Internacional Privado, deberemos tener presente que en este proceso de *electronificación* que estamos viviendo existen dos principios básicos, a saber, en primer lugar, el *principio de equivalencia funcional* que, implica que, tal y como él expresa *"lo que valía, sigue valiendo",* es decir lo que valía en el mundo que hasta ahora conocíamos, aunque tenga que modificarse para adaptarse mejor a la nueva realidad, sigue valiendo en tanto en cuanto no dispongamos de esta nueva regulación. Y ello enlaza con el segundo de los dos principios que comentaba el profesor, que no es otro que la *preexistencia de una regulación*, de una normativa, en definitiva, de un Derecho.

En el ámbito internacional ha sido fundamental el papel desempeñado en la Conferencia de la Haya que tuvo como resultado el Convenio de La Haya de 2 de octubre de 1973, sobre Ley aplicable a la responsabilidad por productos (en vigor en España desde el 1 de febrero de 1989).

Ya conocemos los aspectos generales de esta norma, por tanto, la cuestión de nuevo es la misma, el hecho de que debemos plantearnos cómo encaja con la nueva normativa. Lanzaba antes la cuestión del problema del conflicto de calificación que, ahora, paso a exponer, pues bien, en base a la normativa anterior y, teniendo en cuenta

el escaso avance tecnológico existente en los años en los que se desarrollaron los Convenios de la Haya del 71 y del 73, el supuesto era claro, en un accidente en el que estuviera implicado un vehículo se aplicaría el Convenio de 1971. Sin embargo, teniendo presentes tanto las Propuestas de Reglamentos de 2021 como las nueva Directivas de 28 septiembre de 2022 sobre Inteligencia Artificial y responsabilidad por productos defectuosos, el vehículo autónomo se consideraría producto defectuoso por el hecho de incorporar inteligencia artificial y elementos de software y en consecuencia le resultaría de aplicación toda la nueva normativa sobre productos defectuosos, además del Convenio de 1973. Por tanto, y, en definitiva, ahora el problema es la elección de norma ya que, en base a la armonización realizada por la UE, actualmente en un accidente de coches autónomos, tenemos dos convenios específicos, uno sobre accidentes de circulación, en el que encaja el supuesto, pues, aunque el coche sea autónomo, sigue dándose un accidente de circulación. A mayores, podría incluso darse la situación de que sólo uno de los vehículos implicados en el accidente sea autónomo. Pero, además, con la nueva regulación el coche autónomo se considera producto a todos los efectos, por lo que, si causa un daño por poseer algún elemento defectuoso, también se encuentra dentro del ámbito de aplicación del Convenio del 73. Dado que se trata de una problemática nueva, lo más probable sea que el propio TJUE deba encargarse de delimitar el ámbito de aplicación actual de cada una de estas normas y nos deje claro a qué instrumento debemos acudir cuando se nos plantee este supuesto. Otra posibilidad que es un interrogante actualmente es si en este tipo de conflictos de calificación pudiera ser una posible solución la coordinación de los distintos instrumentos con los que contamos o, por último, ¿Sería otra posible solución la denuncia de los Convenios de la Haya, tanto el de 1971 como el de 1973 para aplicar con exclusividad en los casos de responsabilidad el Reglamento Roma II?

# 4.- LA AFECTACIÓN DE LOS SMART CONTRACTS Y LA TECNOLOGÍA BLOCKCHAIN AL DERECHO INTERNACIONAL PRIVADO DE CONTRATOS

## 4.1.- QUÉ SON LOS SMART CONTRACTS Y LA TECNOLOGÍA BLOCKCHAIN

Los *smart contracts* o, en nuestro idioma, contratos inteligentes, son contratos que, tal y como fueron definidos por Nico Szabo[8] se consideran *"acuerdos contractuales donde la verificación, aplicación y ejecución de los términos del contrato está automatizada"* o *"conjunto de promesas, especificadas en forma digital, que incluyen los protocolos según los cuales las partes cumplen estas promesas"*[9].

No podemos concebir un Smart Contract sin la denominada *Tecnología Blockchain* la cual permite que los términos y condiciones del contrato inteligente se almacenen en una cadena de bloques autoejecutable, garantizándose de ese modo la neutralidad e inmutabilidad del contrato.

El funcionamiento de blockchain se basa en el modelo *peer to peer*, o, lo que es lo mismo usuario a usuario, de forma encadenada e inseparable. Cada vez que se lleva a cabo un cambio en la cadena de bloques, éste queda registrado y su contenido es encriptado mediante el denominado algoritmo "*hash*". El encriptado se realiza basándose en la transacción realizada anteriormente en la cadena, lo cual permite que, si se ha manipulado la anterior transacción, la posterior no se podrá leer.

La información almacenada en cada cadena no se puede modificar sin el consentimiento de la red proporcionando por ello una gran seguridad jurídica, hasta el punto de que algunos autores consideran que la blockchain es *"resistente, transparente e inviolable"*[10].

¿Cómo funciona la transacción?

---

[8] N. SZABO, *Smart Contracts*. *Chamber of digital commerce, "smart contracts: 12 use cases for business & beyond. a technology, legal & regulatory introduction – foreword by nick szabo" white paper prepared by smart contract alliance in collaboration with deloitte.*1994.

[9] N. SZABO, N. OP. Cit. Pág. 9.

[10] B. CARRON Y V. BOTTERON, *"How smart can a contract be?" en D. Kraus, T. Obrist y O. Hari (eds.), blockchains, smart contracts, decentralised autonomous organisations and the law, cheltenham*, Edward Elgar publishing, 2019.

Cada integrante del sistema de bloques posee dos claves que conforman la denominada "*Wallet*".

