EL FUTURO DIGITAL EN LA UE: DE LA PROTECCIÓN DE DATOS A LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL

Autor: David Fernández García

5º E3-Analytics

Derecho Internacional Privado

Tutora: Salomé Adroher Biosca

Madrid

Abril 2020

RESUMEN

La revolución 4.0 y el desarrollo tecnológico ocupan la posición central en el marco geopolítico actual. Europa se encuentra en una situación delicada entre las grandes potencias tecnológicas EEUU-China. En este contexto incierto, la UE ha venido definiendo los parámetros de su estrategia digital. La protección de los derechos fundamentales y libertades de los ciudadanos europeos es uno de los pilares de dicha estrategia. La aprobación y entrada en vigor del Reglamento (UE) 679/2016, General de Protección de Datos supuso el primer paso en la consecución de dicha protección de la UE y marcó un precedente en materia de regulación de los riesgos generados por el desarrollo tecnológico. Sin embargo, la tecnología y la ciencia siempre avanzan más rápido que las normas. Claro ejemplo de ello encontramos en la irrupción de la Inteligencia Artificial. Si la UE pretende conservar o mejorar la posición geopolítica en la que se encuentra actualmente, además de llevar a cabo políticas que favorezcan la inversión público-privada en el continente, deberá continuar en la vanguardia normativa y por ello no debe aplazar la adopción de normas relativas a la IA.

Este trabajo analizará la situación geopolítica de la UE, la eficacia del Reglamento General de Protección de Datos, con sus implicaciones de Derecho Internacional Privado, así como también el estado actual de la regulación IA en el plano internacional incluyendo una propuesta final de *lege ferenda* en materia de IA para la UE.

ABSTRACT

The 4.0 revolution and technological development occupy the central position in the current geopolitical framework. Europe finds itself in a delicate situation between the major technological powers USA-China. In this uncertain context, the EU has been defining the parameters of its digital strategy. The protection of the fundamental rights and freedoms of European citizens is one of the pillars of this strategy. The approval and entry into force of the General Data Protection Regulation was the first step in achieving such EU protection and set a precedent in terms of regulating the risks generated by technological development. However, technology and science always advance faster than the norm. A clear example of this can be found in the emergence of Artificial Intelligence. If the EU intends to preserve or improve the geopolitical position in which it currently finds itself, in addition to pursuing policies that favour public-private investment in the continent, it must continue to be at the forefront of regulation and therefore should not procrastinate in the adoption of standards relating to AI.

This paper will analyse the geopolitical situation in the EU, the effectiveness of the General Data Protection Regulation, with a focus on the Private International Law implications, as well as examine the current state of AI regulation at the international level including a final *lege ferenda* proposal on AI for the EU.

ÍNDICE

ABREVIATURAS

AEPD – Agencia Española de Protección de Datos

CDFUE – Carta de Derechos Fundamentales de la Unión Europea

EEUU – Estados Unidos

IA – Inteligencia Artificial

RGPD – Reglamento General de Protección de Datos

STJUE – Sentencia del Tribunal de Justicia de la Unión Europea

TFUE – Tratado de Funcionamiento de la Unión Europea

TJUE – Tribunal de Justicia de la Unión Europeo

UE – Unión Europea

1. INTRODUCCIÓN: DESARROLLO TECNOLÓGICO Y GEOPOLÍTICA

1.1 El Contexto

El nacimiento de Internet en los años 80 supuso el punto de partida de la nueva revolución industrial que vivimos actualmente. Klaus Schwab, fundador del Foro Económico Mundial, señaló que la nueva revolución industrial no es la mera aparición de una serie de tecnologías emergentes, sino la transición hacia la integración de sistemas construidos sobre dichas técnicas en nuestra vida cotidiana (Schwab, 2016).

La revolución digital se configura, así, como la nueva revolución industrial que ansía cambiar la forma en la que los seres humanos nos relacionamos, trabajamos o pensamos.

Tecnologías como el 5G, la computación cuántica, inteligencia artificial o el llamado Internet de las cosas, han sido desarrolladas en un periodo de tiempo muy reducido. Esto nos permite apreciar la magnitud de la transformación digital.

Mientras que el 17% de la población aún no ha experimentado plenamente los avances de la segunda revolución industrial, internet ya ha sido capaz de permear todo el mundo en menos de una década (Schwab, 2016).

Si bien es cierto que la llegada de Internet a la población a través de las redes telefónicas existentes supuso una herramienta esencial para la globalización, que pretendía reducir el papel que juegan los Estados en la vida de los ciudadanos, su exponencial influencia en la economía mundial dio lugar a una lucha por su gobernanza que sentaría las bases para la posterior competencia tecnológica.

Por un lado, Estado Unidos abogó por una gobernanza llevada a cabo por instituciones privadas. Frente a esto, estados como China y Rusia apostaron por una gobernanza puramente estatal. Europa, por otro lado, terminó por inclinarse hacia una gobernanza privada en su seno en la que los Estados tuvieran cierto protagonismo (Puddephatt, 2020).

Sin embargo son las grandes corporaciones tecnológicas las que en última instancia han acabado por controlar lo que sucede en la red a través de sus políticas de uso, normas y condiciones generales (Schwab, 2016).

Por ello, los grandes actores de este partido geopolítico dejaron atrás la gobernanza de Internet para centrar todos sus esfuerzos en desarrollar grandes empresas tecnológicas bajo la premisa de que el verdadero dominante de la revolución 4.0 sería aquel que consiguiera contar con un mayor número de gigantes tecnológicos en su equipo.

Así, el desarrollo tecnológico se configura en el presente como clave para la determinación de las potencias mundiales en una suerte de "neocolonialismo tecnológico" (Ortega Klein, 2020).

Tal como sucedió durante la Guerra Fría con el desarrollo tecnológico-militar entre Estados Unidos y Rusia, actualmente somos testigos de una nueva disputa por coronarse como la primera potencia tecnológica mundial. Esta vez, Estado Unidos y China son los protagonistas de la contienda, mientras que otros como India, Rusia, la UE, Japón, Corea del Sur o Australia buscan hacerse hueco en este nuevo mercado digital.

Estados Unidos

Actualmente Estados Unidos es el líder mundial en desarrollo tecnológico, especialmente en tecnología militar. Cuenta con las mayores empresas tecnológicas del planeta como *Apple, Amazon, Alphabet, Microsoft* o *Facebook* que son las principales prestadoras de servicios digitales a nivel mundial a día de hoy (Ortega Klein, 2019).

Como se ha señalado, cada vez más ciudades estadounidenses quieren imitar el modelo de Silicon Valley. Al mismo tiempo, son muchas las empresas tecnológicas americanas que están llevando a cabo estrategias de descentralización de sus oficinas así como una expansión de las mismas a diferentes centros del país, creando un ecosistema que favorece la innovación, la diversidad y el crecimiento económico (KPMG, 2018).

La innovación, la inversión privada, el talento, la infraestructura y la calidad en los servicios ofrecidos son actualmente la gran apuesta de los americanos.

Estados Unidos es líder mundial a día de hoy en Inteligencia Artificial, tecnología determinante en el desarrollo digital y que en los próximos años será la tecnología que marcará la verdadera diferencia entre Estados.

Según el Informe anual de IA de la Universidad de Stanford, EEUU posee el mayor número de patentes registradas relacionadas con IA y cuenta con los estudios de mayor calidad en este ámbito.

China (Ortega Klein, 2019)

El gigante asiático pretende convertirse en la primera potencia económica mundial para el año 2049, siendo cabeza mundial en tecnología. En 2015 el gobierno chino presentó el documento *Made in China 2025* en el que se planteó alcanzar una posición dominante en diez sectores estratégicos como la robótica o la biotecnología.

En 2016, tras la victoria por un ordenador de una serie de partidas del popular juego *Go* a uno de los mejores jugadores del mundo, la inteligencia artificial adquirió un protagonismo sin precedentes. A día de hoy, parece que los objetivos fijados para el año 2049 pueden llegar a cumplirse con bastante antelación a lo planeado.

Además de su estrategia geopolítica de infraestructuras de *La Nueva Ruta de la Seda*, China controla más del 40% del comercio electrónico mundial, es líder en otros sectores claves para la revolución digital como en la producción de las baterías, venta de vehículos eléctricos, pago digital o en energías renovables. Es el país en el que más robots industriales se instalan y que cuenta con el mayor número de ingenieros.

Su régimen jurídico en materia de datos o de inteligencia artificial es permisivo con las empresas nacionales y en muchas ocasiones deja de lado la protección de los derechos de sus propios ciudadanos y, por supuesto, los del resto de sus clientes internacionales.

Es evidente también su apropiación, en muchos casos reprochable, de tecnología extranjera a través de prácticas desleales, *hackeos* o exigencias draconianas a usuarios. Esto le confiere una ventaja aún mayor respecto a sus principales competidores que, por lo general, son democracias desarrolladas en las que muchas de estas acciones no están permitidas.

En consonancia con su estrategia, China busca así reducir su dependencia de EE.UU. creando sus propias compañías nacionales tecnológicas que compitan con homólogas americanas mientras continúa incrementando su posición dominante en lo que a materias primas respecta (por ejemplo, a través de la inversión en infraestructura en el continente africano). Actualmente China cuenta con varias compañías en el top 10 de las mayores tecnológicas como *Alibaba* o *Tencent.*

Otros (Ortega Klein, 2019)

Japón y Corea del Sur son jugadores importantes en la partida *geotecnológica*. Cuentan con infraestructura y capital necesarios para su propia revolución 4.0 y son partidarios de una regulación efectiva de las nuevas tecnologías. Australia y Canadá son otro ejemplo similar, algo por detrás de los asiáticos en cuanto a la infraestructura digital. Son probablemente los aliados más factibles para la UE por su situación geopolítica, desarrollo e interés por la protección de los derechos y libertades de sus ciudadanos.

Rusia o India, por otra parte, cuentan con la población y recursos necesarios para ser estratégicos en la lucha por la supremacía digital. De hecho, India parece estar avanzando a pasos agigantados en lo que a la digitalización respecta. De los 1.365 millones de habitantes indios, 560 contaban con suscripción a Internet en 2018, lo que supone cuatro veces más que en 2016 (McKinsey Global Institute, 2019). Se calcula que la totalidad de la población estará conectada para 2025.

2. LA UE: ESTRATEGIA DIGITAL EUROPEA DE LA ÚLTIMA DÉCADA

2.1 Introducción

Como he analizado anteriormente, Europa se encuentra en una posición de desventaja frente a China y Estados Unidos, principalmente por su dependencia tecnológica y de recursos. Europa en estos momentos no es totalmente soberana ni independiente.

Ninguna de las 20 grandes compañías de la economía digital es europea, lo que genera una tremenda dependencia de empresas extranjeras tanto a nivel de servicios como de producción.

Pese a los planes de inversión de las instituciones europeas y las numerosas estrategias planteadas (algunas de ellas las analizaré más adelante) Europa se encuentra muy lejos de poder competir con los bloques EE.UU. – China por lo que tendrá que buscar alianzas en alguno de ellos, en ambos o en otros estados.

No obstante, Europa no se encuentra totalmente fuera de esta contienda como sí sucedió durante los años de la Guerra Fría (Giddens, 2020), ya que es un actor geopolítico estratégico en esta batalla tanto para Estado Unidos como para China, puesto que las relaciones comerciales con el antiguo continente pueden resultar claves para decantar la balanza del poder. Las características del mercado europeo son más que atractivas para las grandes corporaciones tecnológicas y, por ende, para la inversión privada extracomunitaria.

Sin embargo, Europa no puede conformarse con ser un mero cliente de los productos/servicios que otras superpotencias ofrezcan. Europa tiene el potencial económico, tecnológico y educativo para convertirse en una potencia tecnológica a nivel mundial y de alcanzar su soberanía digital.

La publicación en 2016 del Reglamento General de Protección de Datos[1] supuso un hito sin precedentes de aplicación global de una norma dirigida a regular una sector tan importante en el mercado digital como los datos personales respecto de aquellas

[1] Reglamento (UE) nº 679/2016 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

organizaciones que tuviera datos de ciudadanos residentes en la UE. Tras esto, también se han aprobado normas posteriores que dan respuesta a los retos que plantean las nuevas tecnologías como la regulación de los vehículos terrestres y pretende continuar con la regulación del carbono, el comercio digital o la Inteligencia Artificial.

La cuestión reside en cuánto tiempo resistirá Europa como motor legislativo de la nueva revolución digital. A ojos de la comunidad internacional, la regulación europea ha sido acogida favorablemente, pero, Europa necesitará de nuevos aliados de características similares como Japón o Australia si pretende que sus normas sean el estándar regulatorio internacional.