La transacción se pone en marcha en el momento en el que el remitente introduce en una cadena de firmas digitales de internet su clave digital única que recibe el nombre de "*clave privada*" puesto que permanece en secreto ya que solo la conoce él, es una especie de contraseña, y, a su vez, el destinatario tiene una clave que es conocida y recibe el nombre de "*clave pública*". Se le denomina así porque cualquier otro participante de la cadena de bloques podrá visibilizar dicha clave. La clave pública sería la propia identidad del usuario, que queda registrado, pero sin identificarse personalmente.

Todas las transacciones son públicas, sin embargo, tienen el carácter de ser anónimas ya que no hay identificación entre los sujetos que las realizan y las cuentas que aparecen en la propia operación.

Los Smart Contracts funcionan dentro de la cadena de bloques, pero se relacionan con la realidad mediante los denominados *oracles* u oráculos, que son los instrumentos a través de los cuales estos contratos obtienen información externa.

Pondré un sencillo ejemplo para poder entenderlo mejor.

Un Smart Contract podría ser el siguiente:

En una operación financiera si el precio de A supera los 1.000 euros, B debe pagar a C 500 euros. Ese contrato se almacena en una cadena de bloques. La pregunta es ¿cómo sabrá si el precio de A ha superado los 1.000 euros? Para ello utilizará el denominado oráculo, el cuál aportará esa información externa a la cadena de bloques, pero necesaria para la ejecución del contrato.

Algunos autores definen al oráculo como un *"puente entre el mundo del blockchain y el mundo externo"*[11].

¿Cuál es el mayor riesgo que ello entraña? Que aquél que controle el oráculo será el que pueda controlar la ejecución del Smart Contract. Por ello será fundamental que el oráculo elegido sea de confianza y esté descentralizado.

[11] FEDERICO AST. "Oráculos: conectando los smart contracts con el mundo". AESTEC. https://medium.com/astec/or%C3%A1culos-conectando-los-smart-contracts-con-el-mundo-9bcfda4ebffb

¿Cuáles son las ventajas y los inconvenientes de esta tecnología?

Como ventajas podemos citar las siguientes:

- Autonomía. No será necesario acudir a un intermediario para poder llevar a cabo el Smart Contract ya que el mismo se ejecuta de forma automática cuando se cumplen las condiciones programadas.
- Confianza y seguridad. Generada gracias a la técnica de la encriptación y todo el proceso de almacenaje de información y dificultad para su modificación antes descrito.
- Rapidez. Dado que el contrato se autoejecuta, no es necesaria actuación alguna de la otra parte contratante, así como tampoco de terceros.
- Ahorro. El cumplimiento del contrato es automático, no siendo necesaria la reclamación judicial ni extrajudicial del cumplimiento.
- Exactitud. El contrato se ejecutará en los términos exactos en los que se haya establecido sin interpretaciones algunas.

Como inconvenientes encontramos los que se exponen a continuación:

- Falta de desarrollo de normativa en materia de protección de datos.
- Oscuridad en torno a los derechos de supresión y rectificación.
- Inmutabilidad que da lugar a la imposibilidad de modificación del contrato cuando se dan circunstancias sobrevenidas y, a su vez, no permite la adaptación a los cambios legislativos.
- Problemas derivados del uso tecnológico: bugs o errores de programación, hackers…

Los retos a los que el Derecho Internacional Privado se enfrenta derivados de esta nueva tipología de contratación son diversos y variados y, entre ellos, podemos citar los siguientes:

La fijación de la competencia judicial internacional en caso de conflicto será compleja debido a que la descentralización producirá que no se sepa la ubicación exacta de las partes contratantes, así como el anonimato mismo dificultará conocer la propia identidad de las mismas y supondrá que la reclamación de la responsabilidad sea compleja. De ello también se deriva la consecuencia de que se complicará en gran medida saber cuál será la ley aplicable al contrato, todo ello, cuestiones que, a continuación, pasaremos a examinar en mayor profundidad.

## 4.2.- RECLAMACIONES INTERNACIONALES Y COMPETENCIA JUDICIAL INTERNACIONAL

Las tres normas fundamentales a tener en cuenta en materia de competencia judicial internacional son las siguientes:

1) Reglamento UE 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Bruselas I Bis).

2) Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Lugano el 30 de octubre de 2007 (Convenio de Lugano).

3) Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ).

Es importante tener presente la aplicación de estas tres normas explicada ya anteriormente, aunque, de nuevo, nos centraremos fundamentalmente en analizar el funcionamiento del primero de ellos, el Reglamento Bruselas I Bis, por ser el de mayor aplicación práctica.

Pues bien, la norma general será que el tribunal competente es aquel donde se encuentre el domicilio del demandado (art. 4)[12].

Se contempla, no obstante, la posibilidad de acudir a los denominados foros especiales (art. 7)[13] e interponer en dichos supuestos la demanda ante el tribunal de un estado miembro distinto al del domicilio del demandado. En el caso de un smart contract, para poder disponer de esta opción tendría que especificarse cuál es el lugar de cumplimiento de la obligación contractual, si el mismo no incluye un contrato escrito subyacente. ¿Qué pasa si no existe un contrato subyacente y el lugar donde deba cumplirse la obligación que sirva de base a la demanda no está definido en el smart contract? Según el TJUE en el asunto C-381/08, relativa a la competencia en materia contractual y a la determinación del lugar de cumplimiento de la obligación se debe proceder a realizar de forma autónoma la determinación del lugar. A modo de ejemplo, si el objeto principal del smart contract es la prestación de un servicio en

[12] La misma regla se contiene en el art. 2 del Convenio de Lugano y en el art. 22.ter.1 LOPJ.