Si la UE no es capaz de sacar el máximo provecho de este marco normativo desde un principio para desarrollar la industria europea propia, muy probablemente nos encontraremos siendo meros clientes y el poder de negociación y establecimiento de normas quedará limitado al ámbito interno de la UE.

2.2 Los retos tecnológicos de Europa

Europa cuenta con el marco político, jurídico y reglamentario más desarrollado en cuestiones digitales del mundo. No está dispuesta a consentir una cesión del dominio tecnológico, por lo que viene adoptando una serie de medidas y políticas digitales, convirtiéndose en una especie de super reguladora (Ortega Klein, 2020).

Es por ello que son varios los retos a los que se enfrenta nuestro continente:

- Como sabemos, la revolución digital produce nuevas tecnologías a una velocidad nunca antes vista. Por ello, Europa debe anteponerse a la llegada de dichas tecnologías a las vidas de los ciudadanos para que su implementación en la sociedad sea segura a través de la **regulación.**

- Europa debe seguir desarrollando su infraestructura tecnológica interna para **reducir la dependencia** que actualmente padece del resto de potencias tecnológicas.

- Europa debe **fomentar** a través de la **inversión** tanto pública como privada la creación de nuevas corporaciones cuyo núcleo de negocio sean los servicios tecnológicos que compitan de tú a tú con las grandes multinacionales americanas y chinas.

2.3 Estrategia Europa 2020 de 2010.

La Comisión Europea publicó en el año 2010 una comunicación dirigida a afrontar los retos que planteábamos bajo el título "EUROPA 2020. Una estrategia para un crecimiento inteligente, sostenible e integrador"[2]. Se trata de un documento cuyo objetivo es la aprobación de diferentes reformas cono respuesta a la entonces reciente crisis económica, así como la definición de los objetivos a largo plazo de la UE en diferentes ámbitos entre los que se encuentra el tecnológico.

El documento estableció 7 iniciativas emblemáticas abarcando diferentes ámbitos como el económico, el educativo o el medioambiental. Es de especial interés para el presente trabajo una de las 7 iniciativas: La Agenda Digital para Europa 2020[3].

El objetivo de la Agenda es impulsar la innovación en el continente aprovechando todo el potencial económico que ya presentaban las TIC y la red.

Esta Agenda contemplaba hasta 101 acciones mediante las que se buscaba la modernización de la UE en un intento de no quedarse fuera de la competencia tecnológica internacional. Uno de los pilares de la Agenda fue el desarrollo de un Mercado Único Digital para Europa, que en particular considero como base indispensable para un verdaderos verdadero desarrollo tecnológico Europeo.

[2] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "EUROPA 2020. Una estrategia para un crecimiento inteligente, sostenible e integrador", COM (2010) 2020 final.

[3] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "Una Agenda Digital para Europa", COM (2010) 0245 final.

Lo mismo que supuso la libre circulación de personas y mercancías en la creación de la propia UE, considero el Mercado Único Digital como la base sobre la que construir toda la transformación digital.

2.4 Una Estrategia para el Mercado Único Digital de 2015[4]

No fue hasta el año 2015 que la UE desarrolló las acciones que se contemplaban en la Agenda Europea 2020 en relación al Mercado Único Digital. La Comisión Europea adoptó en 2015 la Estrategia única para el Mercado Único Digital de Europa. Son varios los puntos clave de este documento que pretendía trazar las líneas de acción para un Europa líder en economía digital como parte del programa de la Agenda Digital para Europa 2020.

En el propio documento, se define el Mercado Único Digital como "aquél en el que la libre circulación de mercancías, personas, servicios y capitales está garantizada y en el que personas y empresas pueden acceder fácilmente a las actividades y ejercerlas en línea en condiciones de competencia, con un alto nivel de protección de los datos personales y de los consumidores, con independencia de su nacionalidad o lugar de residencia."

El principal objetivo del Mercado Único no es otro que la eliminación de las barreras que actualmente existen en el ámbito digital en dentro de la UE. Reducir estas barreras supone una oportunidad sin precedentes que permitiría, entre otros servicios, digitales de mayor calidad, precios más competitivos o nuevos puestos de trabajo. La propia estrategia estima que la eliminación de los obstáculos generaría un importe de hasta 415.000 millones para el PIB europeo.

La Comisión establece 3 pilares para el mercado único digital:

[4] Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, "Una Estrategia para el Mercado único Digital de Europa", COM (2015) 192 final.

- "Mejorar el acceso de los consumidores y empresas a los bienes y servicios transfronterizos".

Han de eliminarse las diferencias normativas interestatales, principalmente en materia de derecho contractual, derecho de la propiedad intelectual y derecho fiscal. La fragmentación normativa en estas materias anula la idea de un comercio electrónico transfronterizo sólido en el que no haya discriminaciones a los clientes.

Se evidencia la necesidad del establecimiento de una serie de normas comunes, eficaces y simples en su aplicación que promocionen el comercio en línea transfronterizo.

- "Crear las condiciones adecuadas para que las redes y los servicios digitales prosperen".

Por un lado, no debemos olvidar que el Mercado Único Digital debe proteger los derechos fundamentales de los consumidores (intimidad, protección de datos…). Si bien en un pasado se dieron pasos en el establecimiento de un marco regulatorio para los medios de comunicación, por ejemplo, con la aprobación de la Directiva de Servicios de Comunicación Audiovisual (Directiva 2010/13/UE[5], ya actualizada por la Directiva 2018/1808/UE[6]), consideran necesario hacer una revisión de la legislación existente para diseñar un marco regulador de las plataformas de servicios en línea actuales (redes sociales, buscadores, plataformas de *streaming*, comercio electrónico etc.).

Por otro, tampoco se debe dejar pasar por alto el enorme poder que ejercen las grandes plataformas en línea en el mercado digital. El control que ejercen en el acceso a sus plataformas, su fuerte poder de negociación con clientes y competidores y la falta de

[5] Directiva (UE) nº 13/2010 del Parlamento Europeo y del Consejo de 10 de marzo de 2010 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual).

[6] Directiva (UE) nº 1808/2018 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), habida cuenta de la evolución de las realidades del mercado.

transparencia suponen un fuerte riesgo para los derechos de la parte débil de la relación contractual. La propia estrategia recoge que el 72% de los europeos teme por la cantidad de datos que ceden a empresas al hacer uso de sus servicios.

Así el refuerzo de la confianza y la seguridad en los servicios digitales que una vez más pasan por la necesidad de establecer un marco normativo sólido y transfronterizo.

- "Aprovechar al máximo el potencial de crecimiento de la economía digital europea".

Si la UE pretende ser competitiva deberá digitalizar todos sus sectores. Para ello tanto las empresas como las administraciones públicas deben integrar las tecnologías digitales avanzadas.

Según el documento, el sector Big Data, por ejemplo, crece a un ritmo del 40% anual. Sin embargo, para poder aprovechar al máximo sus capacidades, la UE debe contar con la infraestructura necesaria para almacenar información que después será procesada en diferentes actividades económicas.

Pero todo el partido que podría sacar la UE de los datos se puede ver afectado por la fragmentación de infraestructura actual (local) y por una falta de interoperabilidad y reutilizabilidad de los datos en toda la UE.

Por ello, la UE debe ser capaz, por un lado, de atraer inversión tanto privada como pública creando un clima de inversión favorable para las redes digitales para el desarrollo de infraestructuras comunitarias centralizadas y, por otro, retener el talento y conocimiento de ciudadanos duchos en esta materia.

En definitiva, puede concluirse que gran parte del éxito en la creación de un mercado digital único pasa por ser capaces de establecer normas y directrices comunes para los Estados Miembros que por un lado sean sólidas y generen una confianza en los ciudadanos pero que al mismo tiempo sean de fácil implementación tanto por agentes

públicos como privados de forma que se siga fomentando la inversión en tecnología europea.

En cualquier caso, considero que a día de hoy la fragmentación estatal en materias como la transferencia de datos que analizaremos después demuestran que aún estamos en una fase casi embrionaria de este mercado.

3. LA REGULACIÓN EUROPEA

Como hemos visto, la Unión hace años que es consciente tanto de los retos como del potencial que supone la digitalización. En el enfrentamiento de dichos retos, el establecimiento de un entorno seguro resultará clave como se señalaba en la Estrategia para el Mercado Único Digital. En la consecución de dicho entorno, la regulación resulta esencial.

Dicho lo cual, la defensa de los derechos fundamentales y las libertades de los ciudadanos de la UE siempre ha sido una prioridad frente a la adopción de cualquier política o estrategia de digitalización o industrialización.

La UE ha realizado esfuerzos por la normativización y actualización de las normas existentes para adaptarse a las necesidades de la sociedad actual. Claro ejemplo de ello son normas como la Directiva 2016/1148/UE[7] sobre la seguridad de las redes y sistemas de información, la Directiva 2018/1808/UE de servicios de comunicación audiovisual o el RGPD, siendo esta última aún a día de hoy la norma adoptada con mayor relevancia tanto jurídica como social en relación a la estrategia digital de la UE.

[7] Directiva (UE) nº 1148/2016 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Pero como venimos analizando, la posición geopolítica de la UE dependerá en gran parte de su capacidad para anteponerse en el futuro a sus competidores en aquellos ámbitos en los que la UE pueda destacar (como el caso de la Inteligencia Artificial).

Evidentemente, por razones físicas la UE no podrá competir en extracción y procesamiento de materias primas con el gigante asiático o difícilmente podrá sobrepasar a EEUU en la oferta de servicios punteros, pero podrá destacar en ser pionera en ofrecer un entorno seguro en el que desarrollar servicios punteros y que esto suponga un atractivo para la inversión extranjera.

Por todo ello, a continuación, se analizará el RGPD, en relación a aquellas cuestiones que, por un lado, han supuesto una mayor litigiosidad a la hora de aplicarse y, que, por otro, advierten de la eficacia de la UE a la hora de aplicar las disposiciones de la misma, sobre todo sobre agentes extracomunitarios, así como la imposición de sanciones económicas.

3.1 Reglamento General de Protección de Datos – Reglamento (UE) 2016/679.

Fruto del mencionado acondicionamiento normativo al que se aludía en la estrategia para el Mercado Digital Único Europeo, se aprobó el Reglamento General de Protección de datos.

El RGPD tenía por objeto actualizar el marco normativo existente en relación a la protección de datos adaptándolo a las necesidades modernas, derogando la Directiva 95/46/CE. Si bien es cierto que dicha norma ya hacia frente a varios de los retos que la protección de datos planteaba, era evidente la necesidad de adaptar una norma adoptada en 1995 a la realidad digital.

Puesto que la recopilación de datos a nivel global se ha visto exponencialmente aumentada, tanto por la capacidad de generar datos sobre casi cualquier actividad que llevemos a cabo los humanos como por la capacidad de almacenamiento de los mismos, organismos públicos y privados han advertido la oportunidad que supone el buen uso de los mismo, principalmente de carácter económico.

Por un lado, el RGPD suponía una actualización a la legislación europea por su capacidad de unificación legislativa de los Estados Miembros, por la propia naturaleza de la norma que no requiere de una trasposición estatal como sí la requería la norma previa, dando margen a una mayor fragmentación normativa.

Por otro, supuso también un precedente a nivel global tanto por su contenido como por su ámbito de aplicación puesto que, también extiende su alcance a agentes externos a la UE al abrir la puerta a que los tratamientos de datos de europeos realizados fuera del territorio de la UE quedaran sujetos a la legislación europea.

Este objetivo fue cuanto menos ambicioso teniendo en cuenta la disparidad de estándares de tutela del derecho a la protección de datos.

La protección de datos personales se configuró como un derecho fundamental (artículo 8.1[8] de la CDFUE y 16.1[9] del TFUE). No obstante, siguiendo la premisa que mencionábamos anteriormente, la UE, consciente de su posición geopolítica estratégica se adelanta estableciendo una norma de aplicación extracomunitaria.

a) Principios establecidos por el RGPD

El artículo 5 recoge los principios que salvaguarda el Reglamento que la AEPD clasifica y describe de la siguiente manera[10]:

- Principio de "licitud, transparencia y lealtad". Los datos han de ser tratados lícitamente y de forma leal y transparente al interesado.

[8] Artículo 8.1 CDFUE: "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan."

[9] Artículo 16.1 TFUE: "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan."

[10] Agencia Española de Protección de Datos (2019). Principios del Reglamento de Protección de Datos. Obtenidos el 30/03/2021 de https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios

- Principio de “limitación de la finalidad”. Los datos han de tratarse para una o varias finalidades “determinadas, explícitas y legítimas”. Los datos no podrán por tanto ser tratados para un fin distinto a ellos.

- Principio de “minimización de datos”. Los datos han de ser los necesarios y pertinentes para con los fines que se determinen.

- Principio de “exactitud”. Los datos han de ser exactos y actualizados si es preciso. Han de tomarse las medidas necesarias para que se rectifiquen o eliminen datos inexactos.