[13] La misma regla se contiene en el art. 5.1 del Convenio de Lugano y en el art. 22. quinquies. a) de la LOPJ.

Madrid, si no se define otro lugar en el mismo, los tribunales de Madrid asumirían la competencia por falta de otro lugar expresamente indicado en el smart contract.

Tratándose de foros de protección de una parte débil, que puede ser un asegurado, un consumidor o un trabajador (secciones 3,4 y 5) la demanda se podrá interponer o bien ante el estado miembro de su domicilio o del lugar donde trabaje en caso del trabajador o ante el domicilio del demandado. En caso de ser demandada la parte débil el único foro posible será el del lugar de su domicilio. El problema en todos los supuestos analizados en los que como podemos observar, no existe cláusula de sumisión expresa, es el anonimato. Será difícil saber cuál es el tribunal competente si el punto de conexión se basa en una identidad. Por ello lo que muchos autores propugnan, entre ellos, Zimmermann[14] es exigir a los usuarios de la cadena de bloques algún tipo de identificación.

Sin embargo, se trata de una norma que ya existe en el ordenamiento jurídico dado que el art. 5 de la Directiva de comercio electrónico dispone que: "*Además de otros requisitos en materia de información contemplados en el Derecho comunitario, los Estados miembros garantizarán que el prestador de servicios permita a los destinatarios del servicio y a las autoridades competentes acceder con facilidad y de forma directa y permanente como mínimo a los datos siguientes:*

*A) Nombre del prestador de servicios;*

*B) Dirección geográfica donde está establecido el prestador de servicios.*

*C) Señas que permitan ponerse en contacto rápidamente con el prestador de servicios y establecer una comunicación directa y efectiva con él, incluyendo su dirección de correo electrónico*".

La misma regla se contiene en el art. 2 del Convenio de Lugano y en el art. 22.ter.1 LOPJ.

La misma regla se contiene en el art. 5.1 del Convenio de Lugano y en el art. 22. Quinquies. A) de la LOPJ.

[14] S. ZIMMERMANN, A. (2018). *Blockchain networks and european private international law.* Blog. http://conflictoflaws.net/2018/blockchain-networks-and-european-private- internationale-law/

Otra de las soluciones que trata de impulsarse ante esta problemática es exigir a los propietarios de las plataformas de blockchain que requieran una identificación a aquellos que quieran operar en éstas.

Otro problema que se identifica en este apartado es que, en ocasiones, los smart contracts son celebrados mediante operaciones "*M2M*", es decir, de máquina a máquina.

En estos supuestos lo que se está haciendo es considerar a comercializador de la máquina como responsable, de modo que se atribuye la competencia al tribunal de su domicilio cuando sea demandado.

Lógicamente, también debemos tener presente en el campo de los smart contracts la posibilidad de aquellos que incluyan cláusula de sumisión expresa (art. 25), que se podrá acordar siempre que ello no contravenga competencias exclusivas (art. 24), que la competencia se atribuya a los tribunales de un EM y que el acuerdo no incurra en nulidad de pleno derecho. Se trata de la opción más ventajosa pues de esta manera será competente el tribunal del lugar que las partes hayan acordado, aportando a la operación una mayor seguridad jurídica.

Analizando con mayor profundidad esta cuestión y, siguiendo al profesor Josep Gunnar[15] podemos distinguir en este punto tres tipos de acuerdos atributivos de jurisdicción en el ámbito de los smart contracts y la tecnología blockchain, a saber:

1) Acuerdos de Jurisdicción en los smart contracts que disponen de un contrato subyacente por escrito. En cuanto al requisito de forma, este tipo de sumisión expresa sería válida puesto que se realizaría por escrito y cumpliría lo establecido en el art. 25.1 a) del Reglamento Bruselas I Bis. También cumpliría con lo dispuesto en el art. 25.2 del mencionado Reglamento si el pacto se hace por medios electrónicos que permitan el registro duradero de ese acuerdo. Por ello, y siguiendo al citado profesor, *"el acuerdo atributivo de jurisdicción también podrá ser plasmado en la infetraz de un smart contract, en cuyo caso cumplirá con los requisitos de forma exigidos por el art. 25.2 RBI bis, como indica el TJUE, si dicha interfaz permite descargar y almacenar las condiciones pactadas, o,* al *menos, permite visualizarlas a través de una pantalla".*

[15] Josep Gunnar Horrach Armo, "Jurisdiction agreements in the field of smart contracts and blockchain technology". Revista electrónica de estudios internacionales (2021).

Pasando ahora a analizar los requisitos materiales, teniendo en cuenta que no existen unas específicas para los smart contracts, tendrían que cumplirse los de carácter general, es decir, que exista un verdadero acuerdo entre las partes, que se designe de forma genérica o concreta el tribunal, es decir, que se designen los tribunales de un EM con carácter general o que se indique un órgano jurisdiccional concreto de dicho EM. En último lugar, para cumplir con todos los requisitos de validez material habrá de ser analizado el ordenamiento jurídico del EM al que se sometan las partes. Por último, recalcar que el hecho de que finalmente el contrato resultase nulo no invalidaría la cláusula de sumisión expresa.

2) Smart contracts que se basan en un acuerdo verbal entre las partes. En este caso y siguiendo las exigencias del art. 25 del Reglamento Bruselas I Bis, el acuerdo verbal necesitaría para ser válido una posterior confirmación por escrito. Siguiendo de nuevo al profesor citado, la pregunta es si esa confirmación escrita se puede realizar en un código informático o no. Para el mencionado autor la clave se encuentra en este sentido en que la confirmación por escrito no venga únicamente redactada en lenguaje informático, sino que también venga traducida en lenguaje tradicional con el objeto de que las partes puedan corroborar su contenido y así sea válido el consentimiento.
3) Smart contracts que no disponen de un contrato subyacente o smart contracts puros. Siguiendo de nuevo al autor, no sería posible este tipo de acuerdo realizado puramente en un código informático ya que las partes estarían consintiendo sin comprender acerca de lo que consienten. No obstante, también considera que si el acuerdo pudiera llegara visibilizarse en la interfaz del smart contract, en ese caso sí sería posible.

Finalmente, otro problema que se puede presentar en este punto es que, el porcentaje mayor de este tipo de contratos son de adhesión, con lo cual, en aquellos casos en los que exista una parte débil sólo se podría acordar la sumisión tras el surgimiento de la controversia (art. 26.2) o si se permite en el caso del consumidor, interponer la demanda ante un tribunal distinto de los indicados en el Reglamento. Por último, recordar la posibilidad de sumisión tácita (art. 26) en aquellos casos en los que se demande a una parte y ésta comparezca sin efectuar impugnación alguna.

## 4.3.- LEY APLICABLE A LOS SMART CONTRACTS INTERNACIONALES

Una vez más la cuestión a plantearnos es si la actual normativa de Derecho Internacional Privado en la materia es suficiente o si, por el contrario, se necesita adaptar la misma a las necesidades que este tipo de contratación está generando. En este sentido existe entre la doctrina un debate. Así pues, hay autores que se posicionan a favor de la primera de las posturas, considerando que la normativa es suficiente y no es necesario llevar a cabo modificaciones o adaptaciones ni elaborar nuevos factores de conexión ni normas de conflicto entre los que podemos citar, entre otros, a Zimmermann[16] o Legerén-Molina[17].

Otros autores defienden la otra de las tesis en virtud de la cual se considera necesaria una adaptación de las normas de Derecho Internacional Privado, entre los que podemos citar a Wojdylo[18] o a S. Zimmermann, A. (2018).

A mi juicio la normativa existente es suficiente y ello lo justificaré mediante la explicación de la misma que procedo a realizar a continuación. Sin embargo, sería conveniente para algunos supuestos dar una solución de conflicto específica en materia de contratación inteligente.

Pasamos pues a analizar el Reglamento (CE) 593/2008 del Parlamento Europeo y del Consejo de 17 de junio de 2008 (Roma I).

La norma de conflicto puede ser definida como aquella técnica de reglamentación indirecta que utiliza la norma de Derecho Internacional Privado para determinar de entre los diferentes ordenamientos jurídicos implicados en el caso concreto, la normativa de cuál de todos ellos debe aplicarse para la regulación de la situación privada que, es internacional, precisamente porque confluyen varios ordenamientos. Es, por tanto, una técnica de localización de la norma a aplicar. El Reglamento Roma I es la norma de la que dispone la UE para determinar la ley aplicable a las obligaciones contractuales, que sería el supuesto en el que encajarían los Smart Contracts, en base al art. 1 relativo a su ámbito material. El art. 2 del Reglamento consagra el carácter universal de las normas de conflicto contenidas en el mismo. El

[16] S. ZIMMERMANN, A. N. OP.

[17] LEGERÉN-MOLINA, A. *Los contratos inteligentes en España.* Revista de Derecho Civil, v (2). 2018.

[18] WOJDYŁO, K. *How may we regulate the blockchain?* blog. https://newtech.law/en/how-may-we-regulate-the-blockchain/

principio fundamental del Roma I queda consagrado en su art. 3 que dispone que "*el contrato se regirá por la ley elegida por las partes. Esta elección deberá manifestarse expresamente o resultar de manera inequívoca de los términos del contrato o de las circunstancias del caso. Por esta elección, las partes podrá designar la ley aplicable a la totalidad o solamente a una parte del contrato*". La autonomía de la voluntad tiene una gran presencia en este ámbito.

Para Ana Mercedes López Rodríguez[19], opinión que yo misma comparto, este principio "*es la mejor forma de garantizar la seguridad jurídica de los smart contracts, ya que la elección de la ley aplicable por las partes evita controversias respecto al marco jurídico que rige el contrato, facilita la labor del juez y permite a las partes diseñar su relación jurídica conforme al Derecho sustantivo que mejor se adapte a sus intereses*".

Se trata, por tanto, de una elección de ley expresa o tácita, pero, en ningún caso presunta.

Sin embargo, dicha elección de ley llevará aparejada la condición de que el Estado cuya ley sea elegida deberá considerar válida la contratación inteligente ya que de otro modo dicha contratación no sería vinculante para las partes (art. 3.5 Roma I en relación con el art. 10.1 Roma I).

La ley podrá elegirse mediante pacto entre ambas partes contratantes, de forma solitaria por una de ellas o, incluso, se puede incluir en un contrato independiente al smart contract donde se recojan todos los términos del negocio jurídico.

Por supuesto, también existe la posibilidad de realizar la elección de ley en el propio smart contract. Finalmente, otra opción es que la sumisión se haga por la aceptación de las condiciones generales de la blockchain y, de hecho, la mayoría de las plataformas de blockchain ya imponen cláusulas de sumisión. Es el caso de la plataforma Ethereum que dispone que "*todos los asuntos relacionados con los Sitios web o estas Condiciones de uso y cualquier disputa o reclamación que surja de los mismos o esté relacionada con ellos (…), se regirán e interpretarán de acuerdo con las leyes internas de Suiza, sin dar efecto a ninguna disposición o norma de elección o conflicto de leyes (…)*".