- Principio de “limitación del plazo de conservación”. La conservación de los datos también ha de ser limitada en el tiempo, de forma que no se extienda más allá del tiempo necesario para lograr los fines para los que se recopilaron.

- Principio de “integridad y confidencialidad”.

Destaca además, como principio más importante el de “Accountability” o responsabilidad proactiva en el cumplimiento de la normativa de protección de datos (Biurrum Abad, 2017).

Los responsables habrán de aplicar las medidas técnicas y organizativas necesarias para demostrar que todo tratamiento se realiza de acuerdo a las disposiciones de la norma.

Esto implica que las empresas deben demostrar que cumplen con la norma y no debe hacerlo ya la administración.

También se prevé un régimen sancionador común en la Unión, rompiendo con la impunidad que reinaba bajo la anterior Directiva al mismo tiempo que se incorporan nuevos derechos denominados por ese mismo autor como “derechos digitales” (Rallo Lombarte, 2018).

b) <u>Conceptos clave:</u>

La norma gira en torno a la protección de datos personales de los ciudadanos europeos. Para ello, define y configura nuevos conceptos que desde la entrada en vigor de la norma han adquirido una relevancia singular.

El propio RGPD en su artículo 4 recoge un listado de 26 definiciones necesarias para la comprensión y aplicación de la norma. De todas ellas, nos serán útiles para el posterior análisis de la efectividad e implicaciones de derecho internacional privado las siguientes:

a) Datos personales

El artículo 4.1 los define como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;".

Es una definición que no solo incluye aquellos datos que directamente puedan identificar a una persona sino también aquellos datos que identifiquen a la persona de forma indirecta de forma que han de relacionarse diferentes datos hasta llegar a ella siempre que no "suponga un esfuerzo desproporcionado en cuanto a los medios o el tiempo que se ha de emplear para llegar a identificarle" (Muñoz Ontier, 2018).

Además, es un concepto amplio que abarca incluso datos que permitan simplemente identificar a la persona, lo cual no conlleva que sea necesario conocer su nombre y apellido bastando una dirección IP en determinados casos (de Miguel Asensio, 2015.II).

b) Tratamiento

Por tratamiento el reglamento entiende "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta,

utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"

c) Responsable de Tratamiento

El responsable queda definido como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;".

Junto con el Encargado de Tratamiento que se describe a continuación, es uno de los sujetos que participan en el tratamiento de los datos. El Dictamen 1/2010 emitido por el GT29 ya estudió este concepto para la Directiva 95/46/CE determinando que la función principal del responsable es establecer quién es responsable de que un determinado tratamiento de datos sea acorde a las disposiciones del RGPD. Es quien tiene mayor margen de maniobra y control sobre cómo se realiza dicho tratamiento. Puede determinarse quién es el responsable por criterios de hecho o por atribución legal. A su vez es su función designar quien será el encargado del tratamiento de los datos, que podrá ser el propio responsable o un tercero.

d) Encargado del Tratamiento

Como acabamos de comentar es una persona que realiza el tratamiento de datos por cuenta del responsable. El RGPD lo define como "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;".

Si bien el artículo 28 RGPD estipula la relación jurídica que existirá entre el responsable y el encargado, resultando lo más habitual que dicha relación sea contractual, el mencionado Dictamen 1/2010 no considera dicho contrato decisivo para la constatación de la existencia de la relación jurídica. La determinación ha de realizarse caso por caso

por lo que podrá considerarse responsable de una vulneración de derechos a alguien que actúe de hecho como encargado sin que exista contrato que así lo estipule.

e) Interesados

Son aquellas personas físicas a las que pertenecen los datos personales que son tratados por el responsable o por el encargado del tratamiento. El RGPD los define como "persona física identificada o identificable"

3.2 Eficacia del Reglamento General de Protección de Datos

Resulta de especial interés para este estudio las implicaciones de derecho privado de las disposiciones del RGPD y la resolución por parte de la justicia europea de los conflictos.

La efectividad de este Reglamento resulta de gran importancia puesto que supone el precedente de referencia para la futura regulación de la UE en materia tecnológica y digital.

Partiendo de la base que venimos comentando de que la regulación es una de las mejores herramientas que tiene la UE a la hora de competir en el plano internacional, es predecible que del éxito de esta norma dependerá el de las futuras.

Bien es cierto además que no podemos saber hasta qué punto los países extracomunitarios cumplirán con todas aquellas normas comunitarias que la UE imponga, especialmente si la UE deja de ser un punto estratégico para los bloques EEUU-China. Sin embargo, la coyuntura actual favorece que la UE aproveche el momento e intente imponer las normas de juego por lo menos en su territorio.

Sin embargo, este objetivo no resulta sencillo. Por ello, analizamos a continuación cómo se enfrenta el Reglamento a las dificultades que supone la defensa de los derechos y libertades de los ciudadanos europeos frente a las amenazas internacionales.

3.3 Reglas de Derecho Internacional Privado en el RGPD.

3.3.1 Competencia Judicial Internacional

a) Reglas de Competencia judicial internacional del Reglamento General de Protección de datos

En derecho privado, el lugar de situación del afectado por el tratamiento de datos es un criterio legítimo para determinar la ley aplicable y la competencia internacional (Conferencia de la Haya de Derecho Internacional Privado, 2000).

El artículo 79 RGPD, por remisión del artículo 82, es el que determina la competencia judicial internacional. Se establece que para acceder a la tutela judicial efectiva a través de la interposición de una acción contra un encargado o responsable de tratamiento las acciones deberán dirigirse ante los tribunales competentes del Estado Miembro donde estos tengan un establecimiento.

El afectado podrá así interponer su demanda en el Estado Miembro donde el responsable o encargado del tratamiento de los datos tenga su establecimiento, atendiendo al concepto flexible de establecimiento derivado de la sentencia Weltimmo que analizaremos en los supuestos del apartado "Ámbito de aplicación". Así, aunque un establecimiento en concreto no tenga que ver con la actividad concreta que origina la acción lesiva de derechos, el afectado podrá dirigirse a los tribunales del Estado Miembro en el que esté ubicado dicho establecimiento.

También existe la posibilidad de dirigirse a los tribunales del Estado del lugar de residencia habitual del interesado en ejercer la acción (Cdo. 145).

Observamos en dicho considerando que el Reglamento permite como foro alternativo demandar ante los tribunales del Estado en el que el afectado tenga su residencia habitual, si bien no parece la mejor opción para la protección de los derechos del afectado por dar lugar a situaciones en las que se demandaría ante los tribunales de un Estado en el que quizás el daño ni si quiera se había producido (Orejudo Prieto de los Mozos, 2013).

Por tanto, nos encontramos con una doble posibilidad dentro del RGPD, que en principio favorece al interesado en tanto en cuanto puede optar por dirigirse a los tribunales allí donde considere que le sea más favorable.

No obstante, la acción de responsabilidad, recogida en el artículo 82 es de carácter civil, y, por tanto, también es de aplicación el artículo 1.1 del Reglamento (UE) 1215/2012 "Bruselas I Bis" puesto que, además, es una materia que no está incluida entre las exclusiones del artículo 1.2 de dicho reglamento[11].

El Reglamento Bruselas I bis es un Reglamento de aplicación a los Estados de la Unión que trata de facilitar el acceso a la justicia aclarando asuntos sobre competencia judicial y sobre sobre el reconocimiento y la ejecución de las resoluciones judiciales en materia civil y mercantil (European Justice, 2020).

b) Reglas de competencia judicial internacional del Reglamento Bruselas I bis

En relación al foro existe cierta confusión entre el determinado por el artículo 79.2 del RGPD (norma específica) frente al establecido por el Reglamento Bruselas I bis en su artículo 67. En este último, se recoge el principio de especialidad que implica la aplicación prioritaria de lo dispuesto en el RGPD.

No obstante, del Considerando 145 se desprendía que los afectados debían poder tener la opción de elegir ante qué Estado Miembro ejercitar la acción, bien ante el Estado Miembro en el que el responsable/encargado tenga un establecimiento, bien ante el Estado Miembro en que el afectado tenga su "residencia habitual"

Dicho lo cual, el foro podrá determinarse, de acuerdo con el Reglamento Bruselas I bis, de acuerdo con los foros prevalentes (sumisión y domicilio del demandado) o los especiales en atención a su cualificación, bien extracontractual o contractual.

a) Sumisión tácita del artículo 26 cuando l demandante presenta demanda ante el tribunal de un determinado Estado Miembro y el demandado comparece.

[11] Reglamento (UE) nº 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.

b) Sumisión expresa en virtud del artículo 25 que determina que *si las partes han acordado que un órgano u órganos jurisdiccionales de un Estado Miembro sea competente para conocer los litigios surgidos con ocasión de una relación jurídica tales órganos serán competentes* siempre que dicho acuerdo sea acorde al derecho de dicho Estado Miembro. Se trata de una vía poco utilizada en la práctica.

c) Domicilio del demandado (foro recogido en el artículo 4). A falta de pacto expreso o tácito, el tribunal del domicilio del demandado será el competente. En el caso del Reglamento Bruselas I bis se entiende por domicilio de una persona física aquel que determine la normativa nacional de cada estado en el que dicha persona tenga su residencia habitual y para las personas jurídicas: el estado en el que se encuentre su sede estatutaria, su administración central o su centro de actividad principal.

d) Foro especial en materia extracontractual. Lugar donde se hubiere producido o pudiere producirse el hecho dañoso. El artículo 7.3 establece este foro para las acciones extracontractuales por daños y perjuicios. Este es el criterio más habitual a la hora de determinar el foro (Ortega Giménez, 2013). Sin embargo, no es fácil determinar donde se ha producido el daño puesto que es común que el acto que genera el daño ocurra en un determinado estado, pero el resultado lesivo se produzca en otro distinto o incluso en varios, dando pie a poder reclamar por los daños en varios estados.

   La STJUE eDate Advertising[12], reduce esa *dispersión competencial* al permitir que el afectado pueda exigir la indemnización total de los daños o perjuicios sufridos bien en el Estado promotor de la acción o bien allí donde la víctima tenga su centro de interés.

[12] Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Gran Sala) de 25 de octubre de 2011, C-509/09. eDate Advertising GmbH y otros contra X y Société MGN LIMITED.

e) Foro especial en materia contractual. Lo más habitual será que una vulneración de derechos de un ciudadano como consumidor, por lo que en estos casos habrá que estar a lo dispuesto en los artículos 17 a 19.

El artículo 18 determina el tribunal competente en los dos casos que pueden darse en el caso de contratos con consumidores: que el demandante sea el consumidor o que el demandante sea la otra parte.

En el caso en que el demandante sea el consumidor, el artículo 18 prevé que la acción contra la parte contratante "podrá interponerse ante los órganos jurisdiccionales del Estado miembro en que esté domiciliada dicha parte o, con independencia del domicilio de la otra parte, ante el órgano jurisdiccional del lugar en que esté domiciliado el consumidor". Es decir, el consumidor podrá dirigirse tanto a los órganos judiciales de su propio domicilio como a los del domicilio de la otra parte.

En el caso contrario en el que la otra parte sea la demandante, esta solo podrá interponer la acción "ante los órganos jurisdiccionales del Estado miembro en que esté domiciliado el consumidor".

Es decir, el Reglamento recoge un principio de *favor debilis* por el cual el consumidor siempre tendrá la opción de acudir, tanto cuando sea demandante como cuando sea demandado, a los órganos judiciales de su domicilio.

3.3.2 Derecho aplicable

El ámbito de aplicación del Reglamento se encuentra definido en el artículo 3 del RGPD, en el que claramente se aprecia la intención de la UE de que la norma sea de aplicación global.

En la Directiva 95/46/CE el artículo 4 titulado "Derecho nacional aplicable" determinaba qué regulación de las 28 de la UE debía aplicarse en la defensa del derecho de protección de datos. El artículo 3 RGPD, salvo en determinadas excepciones como la del art. 8

RGPD, acaba con esta fragmentación normativa sometiendo a la totalidad de los Estados Miembros a una única norma.

Como es evidente, este artículo ha sido foco de litigios desde su entrada en vigor. Varios de los conceptos que recoge el artículo han sido ya objeto de interpretación judicial por el TJUE en asuntos clave para poder valorar el éxito de la aplicación del RGPD en el plano extracomunitario.