[19] LÓPEZ RODRÍGUEZ, A. M. (2021). Ley aplicable a los smart contracts y lex crytographia. *CUADERNOS DE DERECHO TRANSNACIONAL*, *13*(1), 441-459.

Mayor problema presentará la falta de elección de ley ya que en este tipo de supuestos el Reglamento prevé en su art. 4 la ley aplicable a ocho tipos de contratos típicos, entre los que no se contemplan los Smart Contracts. En estos supuestos, por tanto, habrá que acudir a la ley del lugar de residencia habitual del prestador característico, dejando siempre a salvo la posibilidad del juez de elegir una ley que considere que se encuentra más estrechamente vinculada con el supuesto (art. 4.4). Que se entienda por prestación característica habrá que determinarlo acudiendo al denominado centro de gravedad del contrato tal y como se desprende del Considerando 19 de Roma I. En los supuestos en los que una de las partes contratantes sea una "*parte débil*", esto es, un consumidor, un trabajador o un contrato de seguro, se podrá elegir la ley más favorable o, en defecto de ésta, la ley de residencia habitual de la parte débil.

El problema principal se presentará en este tipo de contratos cuando sólo existan en forma de código ya que si la blockchain no se localiza en un único punto y las partes permanecen en el anonimato, no se puede localizar ni la ley del lugar de residencia habitual del prestador característico ni tampoco la ley más vinculada con el supuesto.

Siguiendo a López Rodríguez[20], *"en la cadena de bloques cualquier conexión a la ubicación de la cuenta del usuario es demasiado superficial y aleatoria, ya que implica establecer la ubicación de su clave privada. Si ya es difícil en la práctica determinar la ubicación de una cuenta de valores con intermediario, aún lo es más establecer la ubicación de una cartera digital. Por ello, entendemos que la solución más práctica y previsible en estos casos, a la vez que la menos arbitraria, es la aplicación de la lex fori (…). Al mismo tiempo, la aplicación de la lex fori en ausencia de elección, cuando la deslocalización de la transacción impida establecer razonablemente la ley del país con las conexiones más estrechas, constituye una solución que aporta seguridad jurídica y previsibilidad".*

No quiero ni debo finalizar este estudio sin antes realizar una breve mención a la Lex Cryptographia, y, es por ello que, siguiendo, de nuevo, a Ana Mercedes López Rodríguez[21] se puede entender por Lex Cryptographia al *"conjunto de normas que operan a través de contratos inteligentes autoejecutables y organizaciones autónomas descentralizadas".*

[20] LÓPEZ RODRÍGUEZ, A.M. N. OP. Cit. Pág. 453.

[21] LÓPEZ RODRÍGUEZ, A.M. N. OP. Cit. Pág. 448.

La autora compara esta ley con la tradicional Lex Mercatoria de modo que al igual que en su momento hicieron los comerciantes, en la actualidad son los agentes de la cadena de bloques los que están formando esta ley en base a nuevas costumbres y principios propios de este nuevo ámbito con el objeto de autorregularse.

Aunque la tendencia seguida tiene por objetivo acabar conformando lo que se ha venido a denominar una "*gobernanza algorítmica*"[22], en la que se pueda prescindir de la intervención del Derecho del estado, de los jueces y de los tribunales, en la actualidad este sigue siendo necesario para todos aquellos supuestos en los que los algoritmos no hayan previsto en algunos casos ni si quiera la propia situación y, para los supuestos en los que sí lo hayan hecho, no tengan una solución.

[22] A. WRIGHT Y P. DE FILIPPI, *Decentralized blockchain technology and the rise of lex cryptographia. file:///C:/Users/34695/Downloads/SSRN-id2580664.pdf*

# CONCLUSIONES

**I.** El objetivo de este trabajo ha sido reflexionar sobre la situación actual de la IA, como afecta al Derecho y, particularmente, al Derecho Internacional Privado y plantear las cuestiones que quedan por resolver como perspectivas de futuro ya que el veloz cambio tecnológico es evidente y ya está provocando un cambio en el sistema de funcionamiento de los operadores privados y ello generará una enorme transformación social a nivel global. Para ello, he ido planteando problemas. Como hemos visto, el primero de ellos, era lograr una definición uniforme acerca de qué es la IA. Como todo término requiere una un concepto, sin embargo, se trata de un problema a solucionar puesto que no hay una definición común del mismo y ya no es sólo que sea necesario alcanzarla, sino que ésta ha de ser, como ya hemos dicho uniforme, pero, además, también atemporal, lo cual es un gran reto para una materia que cambia a cada instante. Además, y, coincidiendo con el objetivo perseguido por el Libro Blanco sobre IA, tiene que ser una definición precisa, pues sólo así se garantiza la seguridad jurídica. Es verdaderamente importante la consecución de este primer objetivo, pues resulta muy difícil legislar acerca de algo que no está bien definido, o, al menos, las propias Instituciones deberían esforzarse por lograr un concepto común a emplear cuando se refieran a IA. No obstante, de todas las definiciones apuntadas me parece que la más precisa, por el momento, es la apuntada por el Parlamento Europeo, que, a modo de recordatorio la define como *"todo sistema basado en programas informáticos o incorporado en dispositivos físicos que muestra un comportamiento que simula la inteligencia, entre otras cosas, mediante la recopilación y el tratamiento de datos, el análisis y la interpretación de su entorno y la adopción de medidas, con cierto grado de autonomía, para lograr objetivos específicos".*

**II.** Recurrir a instrumentos de soft law como recurso temporal puede estar bien, pero, sin duda, nuestro sistema jurídico necesita modernizarse. Tenemos múltiples normas como el Reglamento Bruselas I Bis, los Reglamentos Roma I y Roma II, los Convenios de la Haya de 1971 y de 1973, pero, la conclusión en este punto es clara, cuándo todas estas normas se desarrollaron, no se estaba pensando en supuestos como los que pueden presentarse a día de hoy por la

influencia de la IA. Aunque siguen siendo aplicables sería conveniente que comenzasen a detallar este tipo de situaciones. Siendo conscientes de esta necesidad de modernización consecuencia del proceso de electronificación la Unión Europea llevó a cabo en el año 2020 el Libro Blanco sobre IA con el que realizó un compromiso de adoptar una Ley sobre IA. Fue en abril de 2021 cuando presentó las dos propuestas de Reglamentos, uno sobre normas armonizadas en materia de IA y otro sobre responsabilidad civil derivada de la IA. Se trata de normas horizontales sobre IA cuyo foco radica en la prevención de daños, para lo cual, como hemos visto, se establecen distintos niveles de riesgo.

**III.** Sin embargo, dicha normativa necesitaba un desarrollo mayor, razón que llevó a que en septiembre del presente año se presentasen las dos nuevas Directivas que complementan y completan los Reglamentos y que buscan adaptar la normativa a la era digital. Por un lado, la Directiva sobre responsabilidad civil en materia de IA tiene como objetivo evitar la fragmentación jurídica garantizando que las víctimas de daños causados por productos o sistemas que incluyen IA se beneficien de protección al igual que si sufriesen un daño en cualquier otra circunstancia en la que la IA no esté involucrada. Para ello introduce dos elementos principales, a saber, la presunción de causalidad que evitará que los perjudicados deban probar el daño causado y, por otro lado, el acceso a las pruebas que hayan sido presentadas por empresas o proveedores cuando se trate de IA de alto riesgo. Por otro lado, la Directiva sobre responsabilidad por los daños causados por productos defectuosos, busca la cobertura de los daños causados por productos que derivan de las nuevas tecnologías, es decir, busca, de nuevo, modernizar la normativa. Así, esta nueva norma incluye desde productos como sillas de jardín hasta medicamentos contra el cáncer o actualizaciones de software en robots de limpieza o aplicaciones médicas. Esta nueva norma permite la reclamación por daños causados por estos productos defectuosos incluyendo lesiones corporales, daños materiales o, incluso, pérdidas de datos.

**IV.** El problema concreto actualmente es, a mi juicio, la coexistencia de normativa anterior con las normas que acabamos de mencionar. Es decir, ahora se plantea la pregunta de cómo encajará el nuevo marco normativo desarrollado por la UE sobre IA con la normativa que ya conocemos en materia de

Responsabilidad Civil, esto es Roma II o los Convenios de la Haya de 1971 o de 1973. Por ejemplo, en el ámbito de un accidente de circulación ¿qué norma concreta debemos aplicar? Tenemos más de un instrumento en el que podría encajarse el supuesto. Tras haber analizado el tema detenidamente, es mi opinión que la nueva normativa europea no desplaza a las normas materiales con las que contábamos, sino que están destinadas a convivir. La forma en que lo hagan será que cuando la norma de conflicto nos lleve a la normativa de un determinado Estado de la UE, entonces habrá que tener presente y aplicar los reglamentos y las directivas europeas.

**V.** El segundo gran bloque de este estudio ha tratado de abordar el impacto de los Smart Contracts y la tecnología blockchain al ámbito del Derecho Internacional Privado, ya que, como es lógico, esta nueva contratación se desarrolla, principalmente, a través de internet que es un espacio absolutamente global y deslocalizado que le da ese elemento internacional. Hemos podido observar cómo este tipo de contratos se distingue de aquellos a los que acostumbramos puesto que ofrecen inmutabilidad, así como almacenamiento distribuido. Ahora bien, ¿verdaderamente estamos ante contratos? La conclusión que yo alcanzo en este punto es que no es un contrato, sino que simplemente es la ejecución de un contrato tradicional preexistente. No obstante, con el avance que están experimentando, nuevamente, considero que el legislador deberá adaptar la normativa pues, cuando el Reglamento Bruselas I Bis fue realizado, la contratación electrónica no era un punto a tener presente como sí lo es hoy en día. Sin embargo, y pese a que sería una buena opción incluir algún foro específico a estos efectos, debemos tener presente que en el mencionado reglamento están presentes una serie de artículos, en concreto, del 7 al 23, en base a los cuáles pueden extraerse algunos elementos específicos por los que se puede atribuir la competencia al tribunal de un determinado Estado. Por ejemplo, el art. 7.1 de Bruselas I Bis establece como foro de competencia el lugar de cumplimiento de la obligación base de la demanda. Así pues, si el contrato dispone que debe entregarse una determinada mercancía, la competencia la ostentará el Estado Miembro en el que en base al contrato deban entregarse las mercancías. Aplicado esto al marco de un smart contract no habría ninguna diferencia. Es

decir, si en éste surge una controversia el tribunal competente será el del lugar en el que deba cumplirse la obligación base de la demanda.

**VI.** Por otra parte, en lo que al Derecho aplicable se refiere, el problema planteado en el trabajo podría resumirse como qué ley hay que aplicar cuando surge una controversia internacional en un smart contract. El Reglamento Roma I da libertad a las partes firmantes del mismo para que determinen la ley que quieran que rija el contrato. El verdadero problema como hemos abordado se da si las partes no configuran dicho dato en el smart contract, o éstas permanecen en el anonimato. Por ello la solución más precisa en estos supuestos es acudir a la ley del foro con el objetivo fundamental de alcanzar seguridad jurídica.