Así, de la interpretación del propio artículo 3 emitida por el Grupo de Protección de datos en el Dictamen 8/2010[13] sobre el Derecho aplicable actualizado y la doctrina del TJUE podemos concluir que el RGPD establece tres escenarios en los que el RGPD será de aplicación.

a) En primer lugar, será aplicación al tratamiento de datos personales por el responsable o encargado establecido en la UE independientemente de que dicho tratamiento tenga lugar en la UE o no.

b) En segundo lugar, será de aplicación al tratamiento de datos de interesados que residan en la UE aunque el responsable o encargado no esté establecido en la UE siempre que el tratamiento tenga que ver con la oferta de bienes o servicios a dichos interesados en la UE, independientemente de que se les requiera un pago o no a los interesados.

c) En tercer lugar, también será de aplicación al tratamiento de datos de interesados que residan en la UE aunque el responsable o encargado no esté establecido en la UE siempre que el tratamiento tenga que ver con el control de su comportamiento cuando este tenga lugar dentro de la UE.

[13] Dictamen nº 8/2010 del 16 de diciembre de 2010, sobre el Derecho aplicable emitido por el Grupo de Protección de Datos del artículo 29 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

a) En caso de tratamiento de datos por un encargado o responsable con establecimiento en la UE.

El artículo 3.1 RGPD determina que el Reglamento será de aplicación "al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la UE, independientemente de que el tratamiento tenga lugar en la UE o no."

El término establecimiento deja campo a la interpretación y es por ello que ha sido protagonista de debate jurisprudencial. Viene definido en el Considerando 22 como que "un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto"

La STJUE Weltimmo[14] consolidó el concepto de establecimiento como un concepto flexible (párrafo 29) "que rechaza cualquier enfoque formalista según el cual una empresa estaría establecida únicamente en el lugar en que se encontrase registrada. Por lo tanto, para determinar si una sociedad, responsable de un tratamiento de datos, dispone de un establecimiento […] para ello procede interpretar tanto el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades en ese otro Estado miembro tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión […]".

En el marco del art. 3.1 RGPD, el TJUE ha terminado por concluir un solo representante en otro Estado Miembro puede bastar si actúa con un grado de estabilidad suficiente (de Miguel Asensio, 2015.I). Es decir, basta cualquier actividad real y efectiva ejercida de manera estable.

[14] Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Sala Tercera) de 1 de octubre de 2015, C-230/14. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság.

Pero, además de ello, para esclarecer controversias en relación a qué sucede en los casos en los que existen varios establecimientos en el territorio de la UE, el propio RGPD define en su artículo 4. 16) el concepto de *establecimiento principal* además de determinar reglas de especialidad y jerarquía para determinar cuál de los posibles varios establecimientos que tenga el encargado o responsable en la UE es el principal (Gonzalo Doménech, 2018).

En él se establece que será establecimiento principal:

*a) En lo que se refiere a un **responsable** de tratamiento establecimientos en más de un Estado Miembro, el lugar de su administración central en la UE, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la UE y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;*

*b) en lo que se refiere a un **encargado** del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la UE o, si careciera de esta, el establecimiento del encargado en la UE en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;*

Asimismo, el tratamiento debe darse *en el contexto de las actividades del establecimiento*. El Dictamen 8/2010 ha establecido dos elementos clave para poder afirmar que el tratamiento sucede en dicho contexto:

1. El grado de implicación del establecimiento en las actividades en cuyo contexto se traten los datos.

2. La naturaleza de las actividades del establecimiento.

Además, debemos también tener en cuenta la doctrina de la STJUE Google Spain[15] debe también determinarse si la actividad de un establecimiento local y el tratamiento de datos puedan estar "indisociablemente ligadas" como determina el tribunal en su fundamento número 56.[16]

Así, incluso si un establecimiento no establecido en la UE realiza un tratamiento de datos de un ciudadano de un Estado Miembro en el que tiene un establecimiento local pero dicho establecimiento no trata los datos, la legislación europea puede aplicarse a dicho responsable o encargado extracomunitario cuando se confirme esa vinculación como sucedió en la mencionada STJUE Google Spain.

b) Supuesto de tratamiento de datos relacionados con oferta de bienes o servicios en la UE.

En este escenario resulta relevante la aplicación del art. 3.2 RGPD, puesto que es el artículo que realmente amplía el alcance de la norma. Como se mencionaba antes, el

[15] Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Gran Sala) de 20 de junio de 2014, C-131/12. Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González

[16] Párrafos 54-56 de la STJUE Google Spain:

55- Habida cuenta de este objetivo de la Directiva 95/46 y del tenor de su artículo 4, apartado 1, letra a), procede considerar que el tratamiento de datos personales realizado en orden al funcionamiento de un motor de búsqueda como Google Search, gestionado por una empresa que tiene su domicilio social en un Estado tercero pero que dispone de un establecimiento en un Estado miembro, se efectúa «en el marco de las actividades» de dicho establecimiento si éste está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor.

56- En efecto, en tales circunstancias, las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades.

57- Sobre este particular, es necesario recordar que, como se ha precisado en los apartados 26 a 28 de la presente sentencia, la propia presentación de datos personales en una página de resultados de una búsqueda constituye un tratamiento de tales datos. Pues bien, toda vez que dicha presentación de resultados está acompañada, en la misma página, de la presentación de publicidad vinculada a los términos de búsqueda, es obligado declarar que el tratamiento de datos personales controvertido se lleva a cabo en el marco de la actividad publicitaria y comercial del establecimiento del responsable del tratamiento en territorio de un Estado miembro, en el caso de autos el territorio español.

criterio aquí tiene que ver con la proyección de la oferta de servicios que realiza el encargado o responsable externo lo que facilita la aplicación de la legislación europea a agentes establecidos fuera del territorio de la UE.

El Considerando 23 considera una serie de indicios como la lengua, la moneda o la mención de clientes residentes en la UE como determinantes para concluir la existencia de esa proyección. La STJUE Weltimmo considera aún más indicios. Parece que las SSTJUE Pammer y Hotel Alphenor[17], Mühlleitner[18] y Emrek[19] terminan por establecer el criterio aplicable (de Miguel Asensio, 2017).

En Pammer se determina que han de tenerse en cuenta "todas las manifestaciones de voluntad de atraer a los consumidores de dicho Estado". También ofrece una lista no exhaustiva de indicios. Otros consideran que también es posible apreciar la proyección de la oferta a ciudadanos de la UE cuando la oferta se realice de forma mundial sin establecer restricciones que afecten a la UE y los productos o servicios son adquiridos por un amplio número de ciudadanos de la UE, siendo esta una corriente doctrinal establecida por el TJUE cuyo origen es el caso Calder v. Jones resuelto por la Corte Suprema estadounidense (Gonzalo Doménech, 2018) .

> c) Actividades de tratamiento de datos de monitorización del comportamiento de usuarios cuando este comportamiento tiene lugar en la UE.

El art. 3.2 b) parece que limita el alcance de su protección a casos en los que el comportamiento monitorizado suceda en la UE. El Considerando 24 define control de comportamiento como "un seguimiento en internet, inclusive el potencial uso posterior

[17] Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Gran Sala) de 7 de diciembre de 2010, C-585/08 y C-144/09. Peter Pammer contra Reederei Karl Schlüter GmbH & Co. KG y Hotel Alpenhof GesmbH contra Oliver Heller.

[18] Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Sala Cuarta) de 6 de septiembre de 2012, C-218/12. Daniela Mühlleitner contra Ahmad Yusufi y Wadat Yusufi.

[19] Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Sala Tercera) de 17 de octubre de 2013, C-218/12. Lokman Emrek contra Vlado Sabranovic.

de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes."

Así, parece que se dejan para la aplicación del anterior escenario las actividades dirigidas a promocionar u ofertar bienes o productos a los ciudadanos y se centra este apartado en la elaboración de perfiles, análisis de sentimiento o definir patrones de conducta en la red de los usuarios (Gonzalo Doménech, 2018). En mi opinión, en la mayoría de los casos la monitorización del comportamiento de los usuarios no es más que la antesala de una posterior estrategia comercial de los responsables o encargados del tratamiento.

3.3.3 Cambios en el acceso a la tutela judicial efectiva en materia de protección de datos desde la entrada en vigor del RGPD.

El incumplimiento[20] de las disposiciones del RGPD por parte de aquellos sujetos a su régimen puede dar lugar a responsabilidad civil, administrativa e incluso penal. La responsabilidad podrá recaer sobre el titular del fichero, el responsable, el encargado, el responsable de seguridad o cualquier otra persona relacionada con los datos a la que le pueda ser atribuida (Gonzalo Doménech, 2018).

Esta responsabilidad y las posteriores posibles sanciones resultan clave para juzgar la eficacia de la UE en la defensa de los derechos de sus ciudadanos, así como para valorar cómo de efectiva está siendo su jugada en el mencionado tablero geopolítico.

[20] Artículo 6 RGPD licitud del tratamiento: "1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones".

Por un lado, la responsabilidad civil del encargado o responsable derivará de su incumplimiento por acción u omisión de las normas civiles; esta responsabilidad podrá ser a su vez contractual cuando se infrinjan obligaciones contenidas en contratos o extracontractual como consecuencia de lesiones cometidas fuera de esa relación contractual.

En cuanto a las responsabilidades contractuales, ante un incumplimiento que lesiona el derecho a la protección de datos la norma determina que en caso de no poder cumplirse con lo estipulado corresponderá indemnizar al damnificado. Estas indemnizaciones son frecuentemente limitadas en los propios contratos en las que incluso se listan los posibles incumplimientos y las indemnizaciones correspondientes a cada una de ellas.

En lo relativo a la responsabilidad extracontractual sirven para proteger a la persona afectada en relación al riesgo generado por el tratamiento de sus datos

Sin entrar a fondo en los requisitos judiciales para la contemplación de un daño efectivo que dé lugar a dichas responsabilidades, podemos afirmar que el RGPD contempla en sus preceptos una acción de responsabilidad civil extracontractual.

El RGPD prevé al contrario que la anterior Directiva en su art. 82 el derecho a indemnización por daños causados por el incumplimiento de las disposiciones del reglamento:

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente ***Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización*** *por los daños y perjuicios sufridos.*

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente

Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios […].

En el precepto se recoge la responsabilidad directa tanto del responsable como del encargado del tratamiento; limitando la responsabilidad del encargado bajo ciertos supuestos. El propio apartado 3 del artículo recoge los supuestos de exoneración de la responsabilidad de estos, si son capaces de demostrar que no son responsables del daño.

Los daños indemnizables son tanto materiales como inmateriales de acuerdo con la interpretación del concepto de *daños y perjuicios* que realizó el TJUE en Liffers[21]. Por la propia naturaleza de los derechos en cuestión lo más habitual es que se trate de daños morales, y, puesto que la reparación consiste en una indemnización debe poder determinarse una forma de cuantificación del daño.

En la STS 261/2017 de 26 de abril, para el caso de indemnización derivada de incumplimiento se consideraron relevantes el tiempo de permanencia de los datos, el alcance de su divulgación y la inacción por parte del responsable o encargado.

En cualquier caso, como mencionábamos al inicio de este apartado, la acción que prevé el reglamento no excluye la vía administrativa por la que se puede reclamar ante el contecioso administrativo la imposición de sanciones por incumplimiento bien del RGPD como de la LOPD en el caso español o la correspondiente normativa nacional de los Estados Miembros.

3.4 Régimen sancionador e informe de las sanciones impuestas hasta la fecha.

[21]Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Sala Quinta) de 17 de marzo de 2017, C-99/15. Christian Liffers contra Producciones Mandarina, S.L., y Mediaset España Comunicación, S.A., anteriormente Gestevisión Telecinco, S.A.

Los artículos 82 y 83 del RGPD suponen una gran novedad con respecto a la Directiva 95/46/CE puesto que configuran un régimen sancionador por el incumplimiento de las disposiciones del RGPD. Ya hemos analizado previamente el derecho a indemnización que recoge el artículo 82.

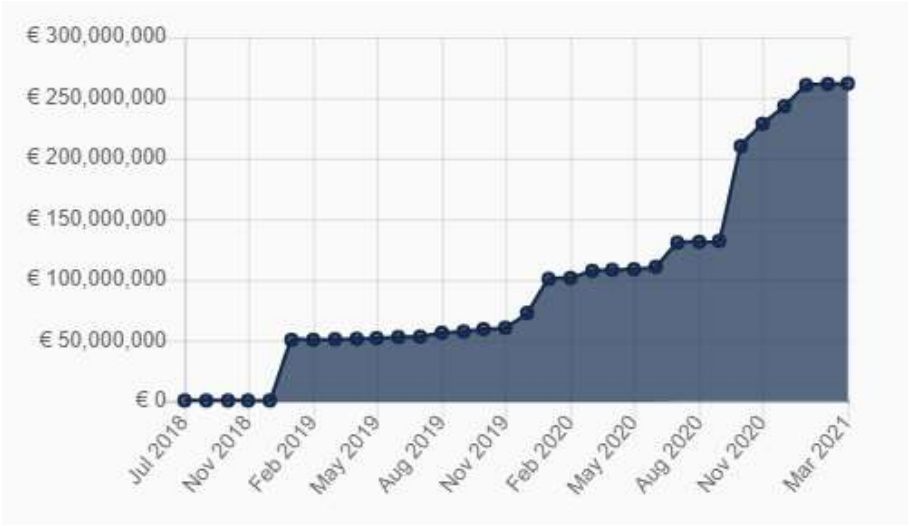
Las consecuencias de una infracción del reglamento son sanciones que se imponen en función de las circunstancias individuales de cada caso. En el artículo 83 se estipulan diferentes tipos de infracciones en función de su naturaleza, gravedad, duración o intencionalidad (Iberley, 2018).

Nos encontramos con un régimen sancionador severo que estipula multas administrativas de hasta 20.000.00 EUR o de hasta el 4% del volumen de negocio total anual global del ejercicio financiero anterior en caso de que el infractor sea una empresa (optando además siempre por la mayor cuantía de las dos)[22].

Las autoridades de control son las encargadas de garantizar la imposición de las multas administrativas. En el caso de España la autoridad de control es la Agencia Española de Protección de Datos.

Si observamos los datos históricos, veremos que tanto el número como la cuantía de las sanciones impuestas por violación de las disposiciones del RGPD ha aumentado de manera significante desde 2018 (GDPR Enforcement Tracker, 2020) (Figura 1 y 2)

[22] Artículo 83.5 RGPD.



(Figura 1)

La cuantía acumulada de todas las sanciones impuestas asciende a marzo de 2021 a más de 260 millones de euros. Italia es el país que más ha recaudado con una cuantía total de más de 70 millones. España por otro lado, es el país de la UE que ha impuesto un mayor número de sanciones.

Country	Sum of Fines
ITALY	**€ 70,601,601** (at 51 fines)
FRANCE	**€ 54,661,300** (at 14 fines)
GERMANY	**€ 48,886,833** (at 29 fines)
UNITED KINGDOM	**€ 44,221,000** (at 4 fines)
SPAIN	**€ 16,160,610** (at 190 fines)
SWEDEN	**€ 12,332,430** (at 17 fines)
THE NETHERLANDS	**€ 3,930,000** (at 7 fines)
BULGARIA	**€ 3,210,690** (at 20 fines)
POLAND	**€ 1,786,498** (at 21 fines)
NORWAY	**€ 1,134,450** (at 20 fines)

(Figura 2)

En la siguiente imagen (Figura 3) podemos observar también un ranking de las sanciones impuestas hasta la fecha ordenado por razón de la cuantía entre las que destaca la reciente sanción del 21 de enero de 2019 que la Comisión Nacional de Informática y Libertades (autoridad de control francesa) a Google por la cuantía de 50 millones de EUR. El motivo fue la falta de transparencia, información y consentimiento en el tratamiento de los datos

personales de los ciudadanos para la elaboración de publicidad personalizada a través de su plataforma Google Ads (GDPR Enforcement Tracker, 2020).

	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Google Inc.	Media, Telecoms and Broadcasting	FRANCE	50,000,000	Insufficient legal basis for data processing	21 Jan 2019
2	H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Employment	GERMANY	35,258,708	Insufficient legal basis for data processing	01 Oct 2020
3	TIM (telecommunications operator)	Media, Telecoms and Broadcasting	ITALY	27,800,000	Insufficient legal basis for data processing	15 Jan 2020
4	British Airways	Transportation and Energy	UNITED KINGDOM	22,046,000	Insufficient technical and organisational measures to ensure information security	16 Oct 2020
5	Marriott International, Inc	Accomodation and Hospitality	UNITED KINGDOM	20,450,000	Insufficient technical and organisational measures to ensure information security	30 Oct 2020
6	Wind Tre S.p.A.	Media, Telecoms and Broadcasting	ITALY	16,700,000	Insufficient legal basis for data processing	13 Jul 2020
7	Vodafone Italia S.p.A.	Media, Telecoms and Broadcasting	ITALY	12,251,601	Non-compliance with general data processing principles	12 Nov 2020
8	notebooksbilliger.de	Employment	GERMANY	10,400,000	Insufficient legal basis for data processing	08 Jan 2021
9	Eni Gas e Luce	Transportation and Energy	ITALY	8,500,000	Insufficient legal basis for data processing	11 Dec 2019
10	Caixabank S.A.	Finance, Insurance and Consulting	SPAIN	6,000,000	Insufficient legal basis for data processing	13 Jan 2021

(Figura 3)

4. NUEVA ESTRATEGIA EUROPEA DE DATOS de 2020 [23]

10 años después de la publicación de la Estrategia Europa 2020, la UE decide actualizar su estrategia digital. Así, el 19 de febrero de 2020 la UE publica una serie de iniciativas[24] claves para dicha actualización entre los que se encuentra la Estrategia Europea de Datos.

En esta Comunicación de la Comisión al Parlamento, La Comisión se pronuncia por primera vez acerca de los datos como *insight* de valor y necesario para el desarrollo tecnológico del continente.

La irrupción del Big Data en la sociedad ya es una realidad. La digitalización económica es inminente y el volumen de datos no personales generados y almacenados diariamente

[23] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "Una Estrategia Europea de Datos", COM (2020) 66 final.

[24] Declaración sobre el futuro digital de Europa, Libro Blanco sobre Inteligencia Artificial y la Estrategia Europea de Datos.

aumenta exponencialmente con el paso del tiempo. El volumen de datos producidos en el mundo crecerá desde 33 zettabytes en 2018 hasta una previsión de 175 zettabytes en 2025. Y cada nueva serie de datos supone una oportunidad para la UE.

Precisamente en ese carácter no personal de los datos reside la oportunidad de la UE. Si bien con el analizado reglamento la UE buscó a toda costa la defensa de los derechos fundamentales y libertades de sus ciudadanos parece que ahora busca sacar el máximo rendimiento a los datos que tiene a su alcance.

No obstante, esta optimización de la utilización de estos datos que redunde en una mayor productividad/competitividad no puede suponer una total liberalización del mercado de datos. Por ello, la UE debe basarse en un marco jurídico actualizado y adaptable a las nuevas tecnologías (que permita una gobernanza en el manejo de los datos segura, en materia de protección de datos, seguridad y mejore la ciberseguridad) y en desarrollar un mercado interior digital fuerte. Además de mejorar su gobernanza en el manejo de los datos y aumentar sus repositorios de datos disponibles para su utilización y reutilización.

La UE también se muestra optimista respecto a su posición respecto a los grandes bloques tecnológicos China-EEUU. Pese a que actualmente unas pocas empresas tecnológicas poseen la mayoría de los datos, gran parte de los datos provendrá de aplicaciones industriales, profesionales, de ámbitos de interés público o de la IA, ámbitos en los que la UE se posiciona como pionera.

Dicho lo cual, la Comisión plantea la creación de un **Mercado Único de Datos** (tanto personales como no personales) que sea accesible tanto para las empresas privadas como por las administraciones públicas, pero siempre bajo el control de la regulación europea de protección de datos personales, protección de consumidores y en materia de competencia.

La Estrategia de Datos delimita los retos a los que se enfrenta la UE en relación a la creación de Mercado Único de Datos.

1. Disponibilidad de los datos. El valor del dato reside en su reutilizabilidad y replicabilidad a coste casi cero. No obstante, para poder hacer un uso innovador de los mismos es necesario contar con un gran volumen de datos y que dichos datos sean abiertos. Esto pasa por facilitar el intercambio de datos tanto entre empresas privadas, como entre administraciones públicas como entre el sector privado y el público.

2. Desequilibrio en el poder de mercado. El acceso a datos del mercado en la nube por parte de las pymes es anecdótico. El hecho de que unos pocos actores posean la mayoría de los datos no solo supone una gran ventaja en cuanto a la competencia en sus mercados específicos sino con respecto a otros en los que también tengan o planeen tener actividad. Esta ventaja les permite incluso fijar las normas sobre sus plataformas imponiendo unilateralmente condiciones a sus usuarios.

3. Interoperabilidad y calidad de los datos. Resulta esencial para el despliegue de la IA en la UE. La aplicación de formatos y protocolos compatibles normalizados y compartidos para la recogida, tratamiento de datos debe fomentarse de forma que la UE pueda destacar en el desarrollo de esta nueva tecnología que se presenta como la tecnología más atractiva.

4. Infraestructuras y tecnología de datos: actualmente persisten problemas tanto en cuanto a la oferta como a la demanda de la nube.

   Los proveedores de servicios en la nube establecidos en la UE solo representan pequeña cuota de mercado de la nube, lo que genera una dependencia total de proveedores externos.

   Además, los proveedores que operan en la UE también pueden estar sujetos a legislación de terceros países que contradigan el marco normativo de la UE. (En particular es reseñable, por lo negativo, varias leyes chinas de

ciberseguridad e inteligencia nacional que permiten el acceso a datos de europeos).

5. Oferta: existe una escasa utilización de la nube en Europa. La utilización de la nube por el sector público es baja. Solo una cuarta parte de las empresas y una quitan parte de las pymes la utilizan. Además existen diferencias entre estados miembros en dichos porcentajes.

6. Cualificación y alfabetización en materia de datos: los macro datos y la analítica se encuentran entre los primeros puestos de los sectores con escasez de mano de obra cualificada con un total de 496.000 vacantes en el sector en 2017.

7. Ciberseguridad: Europa ha desarrollado ya un marco exhaustivo para ayudar a los estados. Pero el rápido avance de la tecnología (como el caso de la tecnología Blockchain que permite la portabilidad dinámica de los datos en tiempo real para las personas y empresas) probablemente exiga futuras actualizaciones normativas.

A la vista de estos retos, la propia estrategia recoge 4 pilares en los que ha de basarse la misma determinando para cada uno de esos pilares una serie de medidas clave (ANEXO I)

5. LA INTELIGENCIA ARTIFICIAL

5.1 Inteligencia artificial en el olano internacional

5.1.1 Concepto y desafío

El concepto de Inteligencia Artificial (IA) nace como fruto de una serie de investigaciones científicas a mediados del siglo pasado. Marvin Minsky la definía como la ciencia de hacer que las máquinas realicen actos que requerirían uso de la inteligencia si fueran realizados por los humanos (Minsky, 1972).

Es una ciencia que incluye varias técnicas como el aprendizaje automático, el razonamiento automático y la robótica. A través de ellas la IA trata de emular el funcionamiento de la mente humana, con las consecuencias que ello conlleva.

Es un pensamiento generalizado considerar que el margen de error de las máquinas es menor al de los seres humanos en aquellas tareas en las que las máquinas han alcanzado un desarrollo tecnológico avanzado. Pero, si nos paramos a pensar en cómo actuamos los seres humanos, nos daremos cuenta de que en ocasiones tomamos decisiones irracionales, que no responden a la lógica.

La IA perfecta por tanto sería aquella que también diera lugar a este tipo de actuaciones imprevisibles con los riesgos que ello conllevaría. Sin embargo, en la actualidad no contamos con una regulación que pudiera dar una respuesta efectiva a una posible vulneración de derechos causada por una decisión tomada por una máquina autónoma.

Consecuentemente, esto supone una preocupación y un reto para los legisladores de todo el mundo. Esta tecnología plantea numerosas cuestiones de interés jurídico que analizaremos a continuación llegando a platear incluso la creación de nuevos derechos tanto para la ciudadanía como para las propias máquinas (Núñez Zorrilla, 2019)

5.1.2 La IA y el Derecho Internacional

Isaac Asimov científico y escritor norteamericano señaló en 1942 tres leyes de la robótica.

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

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

3. “Un robot debe proteger su propia existencia en la medida en que esta protección no entre en conflicto con la primera o la segunda ley” (Asimov, 1989).

La idea subyacente en estos tres principios generales es el sometimiento de la robótica a las normas éticas, morales y jurídicas que se aplican a los humanos en la sociedad.

Las instituciones internacionales ya son conscientes de la inminente llegada de la IA a la sociedad y de los riesgos para los derechos humanos y libertades fundamentales que conlleva esta nueva tecnología.

Como ejemplo de ello la OCDE adoptó en mayo de 2019 los *Principios Éticos en materia de la Inteligencia Artificial*[25] . Fueron adoptados por 42 países y un mes después se incluyeron en la Declaración Ministerial sobre Comercio y Economía Digital del G20 en su cumbre de Japón.

Naciones Unidas también ha comenzado a llevar a cabo diversas iniciativas como la creación del centro para la robótica y la IA adscrito al Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia en la Haya o la promoción de la Unión Internacional de Telecomunicaciones que investiga y elabora informes sobre la IA como el reciente paper "United Nations Activities on Artificial Intelligence"[26].