**VII.** Al igual que en el ámbito de los sistemas de IA y de responsabilidad civil derivada de la misma, también en este ámbito quedan muchos interrogantes abiertos habiendo sido mi cometido con este trabajo plantear algunos de ellos, a saber, ¿hasta qué punto es factible que un sistema de Inteligencia Artificial desarrolle un contrato que vincule a varias partes? ¿Deberán responder éstas de incumplimientos contractuales que sean consecuencia de una mala redacción de este tipo de tecnología? ¿las cláusulas de sumisión expresas generarán problemas específicos de consentimiento en los smart contracts? ¿cómo pueden afrontarse los problemas derivados del anonimato y de la ubicuidad en el ámbito de este tipo de contratos? ¿acabará por crearse una personalidad jurídica específica para los sistemas de Inteligencia Artificial?

# BIBLIOGRAFÍA


ABBOTT, R., «I think, therefore I invent: creative computers and the future of Patent Law», en Boston College Law Review, vol. 57, núm. 4, 2016, pp. 1079-1127.

ABBOTT, R., «Patenting the output of autonomously inventive machines», en Landslide, vol. 10 núm.1, 2017, pp. 16-22.

ABRAMS, D. S. y POLK WAGNER, R., «Poisoning the next Apple? How the American Invents Act harms inventors», en Standford Law Review, vol. 65, 2013, pp. 517-564.

ALBALADEJO, M., *Derecho Civil I. Introducción y parte general* (séptima edición), Ed. Librería Bosch, Barcelona, 1980.

ÁLVAREZ MUNÁRIZ, L., «Niveles de conciencia. Perspectiva socio-cultural», en Thémata. Revista de Filosofía, núm. 37, 2006, pp. 77-97.

ARKIN, R. C., Behavior-based robotics, Ed. MIT Press, Londres, 1998.

BADARO, S., IBÁÑEZ, J. y AGÜERO, M. J., «Sistemas expertos: fundamentos, metodologías y aplicaciones», en Ciencia y Tecnología, núm. 13, 2013, pp. 349-364.

BENEDETTA CAPIELLO, *AI-systems and non contractual liability. A European private international law analysis*. Giappichelli. 2022.

BENÍTEZ, R., ESCUDERO, G., KANAAN, S. y MASIP RODÓ, D., *Inteligencia artificial avanzada*, Ed. UOC, Barcelona, 2013.

BENNETT, M., DENNETT, D., HACKER, P. y SEARLE, J., *La naturaleza de la conciencia. Cerebro, mente y lenguaje*, Ed. Paidós, Barcelona, 2008.

BODEN, M. A., *The creative mind. Myths and mechanisms*, 2nd Edition, Ed. Routledge, Londres, 2004.

BRINGSJORD, S. y SCHIMANSKI, B., «What is Artificial Intelligence? Psychometric AI as an answer», en Proceedings of the 18th International Joint Conference on Artificial intelligence, 2003, pp. 887-893.

CAMACHO CLAVIJO, S., «La subjetividad "ciborg"», en AA.VV., Inteligencia artificial. Tecnología y Derecho (Dir. NAVAS NAVARRO, S.), Ed. Tirant Lo Blanch, Valencia, 2017, pp. 231-257.

CASTILLO, E., GUTIERREZ, J. M. y HADI, A. S., *Sistemas expertos y modelos de redes probabilísticas*, Ed. Academia de Ingeniería, D.L., España, 1996.

CHOPRA. S. y WHITE, L., «Artificial agents –personhood in Law and Philosophy»; en AA.VV., ECAI'04 Proceedings of the 16th European Conference on Artificial Intelligence (Eds. LÓPEZ DE MÁNTARAS, R. y SAITTA, L.), Ed. IOS Press Amsterdam, Holanda, 2004, pp. 635-639.

COHEN, P. R., FEIGENBAUM, E. A., *The Handbook of Artificial Intelligence*, volume 3, Ed. Heuris- Tech Press, California, 1982.

DE MIGUEL ASENSIO PEDRO A. *Conflict of laws and the internet*. Elgar Information Law and practice. 2020.

DE MIGUEL ASENSIO PEDRO A. *Derecho privado de Internet*, Civitas, Madrid, 2022.

DORMIDO S. y DE LA CRUZ, J. M., «Inteligencia artificial: pasado, presente y futuro», en Revista del Centro Asociado a la UNED Melilla, núm. 14, 1989, pp. 9-21.

ERCILLA GARCÍA, J., «Aproximación a una personalidad jurídica específica para los robots», en Revista Aranzadi de Derecho y Nuevas Tecnologías, num. 47, 2018.

ESKRIDGE, W. N. y FRICKEY, P. P., «Statutory interpretation as practical reasoning», en Standford Review, vol. 42, 1990, pp. 321-384.

FLORES LÓPEZ, L. y FERNÁNDEZ FERNÁNDEZ, J. M., *Las redes neuronales artificiales. Fundamentos teóricos y aplicaciones prácticas*, Ed. Netbiblo, España, 2008.

GARCÍA SERRANO, A., *Inteligencia artificial: fundamentos, práctica y aplicaciones*, Ed. RC, Madrid, 2012.

GRIDEL, J.P., Les inventions de salariés à l´ épreuve de la loi du 13 juillet 1978 et du Décret du 4 septembre 1979, Ed. Librairie Générale de Droit et de Jurisprudence (LGDJ), París, 1980.

HIGHAM, N. J., «Programming languages: an applied mathematics view», en AA.VV., *The Princeton Companion to Applied Mathematics* (HIGHAM, N. J., DENNIS, M. R., GLENDINNING, P. A. MAR- TIN, F. S., Y TANNER, J.), Ed. Princeton University Press, Estados Unidos, 2015.

HOLGADO, P., VILLAGRA, V. A., y MATEOS, V., «Redes neuronales aplicadas al proceso de aprendizaje de un sistema de respuestas a intrusiones automático», en

AA.VV., XI Jornadas de Ingeniería Telemática (JITEL 2013) (Coord. DÍAZ VERDEJO, J. E., NAVARRO ORTIZ, J. y RAMOS MUÑOZ, J. J.), Ed. Universidad de Granada, Granada, 2013, pp. 419-426.

IGLESIAS FERNÁNDEZ, C.A., Definición de una metodología para el desarrollo de sistemas multiagentes, (Tesis Doctoral), Departamento de Ingeniería de Sistemas Telemáticos de la Universidad Politécnica de Madrid, Madrid, 1998, pp. 5 y ss. Disponible en http://www.upv.es/sma/teoria/agentes/tesiscif.pdf

KAPLAN, J., *Inteligencia artificial. Lo que todo el mundo debe saber* (Trad. RUÍZ FRANCO, J. C.), Ed. TEELL, España, 2017.

LÓPEZ DE MÁNTARAS, R., «La inteligencia artificial y las artes. Hacia una creatividad computacional», en AA.VV., El próximo paso. La vida exponencial, Ed. BBVA Open Mind, Madrid, 2016, pp. 99-123.

LUGER, F, G., *Artificial Intelligence: Structures and Strategies for Complex Problem Solving* (Fifth Edition), Ed. Addison-Wesley, Harlow, 2005.

MAJID, M. y BISHOP, M., «Weak and strong computational creativity», en Computational Creativity Research: Towards Creative Machines (Eds. BESOLD, T. R.; SCHORLEMMER, M. y SMAILL, A.), Ed. Atlantic Press, París, 2015, pp. 37-49.

MCCARTHY, J., Recursive Functions of Symbolic Expressions and Their Computation by Machine, Part I, en Communications of the ACM, vol. 3, núm. 4, 1960.

MORAVEC, H., *Robot: mere Machine to Transcendent Mind*, Ed. Oxford University Press, Estados Unidos, 2000.

NAVAS NAVARRO, S., «Derecho e inteligencia artificial desde el diseño. Aproximaciones», en AA.VV., Inteligencia artificial. Tecnología y Derecho (Dir. NAVAS NAVARRO, S.), Ed. Tirant Lo Blanch, Valencia, 2017.

NEWELL, A. y SIMON, H., «Computer science as empirical inquiry: symbols and search», en Communications of the Association for Computing Machinery, vol. 19, núm.3, 1976.

NEWELL, A. y SIMON, H., «The logic theory machine», en Institute of Radio Engineers, Transac- tions on Information Theory, vol. I-T 2, núm. 3, 1956.

NILSSON, N. J., *Inteligencia artificial. Una nueva síntesis* (Trad. MARÍN MORALES, R., PALMA MÉNDEZ, J. T. y PANIAGUA ARIS, E.), Ed. Mc Graw Hill, Madrid, 2001.

OLIVER, N., «Una nueva etapa dorada para la inteligencia artificial», en Harvard Deusto Business Review, núm. 274, 2018.

ORTEGA GIMÉNEZ, ALFONSO. *Smart contracts and private international law. Aranzadi. Pamplona*. 2022.

PINO DÍEZ, R., GÓMEZ GÓMEZ, A. y ABAJO MARTÍNEZ, N., *Introducción a la inteligencia artificial: sistemas expertos. Redes neuronales artificiales y computación evolutiva*, Ed. Universidad de Oviedo, Servicio de publicaciones, 2001.

RUSSELL, S. y NORVIG, P., *Inteligencia artificial. Un enfoque moderno* (2a edición) (Coord. Trad. JOYANES AGUILAR, L.), Ed. Pearson, 2008, Madrid.

SANTOS GONZÁLEZ, M. J., «Regulación legal de la robótica y la inteligencia artificial: retos de futuro», en Revista Jurídica de la Universidad de León, núm. 4, 2017.

SIMON, H., «Why should machines learn?», en AA.VV., Machine learning: and artificial intelligence approach (Eds. MICHALSKI, R.S, CARBONELL, J.G. y MITCHELL, T.M.), Ed. Springer, Berlín, 1983.

STEVENS, L., *Artificial intelligence. The search for the perfect machine*, Ed. Hayden Book Company, New Jersey, 1985.

TUR FAÚNDEZ, C. (2018). *Smart contracts. Análisis jurídico*. Madrid, España: REUS.

VILALTA NICUESA, A. E. (2019). *Smart legal contracts y blockchain. La contratación inteligente a través de la tecnología blockchain*. Madrid, España: Wolters Kluwer.

## JURISPRUDENCIA

STJCE de 30 de noviembre de 1976, as. 21/76, Mines de Potasse d´Alsace.

STJCE 27 septiembre 1988, 189/87, *Kalfelis*.

STJCE 11 enero 1990, C-220/88, *Dumez*.

STJCE 26 marzo 1992, C-261/90, *Dresdner Bank [II]*.

STJCE 7 marzo 1995, C-68/93, *Shevill*.

STJCE 19 septiembre 1995, C-364/93, *Marinari*.

STJCE 27 octubre 1998, C-351/96, *Réunion*.

STJCE 17 septiembre 2002, C-334/00, *Tacconi*.

STJCE 1 octubre 2002, C-167/00, *Henkel*.

STJCE 5 febrero 2004, C-18/02, *Torline*.

STJCE 10 junio 2004, C-168/02, *Kronhofer*.

STS de 31 de octubre de 2007.