No obstante, la regulación de la Inteligencia Artificial es a día de hoy prácticamente inexistente con contadas excepciones. Por nombrar alguna Nueva Zelanda ya ha aprobado una norma que regula el uso de algoritmos por parte de la administración pública[27]. Más

[25] Consejo de la OCDE (2019). Principios de la OCDE sobre la Inteligencia Artificia. Obtenido el 08/04/2021 de https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[26] Unión Internacional de Telecomunicaciones (2019). United Nations Activities on Artifcial Intelligence (AI). Obtenido el 01/04/2021 de https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2019-1-PDF-E.pdf

[27] Parlamento de Nueva Zelanda (2020). Carta de Algoritmos de Nueva Zelanda. Obtenida el 05/04/2021 de: https://data.govt.nz/manage-data/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/#signatories

común es la aprobación de algún tipo de estrategia relativa a la IA la American Artificial Intelligence Initiative[28] promulgada por la administración Trump en 2019.

En definitiva, podemos concluir que con carácter general no existe todavía una regulación de la IA. Si bien es cierto que se han adoptado algunos principios como los mencionados *Principios Éticos en materia de la Inteligencia Artificial de la OCDE*, que no dejan de ser de soft law que por supuesto no vinculan legalmente a aquellos que los adoptan.

5.1.3 Posible regulación internacional

García San José se plantea la necesidad de establecer un marco normativo internacional que encare la protección de los derechos humanos de los riesgos asociados la implantación de la IA en la sociedad. Este autor aboga por un marco normativo que supere la división clásica del *Hard law / Soft law*: y que pueda calificarse de *Global Law (García San José, 2021).*

García San José descarta primero la viabilidad de una norma de *Hard law* como pudiera ser un tratado. Esta parecería quizás la solución más adecuada en tanto y cuanto la adopción de un tratado por parte de un Estado vincula al mismo legalmente y por tanto brindaría una mayor protección a los nacionales de dicho Estado. Sin embargo, la rigidez de este tipo de acuerdos dificulta en muchas ocasiones su ratificación.

El autor compara las dificultades que ha venido encontrando la Conferencia de la Haya para normativizar temas como la gestación subrogada. La propia naturaleza de la IA y su potencial para evolucionar rápidamente pronostican poco éxito a una posible ratificación multitudinaria de un tratado que intente regularla.

También descarta la conveniencia de una norma de *Soft law* como los ya adoptados Principios de la OCDE. Se trata en este caso de mecanismos (declaraciones, programas

[28] Office of Science and Technology Policy. (2019). American Artificial Intelligence Initiative. Obtenida el 01/04/2021 de: https://www.nitrd.gov/nitrdgroups/images/c/c1/American-AI-Initiative-One-Year-Annual-Report.pdf

de acción etc.) que no son legalmente vinculantes para aquellos que los adopten pero que demuestran la conformidad de los Estados con las disposiciones que en ellos se recogen.

En esta ocasión sucedería lo contrario, y es que puesto que no se trata de un mecanismo que vincule a aquel que lo acepta, su adopción resulta más sencilla pero no parece acorde a los principios éticos y de seguridad que las instituciones internacionales vienen demandando para la IA.

El autor propone desarrollar una norma de Derecho Global o Global law. Se trata de un fenómeno jurídico que deriva directamente de la globalización y que ya nos ha permitido aprobar normas uniformes transnacionales, en múltiples órdenes jurídicos, especialmente en lo económico como los principios y convenciones del Institute for the Unification of Private Law (UNIDROIT) (Jiménez Alemán, 2016). García San José considera que la regulación internacional de la IA podría encontrar su origen en el principio de necesidad vinculado al principio de dignidad humana como principio general del Derecho Global ante los riesgos del avance de la IA (García San José, 2021).

Sin embargo, el propio autor se muestra pesimista sobre esta posibilidad. Por un lado, considera que por la novedad y la complejidad de la materia resulta complicado llegar a un acuerdo entre un amplio número de Estados. Por otro, la regulación de la IA ya ha comenzado y pese a que se encuentre en un estado embrionarío, la fragmentación normativa es ya atisbable. Ejemplo de ello, como veremos a continuación, destaca la visión mostrada por la UE en el Libro Blanco en el que entre otros se aboga por una actualización de la legislación ya existente (fragmentada) pero no por una unificación normativa.

5.2 Inteligencia artificial en la unión Europea

La mayor contribución a la mencionada industrialización 4.0 la está produciendo la automatización de procesos por medio del uso de la Inteligencia Artificial.

El Parlamento Europeo define la Inteligencia Artificial como la habilidad de las máquinas de replicar capacidades humanas tales como el razonamiento, el aprendizaje, la creatividad y la estrategia (Parlamento Europeo, 2020).

Podemos encontrar Inteligencia Artificial tanto en software como integrada en hardware (vehículos autónomos, drones o robots, *Internet of Things).*

En el Libro Blanco sobre la Inteligencia Artificial[29], la Comisión vuelve a asentar las bases sobre las que desarrollar una estrategia que coloque a Europa como líder mundial en la innovación en la economía de los datos y sus aplicaciones. La Inteligencia Artificial es una de esas aplicaciones, por lo que, una vez más, la Comisión considera necesario que la inteligencia artificial genere una confianza en los ciudadanos y para ello deberá asentarse en sus valores y derechos fundamentales.

El Libro Blanco pone sobre la mesa una serie de alternativas políticas que faciliten dicho desarrollo. En realidad, viene a recoger pautas e ideas similares a las que ya recogían tanto la estrategia de Datos como la estrategia para el Mercado Digital Único Europeo, así como en anteriores resoluciones como la resolución del Parlamento Europeo del 16 de febrero de 2017 con recomendaciones destinadas a la Comisión con normas de Derecho Civil sobre robótica.

Entre otros:

1. Aprovechar la fuerza del propio mercado industrial y profesional interno de la UE que el propio documento considera infrautilizado

2. Aprovechar las próximas oleadas de datos que permita desarrollar de manera interna su propia tecnología como procesadores de bajo consumo o algoritmos sofisticados.

[29] Libro Blanco de la Comisión Europea sobre la inteligencia artificial, "un enfoque europeo orientado a la excelencia y la confianza, COM (2020) 65 final.

3. Necesidad de financiación público privada.

En consonancia con el presente estudio, nos detendremos a analizar el capítulo relativo a plantear el posible marco regulador de la Inteligencia Artificial.

5.2.1 Un marco regulador de la IA en la UE

La UE ha demostrado ser consciente de las dificultades que plantea la IA y viene publicando consecuentemente diferentes documentos que pretenden configurar su postura con respecto a esta tecnología.

Ejemplo de ello son la publicación de, entre otros, la estrategia sobre Inteligencia artificial[30], la aprobación de un plan coordinado con los Estados Miembros para la armonización de estrategias en relación a la IA así como la creación de un grupo de expertos sobre inteligencia artificial en marzo de 2019[31].

Más recientes son la aprobación por parte del Parlamento Europeo de una serie de informes e iniciativas legislativas entre los que destacan el informe[32] del eurodiputado alemán Axel Voss en relación a la Responsabilidad por los daños causados por la IA o la iniciativa legislativa[33] del eurodiputado español Iban García del Blanco que insta a la UE a diseñar un nuevo marco jurídico para la IA.

Lo cierto es que la IA plantea numerosas dificultades en relación a la defensa de los derechos fundamentales y libertades de los ciudadanos europeos.

---

[30] Comunicación De La Comisión Al Parlamento Europeo, Al Consejo Europeo, Al Consejo, Al Comité Económico Y Social Europeo Y Al Comité De Las Regiones: "Inteligencia Artificial para Europa", COM (2018) 237 final.

[31] Comisión Europea (2021). High-level expert group on artificial intelligence. Obtenido el 12/04/2021 de https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

[32] Voss, A (2020). Civil Civil Liability Regimen for Artificial Intelligence. Obtenido en 04/04/2021 en : https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2014(INL)

[33]García Blanco, I (2020) Informe sobre principios éticos aplicables a la inteligencia artificial, la robótica y otras tecnologías. Obtenido en 04/04/2021 en https://ibangarciadb.eu/informe-sobre-principios-eticos-aplicables-a-la-inteligencia-artificial-la-robotica-y-otras-tecnologias/report-ethical-ai_final_xm/

El propio Libro Blanco junto con el informe de sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica[34] (en adelante Informe IA) señala varias de ellas.

a) Autonomía

La autonomía es una de las funcionalidades principales de la IA que puede dar lugar a resultados no deseados producidos por la IA que podrían perjudicar a los usuarios.

En principio comportamiento de los productos que poseen una IA integrada puede determinarse previamente, mediante la evaluación del riesgo realizada por el fabricante antes de la comercialización si existen una serie de requisitos u mínimos legales que cumplimentar.

Pero por las propias características de la IA, pueden darse situaciones en las que dicha determinación previa puede resultar imposible como consecuencia de un aprendizaje autónomo de la IA posterior a la comercialización del propio producto.

En esas situaciones la evaluación del riesgo realizada antes de comercializar no puede seguir reflejando el uso, el funcionamiento o el comportamiento del producto. Esto puede exigir una nueva evaluación del producto que incorpora aprendizaje automático.

b) Opacidad

La opacidad es otra de las características más comunes dentro del entorno IA, sobre todo en aquellos casos en los que la IA es autónoma y por lo tanto capaz de evolucionar sin necesidad de supervisión u intervención humana.

Según García Blanco se produce lo que se conoce como efecto de “caja negra”, por el cual se desconoce el funcionamiento de los algoritmos internos de la IA y por tanto

[34] Informe De La Comisión Al Parlamento Europeo, Al Consejo Y Al Comité Económico Y Social Europeo: “informe de sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica”, COM (2020) 65 final.

imposibilita la rendición de cuentas o el conocimiento de la razón por la cual una IA puede tomar una decisión u otra (García Blanco, 2020). Esto aumenta consecuentemente la imprevisibilidad de la IA y por consiguiente afecta a la confianza tanto de usuarios como de inversores.

c) Cadenas de valor complejas

Resulta de gran relevancia también poder conocer los intervinientes en el proceso productivo de la IA, así como la determinación de su responsable en cada momento del ciclo productivo.

d) Dependencia de datos

La mayoría de los productos que integren Inteligencia Artificial requieren datos para su entrenamiento.

Sin embargo, tampoco se prevé lo que puede suceder en caso de que los datos que se emplean sean erróneos. También son mencionables problemas relativos a la privacidad y la transferencia de datos a las máquinas sin el consentimiento de los dueños de dichos datos.

Todas estas características de la IA podrán dar lugar a una serie de consecuencias que el propio Libro Blanco clasifica en dos grupos diferentes y que requieren, en mi opinión, de un nuevo marco regulatorio *ad hoc.*

1. Por un lado, considera que suponen riesgos para los derechos fundamentales, espacialmente la protección de datos personales, privacidad y la no discriminación.

   Puesto que la Inteligencia Artificial es capaz de realizar funciones que hasta ahora solo podía realizar los humanos seremos objeto de decisiones que adoptadas por maquinas que podrán afectar a la protección de nuestros derechos fundamentales (Consejo de Europa, 2017).

Por ejemplo, en relación a la analizada protección de datos, la regulación de la misma establecía como responsables al encargado o responsable del tratamiento de los datos pudiendo ser este una persona física o una jurídica. Ahora bien, qué podría suceder en el caso de que el tratamiento ilegal de los datos, por ejemplo, una monitorización no autorizada del comportamiento de un ciudadano europeo, suceda como fruto de la Inteligencia Artificial. Podrían adoptarse también decisiones administrativas basándose en discriminaciones raciales o de género que infrinjan las normas europeas.

2. Por otro, supone tremendas dificultades en relación a la responsabilidad civil puesto que los supuestos que mencionábamos en el anterior punto la legislación actual.

   No sería fácil determinar para la víctima quien es el responsable de una posible lesión no tampoco existe a día de hoy una normativa específica que regule las consecuencias de acciones lesivas de la IA.

5.2.2 Regulación europea actual en materia de responsabilidad civil y la IA.

La responsabilidad civil de los robots y sistemas integrados por la IA han sido objeto de estudio por la UE durante la última década. Como antesala de los citados documentos publicados durante el año pasado, la Resolución del Parlamento Europeo de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)) ya planteaba muchas de las cuestiones relativas a la responsabilidad civil de la IA.

Uno de los objetivos de dicha Resolución era la presentación de una propuesta de Directiva de regulación en materia de robótica. No obstante, de las últimas comunicaciones de la UE se desprenden objetivos diferentes, centrados en la actualización de la normativa nacional ya existente relativa a la responsabilidad civil.

Actualmente, la legislación europea no afronta directamente la regulación de la IA. Una de las pocas menciones a la inteligencia artificial la encontramos en el artículo 22 del RGPD. Este artículo, titulado *Decisiones individuales automatizadas, incluida la elaboración de perfiles* es la primera aproximación la regulación unificada de la inteligencia artificial.

Aplica a aquellos casos en los que una decisión que es adoptada por tratamiento automatizado de sus datos personales. Así, se reconoce el derecho de los afectados a no verse sometidos a una decisión que ha sido tomada por IA.

No obstante, el propio artículo establece unos límites. El derecho es ejercitable cuando el tratamiento de los datos ha sido realizado "únicamente" por la IA y, además, dicho tratamiento produce efectos jurídicos en el afectado. De hecho, ni el propio precepto es claro puesto que no se define que se considera por *intervención humana* ni tampoco lo que debemos entender por *efectos jurídicos* y es solo aplicable a situaciones en las que se produzca un tratamiento de datos personales. Es claramente insuficiente.

En cuanto a la legislación en materia responsabilidad civil, en la UE conviven por un lado Directiva 85/374/CE[35] de responsabilidad por los daños causados por productos defectuosos y por otro las normativas nacionales no armonizadas de responsabilidad civil.

La normativa de responsabilidad de daños causados por productos defectuosos proporciona una protección que algunos de los sistemas de responsabilidad civil nacional subjetivos no garantizan, previendo un sistema de responsabilidad civil objetiva del productor por los daños causados por los defectos de sus productos.

El Libro Blanco considera que la legislación en vigor en la UE en materia de seguridad de los productos y responsabilidad civil, completada con las legislaciones nacionales de

[35] Directiva (CE) nº 374/1985 del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos.

los estados miembros es amplia. Asimismo, considera que en principio la legislación resulta plenamente aplicable independientemente del uso de IA.

La UE deja entrever que habrá que ver si esta legislación resulta finalmente ineficaz para el campo de la IA. Es decir, parece en un primer momento que la UE es partidaria de una cierta adaptación de la legislación vigente a las necesidades de la IA. Esto directamente se aleja de la inicial propuesta de Directiva que se preveía en la Resolución del 16 de febrero de 2017.

Sin embargo, al mismo tiempo, la UE se muestra preocupada una vez más por la fragmentación normativa existente, añadiendo que las diferencias normativas nacionales pueden ser perjudiciales para el Mercado único en el caso en que cada país adapte de manera diferente su normativa en relación a la responsabilidad civil.

Estos pronunciamientos resultan, en mi opinión, del todo incoherentes. Partiendo de la base de que la normativa europea aplicable a conflictos surgidos de la IA está compuesta por Directivas y legislación nacional, intentar adaptar dicha normativa a las nuevas necesidades no hará más que aumentar la ya existente fragmentación normativa.

5.2.3 Dificultades que plantea la IA en materia de responsabilidad civil

El principal problema es que la normativa actual de productos defectuosos prevé una responsabilidad civil que se basa en el defecto. La autonomía de los productos con IA integrada puede alterar sustancialmente las funcionalidades iniciales de dicha IA durante su ciclo vital, cambiando sus características y funcionalidades iniciales. Como recoge el informe “Liability for Artificial Intelligence and other emerging technologies” de la Comisión Europea los productos con IA pueden perjudicar bienes jurídicos importantes como la vida, la salud, la propiedad privada o la privacidad (Comisión Europea, 2019). Pero esto puede suceder sin que el producto presente ningún tipo de defecto y que el perjuicio provenga de una decisión autónoma de la IA. Esto ya acarrea la necesidad de una nueva normativa de responsabilidad civil.

Pero, además, la IA suele estar integrada en entornos de internet de las cosas complejos, en los que interactúan muchos dispositivos y servicios conectados. La combinación de los distintos componentes puede dificultar evaluar dónde se puede producir un perjuicio y quién es el responsable, con especial énfasis en esto último. El derecho nacional actual exige encontrar la figura del responsable para que la víctima pueda reclamar.

El aludido efecto caja negra de algunas IA puede dificultar la obtención de una indemnización por los daños causados por aplicaciones de IA autónomas por la ausencia de la figura del responsable. Según el Informe IA, la víctima rara vez poseerá los conocimientos necesarios para conocer el funcionamiento del algoritmo que le ha producido el daño. Es más, sin la cooperación del responsable probablemente sea imposible acceder al algoritmo y los datos.

En definitiva, la normativa actual en materia de seguridad de los productos presenta carencias que deben cubrirse, en especial la Directiva sobre seguridad general de los productos, la Directiva sobre máquinas, la Directiva sobre equipos radioeléctricos.

Pero la UE solo se plantea esta adaptación, y no la aprobación de un nuevo reglamento que regule la inteligencia artificial o la protección de los derechos de los ciudadanos en relación a los sistemas de inteligencia artificial.

5.3 Propuesta de *Lege Ferenda*.

Como hemos visto, la necesidad de una regulación en materia de IA es necesaria. Las carencias analizadas reflejan la necesidad de por un lado proteger una serie de derechos y por otro actualizar el régimen de responsabilidad civil. En mi opinión, existen claros paralelismos entre la situación normativa actual de la IA y la situación que existía antes de la aprobación del RGPD. Así, considero más oportuna la creación de una nueva norma en contraposición a la propuesta de actualización de las normativas nacionales.

Por ello a continuación presentaré las principales líneas que considero debiera seguir una futura regulación de la Inteligencia Artificial en Europa.

a) Forma

En primer lugar, parece que en cuanto a la forma que adoptará la futura norma que regule las cuestiones relativas a la IA será una Directiva. En mi opinión, esto no es coherente con la Estrategias de datos y de Mercado Único Digital que hemos analizado previamente.

Uno de los pilares en todas estas comunicaciones de la Comisión es intentar acabar con la fragmentación normativa existente entre los Estados Miembros.

Una norma de armonización como una Directiva en mi opinión no sería suficiente para tales propósitos por varias razones. Por un lado, la materia que se pretende regular es una materia tan cambiante que probablemente necesite de futuras revisiones de su marco regulador.

Si se opta por la vía de la Directiva esto supondría tener que actualizar primero la misma para después adaptar a la misma las 27 legislaciones nacionales. En relación con ello, se trataría de un proceso lento que podría dar lugar a que la normativa quede obsoleta casi desde el momento de su entrada en vigor por la naturaleza de su objeto. Además, si como venimos destacando la UE pretende que se protejan los derechos de sus ciudadanos frente a posibles injerencias extracomunitarias no parece tampoco la opción más efectiva.

Siendo factible que la Directiva suponga la antesala de un posterior Reglamento como ya sucediera en anteriores ocasiones, nos encontramos ante una nueva oportunidad de ser referentes mundiales respecto a la regulación de esta tecnología y hacerlo desde un estadio aún más temprano que el momento en el que el Reglamento de Protección de Datos fue aprobado supone una oportunidad interesante. Dicho lo cual, considero la vía del Reglamento la más adecuada para los fines que la UE pretende alcanzar, siendo consciente de las complicaciones que ello conlleva.

b) Contenido

Como ya hemos mencionado y recoge el Libro Blanco, los focos de una regulación de la IA debieran ser dos. Por un lado, la estipulación de una serie de principios generales y

reconocimiento de derechos a los ciudadanos de la UE y, por otro, un régimen de responsabilidad adaptado a las necesidades de la IA, así como la previsión de un régimen sancionador.

En cuanto a los derechos y libertades fundamentales que deberá recoger la norma habrá de analizarse cómo la IA puede afectar a los derechos que los ciudadanos de la UE ya han adquirido y por otro plantear si es necesario el reconocimiento de nuevos derechos como señalaba Núñez Zorrilla (Núñez Zorrilla, 2019).

En cuanto a la responsabilidad civil considero indispensable la determinación de los responsables de las consecuencias derivadas de un uso de la IA. En la eficacia del RGPD resulto determinante la creación de las figuras del encargado y del responsable del tratamiento. A través de estas figuras, junto con las estipulaciones relativas al ámbito territorial de aplicación de la norma, se resolvía tanto el problema de encontrar un responsable de los daños producidos como el problema de la aplicación de las disposiciones del RGPD a agentes extracomunitarios.

La Resolución de 16 de febrero de 2017, que apostaba por la creación de una nueva norma europea, consideraba que, en cualquier caso, la responsabilidad debería recaer siempre en un humano puesto que la IA está lejos todavía de poder adoptar una personalidad jurídica particular que por ende permita una atribución de la responsabilidad. Esto evidencia también que el sistema de responsabilidad que deberá recoger la nueva norma habrá de ser un sistema de responsabilidad objetivo, que transfiera la responsabilidad de actos realizados por una máquina a determinadas personas, para abarcar la totalidad de casos en los que pueda producirse una lesión de derechos.

Así, de la misma forma que el RGPD fue capaz de confeccionar dos figuras como el encargado y el responsable del tratamiento de los datos, la nueva norma deberá considerar quiénes de los agentes participantes en la vida útil de la tecnología con IA integrada serán los responsables en este caso. Para ello deberán considerarse, entre otros, los programadores del software que integre el producto, el propio productor, el propio usuario de la tecnología, la administración, el empresario que adquiere la tecnología para

integrarla en los procesos de su actividad económica o posibles supervisores o controladores del funcionamiento de la misma.

6. CONCLUSIONES

- La situación geopolítica europea es mejorable desde el punto de vista de la inversión público-privada y el estado de desarrollo de la tecnología, de la digitalización o de la inteligencia artificial. En 2019 el Parlamento Europeo anuncio una inversión de 9.200 millones de euros para la próxima década (Parlamento Europeo, 2019). No obstante, esta inversión sigue estando por detrás de la inversión que se realiza tanto en EEUU como en China (Universidad de Stanford, 2021).

  Esta situación deja a Europa en una posición de clara desventaja frente a las dos potencias mencionadas, por lo que su aspiración resultar ser un cliente interesante para alguno de ellos o para ambos. Considero que a día de hoy es irreal pensar que la UE podrá competir con estas dos potencias en el corto plazo. No por ello sin embargo deberá de dejar de invertirse en la digitalización del continente puesto que, bajo mi punto de vista, no hace falta ser el mejor para ser considerado un agente geopolítico relevante.

  Las estrategias analizadas muestran un compromiso por parte de las instituciones europeas para con la digitalización y modernización de la industria europea a largo plazo. Si bien no encuentro factible una competencia directa con los bloques EEUU-China, a corto-medio plazo considero que la UE tiene la oportunidad de convertirse en una potencia tecnológica mundial durante este siglo. No obstante, considero que la UE debería ser más pragmática en sus iniciativas puesto que como pudimos ver en el caso de la Estrategia para el Mercado Único Digital, muchas de las propuestas se quedan sin llevar a cabo y años después la estrategia requiere de actualizaciones.

- La UE es pionera en legislación relativa a nuevas tecnologías. Las normas que han sido mencionadas en el presente estudio reflejan un claro interés por parte de la UE en la defensa de los derechos de sus ciudadanos y, en concreto, puede entenderse que el RGPD ha sido un éxito.

  En mi opinión, por un lado, la UE y sus órganos judiciales han sabido establecer un ámbito de aplicación de la norma amplio y determinado a través de la norma y su posterior interpretación jurisprudencial

  Por otro, encuentro las sanciones previstas el régimen sancionador recogidas en el RGPD son proporcionales a las vulneraciones de derechos fundamentales de los ciudadanos europeos que se producen. Bajo mi punto de vista, los Estados Miembros no deben mostrarse tolerantes ante este tipo de vulneraciones y deben aumentarse los controles y condiciones a las que se deben someter las empresas tecnológicas, en especial las grandes multinacionales.

- En lo referente a la Inteligencia Artificial, considero que la UE no tiene todavía del todo claro cómo enfocar su regulación. Es cierto que se trata de una tecnología puntera que todavía no está plenamente integrada en la sociedad y que por tanto no ha dado lugar aún a que se produzcan vulneraciones graves de derechos. No obstante, creo que la UE tiene la oportunidad de regular una tecnología tan interesante como la IA para su propio beneficio tanto desde el punto de vista de la defensa de derechos como desde el punto de vista de regular la competencia en este ámbito.

  Una regulación temprana de la IA supondría otro motivo más para considerar la normativa europea referente mundial en regulación tecnológica, así como para seguir considerando a la UE un agente principal en la partida geopolítica.

  A mi parecer, los pronunciamientos sobre la IA que se han analizado en este trabajo, además de incoherentes, muestra un enfoque conservador. Una norma sólida permitiría resolver muchos de los problemas que la propia UE se plantea

en sus pronunciamientos (fragmentación normativa, confianza, atracción de inversión, defensa de derechos fundamentales, control sobre el devenir de la IA, etc.)

Por todo ello, considero que las instituciones europeas deberían mostrar una postura proactiva en relación a la regulación de la IA y de las tecnologías venideras.

ANEXO I

La Estrategia de Datos contiene las siguientes medidas clave para cada uno de los cuatro pilares:

Un marco de gobernanza intersectorial para el acceso y utilización de los datos. Superar la fragmentación del mercado interior.

Medidas clave

- Proponer un marco legislativo para la gobernanza de los espacios de datos europeos comunes en el cuarto trimestre de 2020.
- Adoptar una norma de ejecución sobre conjuntos de datos de gran valor en el primer trimestre de 2021.
- Proponer, en su caso, una norma relativa a los datos en 2021.
- Analizar la importancia de los datos en la economía digital (por ejemplo, a través del Observatorio de la Economía de las Plataformas en Línea), y revisar el marco político existente en el contexto del paquete de la norma sobre servicios digitales (cuarto trimestre de 2020).

Inversión en datos y refuerzo de la infraestructura para almacenar, tratar y utilizar los datos, interoperabilidad.

Medidas clave

- Invertir en **un proyecto de gran impacto sobre los espacios de datos europeos** que abarque las arquitecturas de intercambio de datos (incluidas las normas de intercambio de datos, mejores prácticas, herramientas) y mecanismos de gobernanza, así como la federación europea de infraestructuras en la nube eficientes desde el punto de vista energético y fiables, y sus servicios conexos, con vistas a facilitar inversiones combinadas de entre 4 000 y 6 000 millones EUR, de los cuales la Comisión podría aspirar a invertir 2 000 millones EUR. Primera fase de ejecución prevista para 2022.
- Firmar los memorandos de entendimiento con los Estados miembros sobre la federación en la nube en el tercer trimestre de 2020.

- Crear un mercado europeo de servicios en la nube que integre la totalidad de la oferta de servicios en la nube en el cuarto trimestre de 2022.
- Elaborar un manual de normas de la UE para la (auto)regulación de la computación en la nube en el segundo trimestre 2022.

Empoderar a las personas, invertir en cualificaciones y en pymes.

Medida clave

- Explorar el refuerzo del derecho a la portabilidad por parte de las personas de conformidad con el artículo 20 del Reglamento General de Protección de Datos, dándoles un mayor control sobre quién puede acceder a los datos generados por las máquinas y utilizarlos (posiblemente como parte de la norma relativa a los datos de 2021).

Espacios comunes europeos de datos en sectores estratégicos y en ámbitos de interés público.

La Comisión se compromete a apoyar la creación de los siguientes espacios comunes europeos de datos:

a. Espacio común europeo relativo a la industria.

b. Espacio común europeo de datos relativos al Pacto Verde Europeo.

c. Espacio común europeo de datos relativos a la movilidad.

d. Espacio común europeo de datos relativos a la salud.

e. Espacio común europeo de datos en materia financiera.

f. Espacio común europeo de datos relativos a la energía.

g. Espacio común europeo de datos relativos al sector agrario.

h. Espacio común europeo de datos relativos a las administraciones públicas.

BIBLIOGRAFÍA

LEGISLACIÓN Y OTROS DOCUMENTOS OFICIALES

a) Legislación

- Directiva (UE) nº 13/2010 del Parlamento Europeo y del Consejo de 10 de marzo de 2010 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual).

- Directiva (UE) nº 1808/2018 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), habida cuenta de la evolución de las realidades del mercado.

- Directiva (UE) nº 1148/2016 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

- Directiva (CE) nº 46/1995 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Directiva (CE) nº 374/1985 del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos.

- Reglamento (UE) nº 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.

- Reglamento (UE) nº 679/2016 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

b) Otros documentos oficiales

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, “EUROPA 2020. Una estrategia para un crecimiento inteligente, sostenible e integrador”, COM (2010) 2020 final.

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Una Agenda Digital para Europa", COM (2010) 0245 final.

- Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, "Una Estrategia para el Mercado único Digital de Europa", COM (2015) 192 final.

- Comunicación De La Comisión Al Parlamento Europeo, Al Consejo Europeo, Al Consejo, Al Comité Económico Y Social Europeo Y Al Comité De Las Regiones: "Inteligencia Artificial para Europa", COM (2018) 237 final.

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "Una Estrategia Europea de Datos", COM (2020) 66 final.

- Dictamen 8/2010 del 16 de diciembre de 2010, sobre el Derecho aplicable emitido por el Grupo de Protección de Datos del artículo 29 de la Directiva 95/46/CE.

- Informe de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social europeo "Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica", COM (2020), 65 final.

- Libro Blanco de la Comisión Europea sobre la inteligencia artificial, "un enfoque europeo orientado a la excelencia y la confianza, COM (2020) 65 final.

JURISPRUDENCIA

- Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Gran Sala) de 7 de diciembre de 2010, C-585/08 y C-144/09. Peter Pammer contra Reederei Karl Schlüter GmbH & Co. KG y Hotel Alpenhof GesmbH contra Oliver Heller.

- Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Gran Sala) de 25 de octubre de 2011, C-509/09. eDate Advertising GmbH y otros contra X y Société MGN LIMITED.

- Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Sala Cuarta) de 6 de septiembre de 2012, C-218/12. Daniela Mühlleitner contra Ahmad Yusufi y Wadat Yusufi.

- Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Sala Tercera) de 17 de octubre de 2013, C-218/12. Lokman Emrek contra Vlado Sabranovic.

- Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Gran Sala) de 20 de junio de 2014, C-131/12. Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González.

- Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Sala Tercera) de 1 de octubre de 2015, C-230/14. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság.

- Tribunal de Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Sala Quinta) de 17 de marzo de 2017, C-99/15. Christian Liffers contra Producciones Mandarina, S.L., y Mediaset España Comunicación, S.A., anteriormente Gestevisión Telecinco, S.A.

OBRAS DOCTRINALES

- Asimov, I. (1989). Círculo vicioso. Los robots. trad. Domingo Santos. Barcelona: Ediciones Martínez Roca.

- Biurrun Abad, F. (2017). Accountability o responsabilidad activa en el Reglamento General de Protección de Datos. LEGALTODAY. Obtenida el 01/04/2021 de http://www.legaltoday.com/gestion-del-despacho/nuevas tecnologias/articulos/accountability-o-responsabilidad-activa-en-el-reglamento-generalde-proteccion-de-datos

- De Miguel Asensio, P. A. (2015.I) Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia. La Ley Unión Europea, 31, 1-10.

- De Miguel Asensio, P.A. (2015.II). "Estudios y Comentarios Legislativos (Civitas). Derecho Privado de Internet" Madrid: Editorial Aranzadi.

- De Miguel Asensio, P. A. (2017). Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la UE. *Revista Española de Derecho Internacional*, *69* (1), 75-108.

- García Blanco, I (2020) Informe sobre principios éticos aplicables a la inteligencia artificial, la robótica y otras tecnologías. Obtenido el 04/04/2021 de: https://ibangarciadb.eu/informe-sobre-principios-eticos-aplicables-a-la-inteligencia-artificial-la-robotica-y-otras-tecnologias/report-ethical-ai_final_xm/

- 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.

- Giddens, A (2020). Preámbulo. En C. Hobbs y J.I. Torreblanca (eds.), *La soberanía digital de Europa (*pp. 12–16). Madrid: Catarata.

- Gonzalo Doménech, J. J. (2018.I). Algunas cuestiones relevantes de derecho internacional privado del reglamento general de protección de datos. Revista Boliviana de Derecho, 26 , 404-437.

- Gonzalo Doménech, J. J. (2018.II). Big Data, Protección de datos y Derecho Internacional Privado. (p 70).

- Hobbs, C., & Torreblanca, I. (2020). La soberanía digital de Europa. Madrid: Catarata.

- Jiménez Alemán, A. (2016). Derecho Global. Revista de la cultura de la legalidad, 11, 5. Obtenida el 05/04/2021 de: https://e-revistas.uc3m.es/index.php/EUNOM/article/view/3290/1951

- Minsky, M., & Papert, S. A. (1972). Artificial intelligence progress report.

- Muñoz Ontier, J. (2018). Disposiciones Generales (Arts. 1-5) En López Calvo, J. (coord) El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid: Bosch, 335-351.

- Núñez, Zorrilla, M.C. (2019). Inteligencia artificial y responsabilidad civil. (p. 21) Madrid: Editorial Reus.

- Orejudo Prieto De Los Mozos, P. (2013) La vulneración de los derechos de la personalidad en la jurisprudencia del tribunal de justicia. La Ley Unión Europea, 4, 18-25.

- Ortega Giménez, A. (2013). Imagen y circulación internacional de datos. *Revista Boliviana de Derecho*, 15, 130-147.

- Ortega Klein, A. (2019). Geopolítica de la cuarta revolución industrial.. *Revista Economistas*. 21-24. Colegio De Economistas De Madrid. Obtenida el 03/02/2020 de https://www.cemad.es/wp-content/uploads/2019/10/Geopolitica-4RI.pdf

- Ortega Klein, A. (2020). La perspectiva desde España: la apuesta de la UE por la soberanía digital. En C. Hobbs y J.I. Torreblanca (eds.), *La soberanía digital de Europa* (65-90). Madrid: Catarata.

- Puddephatt, A. (2020). Regulando Internet: la creación de un modelo europeo. En C. Hobbs y J.I. Torreblanca (eds.), *La soberanía digital de Europa* Madrid: Catarata, 28-46.

- Rallo Lombarte, A. (2018) España en la vanguardia de la Protección de Datos: nuevos retos del Reglamento Europeo. En López Calvo, J. (coord) El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. (75-80). Madrid: Bosch.

- Schwab, K. (2016). La cuarta revolución industrial. Trad. Portafolio. Madrid: DEBATE.

- Voss, A (2020). Civil Civil Liability Regimen for Artificial Intelligence. Obtenido el 04/04/2021 de : https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/2014(INL)

RECURSOS DE INTERNET

- Comisión Europea (2021). High-level expert group on artificial intelligence. Obtenido el 12/04/2021 de https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

- Conferencia de La Haya de Derecho internacional privado. (2000). Les échanges de données informatisées, Internet et le commerce électronique. (p. 25.) Obtenido el 29/03/2021 de https://assets.hcch.net/upload/wop/gen_pd7f.pdf

- Consejo de la OCDE (2019). Principios de la OCDE sobre la Inteligencia Artificia. Obtenido el 08/04/2021 de https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

- European Justice. (2020). Atlas Judicial europeo en materia civil. Reglamento Bruselas I (refundición). Obtenido el 15/02/2021 de: https://e-justice.europa.eu/content_brussels_i_regulation_recast-350-es.do#:~:text=Reglamento%20Bruselas%20I%20(refundici%C3%B3n),-Informaci%C3%B3n%20sobre%20los&text=El%20Reglamento%20(UE)%20n%C2%BA%201215,dictadas%20en%20los%20Estados%20miembros.

- GDPR Enforcement Tracker. (2020). Fines Statistics. Obtenido el 03/03/2021 de: https://www.enforcementtracker.com/?insights

- Iberley. (2018) Aproximación al nuevo régimen sancionador del Reglamento General de protección de datos a partir del 25 de mayo. Obtenida el 26/03/2021 de: https://www.iberley.es/revista/nuevo-regimen-sancionador-reglamento-general-proteccion-datos-25-mayo-162

- Informe de la Comisión Europea (2019). Liability for Artificial Intelligence and other emerging technologies. Obtenido el 01/04/2021 de https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

- Informe del Consejo de Europa Council (2017). Algorithms and Human Rights. Obtenido el 10/03/2021 de https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

- KPMG. (2018). El cambiante paisaje de las tecnologías disruptivas. Obtenido el 25/03/2021 de https://assets.kpmg/content/dam/kpmg/cl/pdf/2018-06-kpmg-chile-advisory-disruptive-technology.pdf

- McKinsey Global Institute (2019). Digital India. Obtenido el 02/02/2021 de *https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/ digital-india-technology-to-transform-a-connected-nation-fullreport.ashx*

- Office Of Science And Technology Policy (2019). American Artificial Intelligence Initiative. Obtenida el 01/04/2021 de: https://www.nitrd.gov/nitrdgroups/images/c/c1/American-AI-Initiative-One-Year-Annual-Report.pdf

- Parlamento de Nueva Zelanda (2020). Carta de Algoritmos de Nueva Zelanda. Obtenida el 05/04/2021 de: https://data.govt.nz/manage-data/data-ethics/government-algorithm-transparency-and-accountability/algorithm-charter/#signatories

- Parlamento Europeo. (2019). La UE planea invertir 9.200 millones de euros en tecnologías digitales clave. Obtenido el 10/04/2021 de: https://www.europarl.europa.eu/news/es/headlines/economy/20190410STO36624/la-ue-planea-invertir-9-200-millones-de-euros-en-tecnologias-digitales-clave

- Parlamento Europeo (2020). ¿Qué es la Inteligencia Artificial. Obtenido el 10/03/2021 de: https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa

- Unión Internacional de Telecomunicaciones (2019). United Nations Activities on Artifcial Intelligence (AI). Obtenido el 01/04/2021 de https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2019-1-PDF-E.pdf

- Universidad de Stanford (2021). Artificial Intelligence Index Report 2021. Obtenido el 25/03/2021 de https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf