José Antonio Fernández Amor
(Director/Coordinador)

DIGITALIZACIÓN, EMPRESA Y DERECHO

Atelier
LIBROS JURÍDICOS

DIGITALIZACIÓN, EMPRESA Y DERECHO

DIGITALIZACIÓN, EMPRESA Y DERECHO

José Antonio Fernández Amor
Director/Coordinador

Autores
Sandra Camacho Clavijo
Josep Cañabate Pérez
José Antonio Fernández Amor
Zuley Fernández Caballero
Carolina Gala Durán
Miguel Gardeñes Santiago
Carles Górriz López
Jorge Miquel Rodríguez
Susana Navas Navarro
Miguel Ángel Sánchez Huete
Josep Suquet Capdevila

Atelier
LIBROS JURÍDICOS

El presente trabajo se encuadra en el proyecto "Reorientación de los instrumentos jurídicos para la transición empresarial hacia la economía del dato" financiado por el Ministerio de Ciencia e Innovación y la Agencia Estatal de Investigación, con referencia PID2020-113506R-100 REFERENCIA DEL PROYECTO/ AEI/10.13039/501100011033. IP: Dr. José Antonio Fernández Amor

Este libro ha sido sometido a un riguroso proceso de revisión por pares.

© 2024 Atelier
Santa Dorotea 8, 08004 Barcelona
e-mail: editorial@atelierlibros.es
www.atelierlibrosjuridicos.com
Tel. 93 295 45 60

I.S.B.N.: 978-84-10174-99-3

Depósito legal: B 18801-2024

Impresión: Podiprint

ÍNDICE

SEGUNDA PARTE
La empresa y sus relaciones con terceros

I. Empresa y responsabilidad

II. Empresa y actividad

III. Empresa y Administración tributaria

PRESENTACIÓN

José Antonio Fernández Amor

Una idea fácil de comprender es que una empresa implica organizar diferentes componentes como pueden ser personas, capital y bienes con la intención de intervenir en el mercado y obtener un beneficio. Cuando la estructura que se ordena comienza a operar, se forman relaciones en dos ámbitos: el interno y el externo. Ambos espacios son de interés para el Derecho, ya que en ellos surgen conflictos para los que el ordenamiento jurídico ha de funcionar como instrumento de organización.

Desde hace tiempo, las nuevas tecnologías y la digitalización influyen en la configuración de lo descrito y tienen un impacto en cómo el Derecho ha de ofrecer soluciones a los problemas emergentes. Este es el objeto de las presentes páginas, que reúnen diferentes trabajos en torno a los dos ámbitos citados. Por un lado, aquellos que tratan aspectos *ad intra* de la empresa como son las relaciones con su personal, su organización o su ubicación. Por otro lado, aquellos que tratan aspectos *ad extra* como son su responsabilidad con terceros, su actividad empresarial o sus relaciones con la Administración en el ámbito tributario.

Esta obra comienza, dentro del primer ámbito, tratando cómo en los últimos años el desarrollo del teletrabajo ha planteado bastantes retos a las empresas y a los trabajadores, aprobándose finalmente una regulación específica a nivel estatal, tanto en el sector público como en el privado. En su trabajo GALA DURÁN analiza esa regulación desde una perspectiva concreta: la prevención de riesgos laborales. De ese análisis deriva la insuficiencia de la normativa española a la hora de hacer frente a los riesgos concretos que proceden del hecho de trasladar el trabajo de la empresa al ámbito familiar/personal. Está claro que dicha normativa está pensada para el trabajo presencial, por lo que resulta necesario y urgente su adaptación al teletrabajo, con el objetivo de evitar posibles responsabilidades empresariales.

Por lo que hace a la digitalización de las sociedades, se comenta la Directiva 2019/1151, conocida, precisamente, como «Directiva de digitalización de sociedades» que fue incorporada a nuestro ordenamiento por la Ley 11/2023, en lo que supone un avance importante en la constitución en línea de sociedades de

responsabilidad limitada que, salvo excepción debidamente justificada, se podrán constituir sin necesidad de comparecer físicamente en la notaría. Según MIQUEL RODRIGUEZ este procedimiento es posible solamente si las aportaciones son dinerarias, manteniéndose los trámites por vía telemática durante toda la vida de la sociedad y aplicándose también a las sucursales. Así mismo, el autor aprovecha la oportunidad para examinar la Propuesta de reforma de la Directiva en su versión de 2024.

La ubicación territorial de la empresa también tiene un espacio en esta obra. El llamado "principio del Estado de origen" regulado en el artículo 3 de la Directiva de comercio electrónico, adoptada en el año 2000, ha demostrado ser una poderosa herramienta de integración del mercado de servicios de la sociedad de la información en la UE. GARDEÑES SANTIAGO argumenta que, a pesar de ello, por su carácter poliédrico o polivalente, ha dado lugar a problemas de interpretación y aplicación. En su aportación pretende explicar las causas de dichos problemas y proponer soluciones interpretativas que permitan superarlos. Al mismo tiempo, analiza hasta qué punto, y bajo qué modalidades, dicho principio desempeñaría un papel en dos textos posteriores de singular importancia para el mercado único digital: el Reglamento general de protección de datos de carácter personal y el Reglamento de servicios digitales.

Esta aportación se acompaña con reflexiones sobre la competencia judicial en el caso de plataformas digitales. SUQUET CAPDEVILA analiza una serie de cuestiones relativas a las plataformas de intercambio de vídeos (PIV). Así, partiendo del concepto de PIV de la Directiva 2018/1808 y de la Ley 13/2022, de 7 de julio, general de comunicación audiovisual, muestra algunos de los conflictos existentes que la jurisprudencia nacional está resolviendo actualmente, tanto relacionados con contenido que las personas influenciadoras suben a estas plataformas, así como relacionados con las infracciones de contratos publicitarios y de derechos de autor. Desde el prisma del Derecho internacional privado y en el marco del Reglamento 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, sus líneas analizan las especificidades de las PIV en relación con la interpretación del foro de sumisión, del foro contractual de prestación de servicios y del foro de consumo.

La segunda parte de la obra, dedicada a problemas en el ámbito externo de la empresa, comienza con la aportación de CAÑABATE PÉREZ cuyo objetivo principal es analizar el polémico régimen jurídico de las transferencias de datos personales de terceros que pueden hacer empresas europeas a los Estados Unidos. A través de la metodología del derecho comparado estudia el concepto de privacidad estadounidense para determinar las causas que conducen a la UE a considerar que no cuenta con un nivel adecuado de protección. Por otra parte, se centra en el *EU-US Data Privacy Framework,* instrumento cuya función es garantizar el tratamiento de los datos personales de los europeos por parte de las organizaciones americanas que se adhieran, al cual precede una serie de acuerdos anulados por la justicia de la UE.

La responsabilidad de las empresas con los consumidores tiene un peso propio cuando se vincula con las que intervienen en el sector de la salud. La implementación de la telemedicina y de los sistemas de Inteligencia artificial constituyen una vía o solución para liberar un sistema sanitario presionado por las consecuencias asistenciales del envejecimiento de la población. En su aportación CAMACHO CLAVIJO analiza cuál es el grado actual de implementación de la IA en el proceso clínico y las cuestiones de responsabilidad civil que plantea la utilización de estos sistemas como herramientas de apoyo de las decisiones médicas tanto diagnósticas como terapéuticas. Principalmente se ocupa de estudiar la responsabilidad médico-hospitalaria por los daños producidos en el paciente por los errores del sistema de Inteligencia Artificial y el encaje de esta responsabilidad en el marco de nuestro ordenamiento jurídico, pero también en el nuevo marco europeo de responsabilidad compuesto por el Reglamento de Inteligencia Artificial y por la propuesta de Directiva de responsabilidad en esa materia.

El Reglamento europeo sobre Inteligencia Artificial se ha incorporado al régimen jurídico de la responsabilidad de la empresa para con terceros y tiene su espacio en esta obra. En este sentido, con su aportación NAVAS NAVARRO aborda, en primer lugar, la distinción entre sistemas de inteligencia artificial (IA) y modelos de IA de propósito general, un ejemplo de los cuales es la IA generativa. Seguidamente, procede a exponer la regulación de estos modelos en función de que presenten o no un riesgo sistémico. Finalmente, aborda aspectos relativos a la responsabilidad civil por los daños que pudieran ocasionar estos modelos de IA de propósito general en relación con las Propuestas de Directivas en la materia que se publicaron el 28 de septiembre de 2022. A este respecto manifiesta sus dudas acerca de la aplicación de esta regulación a los modelos de IA.

La oportunidad de negocio que implica la digitalización ha dado lugar a la creación de un mercado en el que actúan las empresas y para el que se está desarrollando un marco normativo. La Unión Europea se ha caracterizado por hacer frente a las grandes empresas y luchar contra sus abusos utilizando, entre otros instrumentos, el artículo 102 del TFUE. Sin embargo, GÓRRIZ LÓPEZ considera que esta norma se ha mostrado insuficiente para hace frente a los gigantes tecnológicos, razón de la aprobación del Reglamento de Mercados Digitales. Compara estas dos normas a efectos de determinar cuáles son los puntos fuertes y débiles de la última. Entre los primeros destaca su carácter expeditivo debido a la opción por un control preventivo y la brevedad de los plazos. Respecto de los últimos, no amplia los poderes de la Comisión para controlar las concentraciones en el sector digital y carece de previsiones sobre su aplicación privada.

Entre las cuestiones que la digitalización aporta a la empresa está la de incorporarla a sus procesos lo que implica innovación o mejoras que las Administraciones públicas pueden fomentar. Desde un punto de vista fiscal, se ha de plantear en qué términos estos procesos cuentan con un apoyo claro. Las ayudas públicas para dar impulso a las actividades de investigación, desarrollo e innovación tecnológica (I+D+i) se articulan a través de instrumentos fiscales y parafiscales. FERNÁNDEZ CABALLERO muestra que España tiene implementadas desde

hace varios años diferentes medidas tributarias que benefician la realización de ese tipo actividades. En su estudio analiza los actuales incentivos fiscales por la realización de actividades de investigación, desarrollo e innovación tecnológica y la eficacia de éstos para promover que las personas físicas lleven a cabo dichas actividades.

Pero la relación de la empresa con las Administraciones públicas tiene otras facetas. Entre las aportaciones a esta obra se encuentra el análisis de los perfiles de riesgo empleados por la Administración tributaria en donde la IA parece estar muy presente. SÁNCHEZ HUETE aborda unos interrogantes que parten de delimitar qué es un perfil de riesgo tributario y cuáles son sus funciones y principales efectos jurídicos. Acotar la idea de perfil y su operatividad precisa diferenciar los dos momentos que lo integran: su creación y la decisión que sobre el mismo se toma. La creación de un perfil de riesgo supone definir el modelo de prevención del riesgo de que se parte, e indicar a quien corresponde efectuarlo. La decisión administrativa que se toma sobre el perfil ha de respetar concretas garantías jurídicas, y aquí los interrogantes básicos es dónde se regulan y en qué consisten. La normal intervención de la IA en ambos procesos exige que las garantías y cautelas sean acordes a la singularidad que tales tecnologías integran, y aquí las ausencias de regulación son notorias.

Finalmente, la tecnología ha permitido a las empresas que pasen de ver los datos como fundamentos del conocimiento a tener conjuntos estructurados y singulares de esos elementos que se pueden utilizar como bienes en el tráfico económico. Desde ese momento son de interés para el Derecho tributario como objeto de gravamen, pues son manifestación de capacidad económica. Ahora bien, no es solo en el ámbito de la regulación de los gravámenes tributarios que han de acogerse, sino también en el campo de la ordenación de los procedimientos de aplicación de las exacciones tributarias. La última aportación a esta obra de la que soy responsable se aproxima a esos bienes muebles intangibles con esa perspectiva, abordándose aspectos como los requisitos para obtener información sobre el novedoso bien, su funcionamiento como garantía de la obligación tributaria, su valoración, la prueba sobre sus circunstancias o la extinción de la deuda tributaria con su entrega.

El grupo de personas que nos hemos reunido para esta obra constituimos el Grupo de Investigación DIGIDRET, dentro de la Facultad de Derecho de la Universidad Autónoma de Barcelona. Unidas por un interés común en el estudio de la interacción entre tecnología y derecho, nos dedicamos a desentrañar los complejos interrogantes que surgen. En las páginas que siguen, ofrecemos nuestras reflexiones, fruto de un complejo trabajo de análisis, reflexión y rigor.

PRIMERA PARTE

La empresa y su organización

I. Empresa y organización interna

ANÁLISIS DE LA PROBLEMÁTICA DEL TELETRABAJO DESDE LA PERSPECTIVA DE LA PREVENCIÓN DE RIESGOS LABORALES

Carolina Gala Durán
Catedrática de Derecho del Trabajo y de la Seguridad Social
Universidad Autónoma de Barcelona

ABSTRACT:
The development of teleworking in recent years has posed quite a few challenges to companies and workers, finally approving a specific regulation at the state level, both in the public and private sector. This paper analyses this regulation from a specific perspective: the prevention of occupational hazards. This analysis shows the inadequacy of Spanish regulations when it comes to dealing with the specific risks arising from the fact of transferring work from the company to the family/personal sphere. It is clear that these regulations are designed for face-to-face work, so it is necessary and urgent to adapt them to teleworking, in order to avoid possible business liabilities.

Keywords: telework, workers' rights, companies, occupational hazards

Palabras clave: teletrabajo, derechos de los trabajadores, empresas, riesgos laborales

SUMARIO:

1. INTRODUCCIÓN

La terrible crisis sanitaria provocada por la covid-19 trajo consigo numerosos cambios y reformas en el marco del Derecho del Trabajo y de la Seguridad Social (expedientes de regulación de empleo, prestaciones por desempleo extraordinarias, el ingreso mínimo vital, etc.), y, entre ellos, una mayor presencia de la figura del teletrabajo tanto en el sector privado como en el sector público; siendo aquel impuesto, incluso, con carácter preferente como una medida de contención sanitaria durante ciertos periodos de tiempo[1].

De hecho, la crisis de la covid-19 hizo que una nueva "forma de empleo", o, más bien, una nueva modalidad de organización del trabajo, que es lo que, más técnicamente, constituye el teletrabajo[2], pasase de tener muy poca presencia en España —un 4,3 por 100[3]—, a tener una cierta relevancia, llegando a afectar al 16,5 por 100 de los trabajadores por cuenta ajena, incluido el sector público. Y esta mayor importancia y aplicación también llevó a regular el teletrabajo en septiembre del año 2020, tanto en el sector privado como en las Administraciones Públicas.

A estos efectos, cabe recordar que, si bien en las Administraciones Públicas no se había regulado expresamente el teletrabajo con un alcance general hasta ese año, sí se había hecho con anterioridad en el sector privado, y, además, en dos fases: 1.ª fase) mediante la modificación del artículo 13 del Estatuto de los Trabajadores (dedicado al trabajo a domicilio), a través del Real Decreto-ley

1. Artículo 5 del Real Decreto-ley 8/2020, de 17 de marzo, de medidas urgentes extraordinarias para hacer frente al impacto económico y social del COVID-19.

2. Sobre el concepto y características del teletrabajo como modalidad de prestación de servicios: De las Heras García, A. (2016), *El teletrabajo en España: un análisis crítico de normas y prácticas*. CEF; García Calvente, Y (2020), Avances y desafíos del teletrabajo en la regulación del teletrabajo: reflexiones del ingreso y el gasto público en un contexto de pandemia, *Nueva Fiscalidad*, n.º 3, 53-80; Lousada Arochena, J.F., y Ron Latas, R.P. (2015), Una mirada periférica al teletrabajo, el trabajo a domicilio y el trabajo a distancia en el derecho español", en Mella Méndez, L. (ed.), *Trabajo a Distancia y Teletrabajo* (pp. 31-45). Thomson Reuters Aranzadi; Mella Méndez, L. (2015), Configuración general del trabajo a distancia en el derecho español, en Mella Méndez, L. (Dir.), *El teletrabajo en España: aspectos teórico-prácticos de interés* (pp. 19-82). Wolters Kluwer; Sierra Benítez, E.M. (2011), *El contenido de la relación laboral en el teletrabajo*. CES Andalucía; y Thibault Aranda, J. (2010), *El teletrabajo*, CES.

3. Eurostat 2018, frente al 14% de Holanda, el 13,3% de Finlandia o el 11% de Luxemburgo.

3/2012[4], que incorporó una regulación —escasa, eso sí— del trabajo a distancia, y dentro de este, del teletrabajo; y, 2.ª fase) el Real Decreto-ley 6/2019[5] incluyó en el artículo 34.8 del Estatuto de los Trabajadores[6] el trabajo a distancia como una de las medidas a las que puede recurrir un trabajador que quiere conciliar su vida familiar y laboral. A lo que cabe añadir la regulación del teletrabajo contenida en la negociación colectiva (no demasiado interesada, hasta ese momento, por esta cuestión, ya que, por ejemplo, de todos los convenios colectivos publicados en el Boletín Oficial del Estado entre el 1 de enero de 2017 y el 30 de julio de 2020, solo 81 convenios regulaban el teletrabajo).

Pues bien, esa nueva regulación del teletrabajo se recogió, para el sector privado en el Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia (cuya disposición adicional 2.ª excluía de su ámbito de aplicación al personal laboral de las Administraciones Públicas), y para las Administraciones Públicas en el Real Decreto-ley 29/2020, de 29 de septiembre, de medidas urgentes en materia de teletrabajo en las Administraciones Públicas y de recursos humanos en el Sistema Nacional de Salud para hacer frente a la crisis sanitaria ocasionada por la COVID-19 (aplicable tanto al personal funcionario como al personal laboral de todas las Administraciones Públicas). Cabe tener presente, también, que el Real Decreto-ley 28/2020 resultaba aplicable a las empresas públicas y a las fundaciones de carácter público.

Se trató de normas coincidentes en el tiempo y en el contexto, pero que presentaban, entre otras, tres diferencias sustanciales:

a) El Real Decreto-ley 28/2020 regulaba el trabajo a distancia, mientras que el Real Decreto-ley 29/2020 se centraba exclusivamente en el teletrabajo. Como sabemos, el teletrabajo es una modalidad específica del trabajo a distancia, caracterizada por un uso prevalente o exclusivo de los medios y sistemas informáticos, telemáticos y de telecomunicación[7].

b) El Real Decreto-ley 28/2020 era una norma amplia que recogía y regulaba los aspectos nucleares del trabajo a distancia —y del teletrabajo—, con una voluntad clara de servir como una reglamentación de referencia en esta materia, aun cuando remitía el desarrollo de ciertas cuestiones —importantes— a la negociación colectiva.

En cambio, el Real Decreto-ley 29/2020 tenía una finalidad muy distinta: incorporar el nuevo artículo 47 bis en el TREBEP, donde, a su vez, se recogían solo algunas líneas generales de carácter básico sobre cómo debía desarrollarse el teletrabajo en las Administraciones Públicas. En consecuencia, se dejaba conscientemente en manos de cada Administración Pública, previa negociación colectiva y respetando esas líneas básicas, el desarrollo de la correspondiente re-

4. De 10 de febrero, de medidas urgentes para la reforma del mercado laboral.

5. De 1 de marzo, de medidas urgentes para garantía de la igualdad de trato y oportunidades entre mujeres y hombres en el empleo y la ocupación.

6. Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE de 24 de octubre de 2015).

7. Artículo 2.c) del Real Decreto-ley 28/2020.

glamentación sobre el teletrabajo (tanto a nivel estatal, como autonómico y local)[8]. A nuestro entender, dada la importancia de la materia, quizás hubiera sido más adecuado que el propio TREBEP o bien una norma específica, hubiera recogido una regulación que sirviera de base o modelo para que luego la pudiesen adaptar las diversas Administraciones que quisieran desarrollar el teletrabajo en su ámbito.

En este marco, por su carácter pionero, cabe recordar que algunas Comunidades Autónomas ya habían desarrollado normativas propias sobre teletrabajo antes de la aprobación del Real Decreto-ley 29/2020; a estos efectos, cabe mencionar: la Instrucción de 6 de agosto de 2014, de la Comunidad Autónoma de Aragón; el Decreto 36/2013, de 28 de junio, de la Comunidad Autónoma de las Islas Baleares; el Decreto 92/2012, de 29 de mayo, de la Comunidad Autónoma de Euskadi; el Decreto 1/2018, de 10 de enero, de la Comunidad Autónoma de Extremadura; el Decreto 16/2018, de 7 de junio, de Castilla y León; el Decreto 82/2016, de 8 de julio, de la Comunidad Valenciana; el Decreto 45/2013, de 5 de diciembre, de la Comunidad Autónoma de La Rioja; el Decreto 57/2013, de 12 de agosto, de la Comunidad Autónoma de Castilla-La Mancha; la Orden de 20 de diciembre de 2013, de la Comunidad Autónoma de Galicia; y el Decreto 77/2020, de 4 de agosto, de Cataluña.

Y, c) aun cuando, en ambos Reales Decretos-leyes, se regulaba una materia común — el teletrabajo—, los ámbitos en los que se aplicaban eran muy diferentes desde la perspectiva de la gestión de los recursos humanos. No hay duda de que, en el sector privado, se dejaba un mayor margen y muchos menos condicionantes para la implantación y regulación del teletrabajo que en el marco de las Administraciones Públicas, donde las normas de Derecho Administrativo y la garantía del interés público, imponían algunos límites infranqueables (o al menos, eso parecía en ese momento).

Transcurridos casi cuatro años desde la aprobación de los Reales Decretos-leyes 28 y 29/2020, el panorama legal no ha cambiado en el marco de las Administraciones Públicas —no se ha modificado el contenido del artículo 47 bis del TREBEP—, si bien se han adoptado diversos acuerdos de teletrabajo partiendo de dicho precepto, tanto a nivel estatal, como autonómico y local. En cambio, sí que se ha producido un cambio legal —muy parcial eso sí— en el sector privado, por cuanto el Real Decreto-ley 28/2020, fue objeto de tramitación parlamentaria como proyecto de ley, siendo sustituido por la vigente Ley 10/2021, de 9 de julio, de trabajo a distancia.

A lo que cabe añadir otro dato interesante, el incremento del papel del teletrabajo que se produjo durante la pandemia ha disminuido ligeramente con posterioridad en el sector privado (según datos del INE, el 15% de los trabaja-

8. En el marco de las Administraciones Públicas, Mauri Majós J. (2020), La reglamentación del teletrabajo en las administraciones locales, *Seminario sobre Relaciones Colectivas*. FMC.

dores en 2022 teletrabajaba al menos un día[9]), aunque menos en el sector público. E, incluso, en empresas muy conocidas —por ejemplo, del sector tecnológico—, se ha reducido e incluso eliminado la posibilidad de recurrir al teletrabajo, volviendo al clásico modelo del trabajo presencial. Por tanto, nos encontramos ante una nueva forma de organización del trabajo que, aunque habiéndose desarrollado en un contexto excepcional, parece que "ha venido para quedarse", aunque con un papel claramente secundario respecto del trabajo presencial.

Pues bien, partiendo de este panorama legal, el objetivo de este trabajo es centrarse exclusivamente en uno de los aspectos que, a nuestro entender, plantea más interrogantes —a corto y medio plazo—, y que puede afectar de una manera más directa a los trabajadores en el marco del teletrabajo, como es la prevención de los riesgos laborales. Esto es, analizaremos cómo se regula actualmente la prevención de los riesgos laborales en el caso de los teletrabajadores.

Para ello tendremos en cuenta lo previsto normativamente, con carácter específico, tanto a nivel europeo como estatal y autonómico, así como en la negociación colectiva desarrollada en nuestro país. Y, a efectos de poder contrastar ambos sectores, nos fijaremos tanto en el sector público como en el sector privado, por cuanto, como es conocido, la normativa sobre prevención de riesgos laborales y, específicamente, la Ley de Prevención de Riesgos Laborales del año 1995 resulta aplicable, con algunos matices, en los dos ámbitos.

2. EL DERECHO A LA PREVENCIÓN DE LOS RIESGOS LABORALES EN LOS ACUERDOS Y NORMAS

2.1. El ámbito europeo: el contenido del Acuerdo Marco Europeo sobre Teletrabajo

Por razones evidentes de protección de la vida y la salud de los trabajadores, la prevención de los riesgos laborales constituye un elemento clave en el marco del trabajo a distancia y, particularmente, en el teletrabajo, como, por otra parte, deriva de lo establecido, con carácter general, en la Directiva Marco 89/391/CEE, del Consejo, de 12 de junio de 1989, relativa a la aplicación de medidas para promover la mejora de la seguridad y la salud de los trabajadores en el trabajo, y en las directivas particulares. Actualmente, no existe ningún reglamento o directiva que regule específicamente la prevención de los riesgos laborales en el marco del teletrabajo. Algo que, sin duda, resultaría muy útil.

Partiendo de ello y refiriéndose específicamente al teletrabajo, sí cabe mencionar el Acuerdo Marco Europeo sobre Teletrabajo de 16 de julio de 2002, fir-

9. Curull, M., Maynou, L. y Farré, L. (2024), *Teletrabajo después de la pandemia. Análisis desde la perspectiva del trabajador.* Fundación La Caixa.

mado por la Confederación Europea de Sindicatos y las organizaciones patronales de la Unión Europea UNICE, UEAPME y CEEP.

En el apartado 8 de este Acuerdo Marco se señala que el empleador es responsable de la protección de la seguridad y salud laborales del teletrabajador conforme a lo previsto en las directivas comunitarias. Con ello se reconoce expresamente la aplicación íntegra al teletrabajo de la normativa europea sobre seguridad y salud laboral y la responsabilidad empresarial correspondiente. Y partiendo de esa importante premisa, se añade que:

1) El empleador debe informar al teletrabajador de la política de la organización en materia de seguridad y salud en el trabajo, especialmente sobre las exigencias relativas a las pantallas de datos.

2) El teletrabajador está obligado a aplicar correctamente estas políticas de seguridad y salud laboral.

3) Para verificar la correcta aplicación de las normas en materia de seguridad y salud, el empleador, los representantes de los trabajadores y/o las autoridades competentes tienen acceso al puesto de teletrabajo, dentro de los límites de la legislación y de los convenios colectivos. Si el teletrabajador trabaja en su domicilio, el acceso está sometido a una previa notificación y a un consentimiento previo. Asimismo, el teletrabajador está autorizado para solicitar una visita de inspección.

4) Teniendo en cuenta que uno de los riesgos laborales del teletrabajo es precisamente el aislamiento, se prevé que el empleador se asegurará de que se toman medidas para prevenir el aislamiento del teletrabajador en relación con los otros empleados de la organización, como darle la ocasión de reencontrarse regularmente con sus compañeros de trabajo y tener acceso a las informaciones de la organización.

Y, 5) finalmente, se reconoce el derecho de los teletrabajadores a acceder a la misma formación que los trabajadores presenciales —incluida, por tanto, la formación en materia de prevención de riesgos laborales—. Añadiéndose que los teletrabajadores deben recibir una formación adecuada para utilizar el equipo técnico a su disposición y sobre las características de esta forma de organización del trabajo. El supervisor de los teletrabajadores y sus compañeros directos pueden también necesitar formación adecuada en relación con esta forma de trabajo y su gestión.

En definitiva, y como no puede ser de otra manera, según este Acuerdo Marco el empleador es el garante de la protección de la seguridad y salud laboral del teletrabajador y, en consecuencia, puede acceder su puesto de trabajo, si bien con los importantes límites derivados de la inviolabilidad del domicilio particular. Este Acuerdo Marco ha servido de guía para la adopción de normas estatales y también para la negociación colectiva.

2.2. La normativa estatal y autonómica: sector privado y Administraciones Públicas

En este ámbito cabe mencionar, en primer lugar, la Ley de Prevención de Riesgos Laborales, que no hace referencia al teletrabajo pero que, obviamente, se le aplica, tanto cuando aquel se desarrolla en el sector público como en el sector privado. Y también se aplica la numerosa normativa de desarrollo de la citada Ley.

En segundo lugar, en el marco del sector privado y como norma específica en esta materia, cabe citar lo dispuesto en varios apartados de la Ley 10/2021; así:

1) En el preámbulo de la Ley, a la hora de enumerar los inconvenientes del teletrabajo se mencionan elementos que claramente se identifican con riesgos psicosociales como son el tecnoestrés, el horario continuo, la fatiga informática, la conectividad digital permanente o el mayor aislamiento laboral. Y también se añade que uno de los propósitos de la Ley es regular los aspectos preventivos "relacionados básicamente con la fatiga física y mental, el uso de pantallas de visualización de datos y los riesgos de aislamiento…".

2) En relación con los teletrabajadores menores de edad, en el preámbulo de la Ley se establece que, teniendo en cuenta su vulnerabilidad, las necesidades de formación y descanso y la especial susceptibilidad a los riesgos vinculados con el teletrabajo (fatiga física y mental, aislamiento, problemas de seguridad y de acoso en el trabajo) es aconsejable establecer limitaciones, con el objetivo de garantizar un mínimo de tiempo de trabajo presencial en los acuerdos de teletrabajo. Esta necesidad deriva también de lo que se establece en los artículos 6.2 del Estatuto de los Trabajadores y 27 de la Ley de Prevención de Riesgos Laborales.

3) También en el preámbulo se recuerda que la igualdad de derechos entre los teletrabajadores y los trabajadores presenciales incluye, entre otros, el derecho a la prevención de riesgos laborales.

Y, 4) ya, más específicamente, la sección 4ª de Ley 10/2021 se denomina "Derecho a la prevención de riesgos laborales", e incorpora el siguiente contenido:

a) El articulo 15 —titulado "aplicación de la normativa preventiva"—, regula la prevención de riesgos laborales, señalando, en primer lugar, que los teletrabajadores tienen derecho a una adecuada protección en materia de seguridad y salud en el trabajo, de conformidad con lo establecido en la Ley de Prevención de Riesgos Laborales, y su normativa de desarrollo.

Y, b) con un mayor detalle, el artículo 16 entra en la evaluación de los riesgos laborales y en la planificación de la actividad preventiva, afirmándose que:

1) La evaluación de riesgos y la planificación de la actividad preventiva deben tener en cuenta los riesgos característicos del teletrabajo, poniendo especial atención en los factores psicosociales (aislamiento, tecnoestrés, fatiga…), ergonómicos y organizativos y de accesibilidad del entorno laboral efectivo.

En particular, debe tenerse en cuenta la distribución de la jornada, los tiempos de disponibilidad y la garantía de los descansos y desconexiones durante la jornada.

2) La evaluación de los riesgos únicamente debe alcanzar a la zona habilitada para la prestación de servicios, no extendiéndose al resto de las zonas de la vivienda o del lugar elegido para el desarrollo del teletrabajo. Con ello se pretende garantizar el derecho a la intimidad personal y familiar del teletrabajador, pero también cabe tener en cuenta que, algunas sentencias[10] están declarando como accidente de trabajo el acaecido fuera de esas zonas.

3) La empresa debe obtener toda la información acerca de los riesgos a los que está expuesto el teletrabajador mediante una metodología que ofrezca confianza respecto de sus resultados, y prever las medidas de protección que resulten más adecuadas en cada caso.

Cuando la obtención de dicha información exija la visita por parte de quien tuviera competencias en materia preventiva al lugar en el que, conforme a lo recogido en el acuerdo de teletrabajo, se desarrolla el teletrabajo, debe emitirse un informe escrito que justifique dicho extremo que se entregará al teletrabajador y a los delegados de prevención.

Y, 4) en cualquier caso, la visita requiere el permiso del teletrabajador, de tratarse de su domicilio o del de una tercera persona física. De no concederse ese permiso, el desarrollo de la actividad preventiva por parte de la empresa podrá efectuarse en base a la determinación de los riesgos que se derive de la información recabada del teletrabajador según las instrucciones del servicio de prevención.

Y, junto a lo anterior, lógicamente, es fundamental formar al teletrabajador adecuadamente sobre los riesgos laborales a los que se enfrenta, y actualizar dicha formación siempre que sea necesario.

Y, en tercer lugar, en el marco de las Administraciones Públicas la regulación es mucho más escasa. Así, el artículo 47 bis.3 del TREBEP se limita a señalar que el personal que presta sus servicios mediante teletrabajo tiene los mismos deberes y derechos, individuales y colectivos, recogidos en el TREBEP que el resto del personal que presta sus servicios en la modalidad presencial, incluyendo la normativa de prevención de riesgos laborales que resulte aplicable, excepto aquellos que sean inherentes a la realización de la prestación del servicio de manera presencial.

Sin embargo, la normativa autonómica ha tratado bastante, como veíamos antes, la figura del teletrabajo en las Administraciones Públicas, incidiendo, además, en la materia de prevención de riesgos laborales. De hecho, esa materia está presente en todas las normas autonómicas que regulan el teletrabajo; así:

1) En primer lugar, en el caso de la Comunidad Autónoma de Castilla y León, los artículos 2.5 y 20 del Decreto 16/2018, de 7 de junio, regulan la figura de "la

10. Entre otras, sentencia del Juzgado de lo Social nº 1 de Cáceres de 26 de octubre de 2022 (rec. 273/2022).

oficina a distancia", que se define como el lugar elegido por el solicitante de teletrabajo para desarrollar las jornadas no presenciales. Esta oficina debe disponer de los medios tecnológicos necesarios para realizar las funciones propias del puesto de trabajo y deben garantizarse las condiciones exigidas en materia de prevención de riesgos laborales, prestando especial atención a los aspectos relacionados con la seguridad y la ergonomía. Así mismo, la ubicación de esta oficina debe constar en el "documento de compromisos" que se celebra entre la Administración y el teletrabajador y cualquier cambio en esa ubicación debe comunicarse a la unidad de gestión competente en materia de teletrabajo, con la consiguiente declaración de que se conocen las recomendaciones en materia de prevención de riesgos laborales por parte de los teletrabajadores y el compromiso de su cumplimiento en la nueva oficina.

Cabe destacar también que, en la solicitud de teletrabajo, debe incluirse la ubicación de la oficina a distancia, así como una declaración de que se han leído las recomendaciones en materia de prevención de riesgos laborales facilitadas por la Administración y el compromiso de que, a la fecha de inicio de la autorización del teletrabajo, aquellas se cumplirán en la oficina a distancia[11]. En la misma línea, uno de los requisitos para que se autorice el teletrabajo es declarar que se conocen las medidas en materia de prevención de riesgos laborales y el compromiso de cumplirlas en la oficina a distancia en la fecha del teletrabajo[12].

Por otra parte, una vez autorizado el teletrabajo, el servicio de prevención responsable de la evaluación del puesto de trabajo remite al teletrabajador el correspondiente auto-cuestionario de prevención de riesgos laborales, que deberá ser devuelto debidamente cumplimentado y firmado para su valoración. Es responsabilidad del teletrabajador el cumplimiento de lo declarado en el autocuestionario, así como la adopción de las medidas correctoras que se le propongan.

Finalmente, cabe destacar que la Administración de Castilla y León ha elaborado unos protocolos de desarrollo en materia de prevención de riesgos laborales muy completos y accesibles para los propios teletrabajadores a través de internet.

2) En segundo lugar, en la Comunidad Valenciana uno de los requisitos para poder solicitar el teletrabajo es que el puesto de trabajo desde el que se quiera realizar cumpla con la normativa vigente en materia de prevención de riesgos laborales[13].

Asimismo, el órgano competente en materia de prevención debe verificar, con carácter previo al teletrabajo y mediante la comprobación del cuestionario rellenado por el teletrabajador (se trata de un cuestionario muy completo, recogido en el anexo III del Decreto 82/2016), que las condiciones en que se ejercen

11. Artículo 21.
12. Artículo 5.
13. Artículos 5.1.d y f del Decreto 82/2016.

las funciones del puesto de trabajo en el domicilio no suponen un riesgo para la salud.

Por su parte, el teletrabajador puede solicitar que el órgano competente en materia de prevención de riesgos laborales realice una inspección domiciliaria con la finalidad de comprobar las condiciones alegadas en el cuestionario; esta solicitud puede realizarse durante toda la vigencia del teletrabajo.

Por otra parte, el personal que se seleccione para teletrabajar debe realizar un curso de formación específico sobre la prestación de servicios bajo esta modalidad, donde, entre otros contenidos, se incluirán las cuestiones de seguridad y salud en el trabajo[14]. Entre los contenidos del curso se incluyen: el programa básico de prevención de riesgos laborales, el trabajo con pantallas de visualización de datos (PVD), las medidas de seguridad en los trabajos de carácter administrativo, la prevención de incendios, la actuación ante un incendio y los primeros auxilios.

Finalmente, en el artículo 16 del Decreto 82/2016, de 8 de julio, se recoge la Comisión de Control y Seguimiento del Teletrabajo en la Administración de la Generalitat Valenciana, entre cuyos miembros está la persona titular de la subdirección general a la que corresponde el ejercicio de las funciones de prevención y protección de riesgos laborales correspondiente al sector de la Administración de la Generalitat, lo que denota la transcendencia que se da a la materia que estamos tratando.

3) También existe una regulación bastante extensa en el caso de la Comunidad Autónoma de La Rioja. Así, en primer lugar, el artículo 9 del Decreto 45/2013, de 5 de diciembre, establece como causas de denegación de la solicitud de teletrabajo el no adoptar el trabajador las medidas preventivas y correctoras recomendadas por el servicio de prevención de riesgos laborales o negarse a permitir que su personal efectúe sus funciones de comprobación del cumplimiento de estas medidas. En la misma línea, el artículo 12.f) fija las mismas causas como elementos de revisión de la propia situación de teletrabajo.

Por otra parte, en el artículo 18 se incorporan las siguientes reglas:

a) El servicio de prevención de riesgos laborales facilitará al teletrabajador, la evaluación de los riesgos de su actividad, así como la información necesaria en materia de seguridad y salud laboral para evitar los riesgos laborales o, si son inevitables, minimizarlos y disponer la aplicación de las medidas preventivas necesarias.

b) El teletrabajador debe acudir a una sesión formativa donde se le indica como acondicionar su puesto de trabajo fuera de las dependencias administrativas, así como las nociones necesarias sobre seguridad y ergonomía en los puestos de trabajo con pantallas de visualización de datos. La asistencia a esta sección informativa tiene carácter obligatorio y deben acreditarse los conocimientos adquiridos mediante una prueba.

14. Artículo 10 y anexo IV del Decreto 82/2016.

c) El teletrabajador debe aplicar en todo caso las medidas previstas en su evaluación de riesgos, así como la formación e información facilitada por el servicio de prevención no solo a su actividad, sino también en el diseño de su puesto de trabajo. En todo caso, el servicio de prevención le proporcionará asistencia y asesoramiento telefónico cuando lo requiera.

Y, d) el teletrabajador puede solicitar al servicio de prevención el examen del puesto de trabajo en su domicilio. Se accederá a esta solicitud cuando el servicio de prevención considere que es necesaria la presencia domiciliaria. En caso de que el servicio de prevención recomiende adoptar medidas correctoras en el puesto de trabajo, es responsabilidad del teletrabajador su implantación.

Y, finalmente, en materia de formación, el artículo 19 del Decreto 45/2013 señala que la Escuela de La Rioja de Administración Pública organizará acciones formativas para el personal al que se le ha autorizado el teletrabajo relativas al cumplimiento de esta modalidad de trabajo no presencial, y sobre la protección de la salud y la prevención de riesgos laborales en el puesto de trabajo.

4) En cuarto lugar, en el País Vasco el artículo 16 del Decreto 92/2012, de 29 de mayo, se dedica a la cuestión de la prevención de riesgos laborales, señalándose que:

a) El servicio de prevención facilitará al trabajador que se acoja al teletrabajo la evaluación de riesgos de su actividad, así como la formación e información necesarias en materia de seguridad y salud laboral para evitar los riesgos laborales o, si son inevitables, minimizarlos y disponer la aplicación de las medidas preventivas necesarias. Así mismo, el trabajador debe acudir a una sesión formativa donde se le indicará como acondicionar el puesto de trabajo fuera de las dependencias administrativas, así como las nociones necesarias sobre seguridad y ergonomía en los puestos de trabajo con pantallas de visualización de datos. La sesión formativa es obligatoria y deberán acreditarse los conocimientos adquiridos mediante una prueba.

b) El teletrabajador debe aplicar en todo caso las medidas previstas en su evaluación de riesgos, así como la formación e información facilitada por el servicio de prevención no solo a su actividad, sino también al diseño de su puesto de trabajo. No obstante, el servicio de prevención le proporcionará la asistencia y asesoramiento telefónico que necesite.

Y, c) el teletrabajador puede solicitar al servicio de prevención el examen de su puesto de trabajo. Se accederá a esta petición cuando el servicio de prevención considere que es necesaria esa presencia domiciliaria. Cuando el servicio de prevención recomiende adoptar medidas correctoras en el puesto de trabajo, es responsabilidad del teletrabajador su implantación.

Y, finalmente, el artículo 17 del Decreto 92/2012, establece que el Instituto Vasco de Administración Pública organizará acciones formativas para el personal autorizado para teletrabajar relativas al cumplimiento del propio teletrabajo, así como a la protección de la salud y seguridad en el puesto de trabajo.

5) En el marco de la Comunidad Autónoma de Extremadura, el artículo 9 del Decreto 1/2018, prevé que, una vez autorizado el teletrabajo, y con carácter previo a su inicio, el trabajador debe recibir una formación específica en materia

de prevención de riesgos laborales, y en particular sobre la manera de adaptar su puesto de trabajo, así como sobre las nociones necesarias sobre seguridad y ergonomía en los puestos de trabajo con pantallas de visualización.

Cabe tener presente que, conforme al artículo 14.1.d), uno de los requisitos para poder solicitar el teletrabajo es que el lugar donde se vayan a prestar los servicios cumpla con la normativa vigente en materia de seguridad y salud laborales.

Respecto a la formación requerida, en el artículo 9 se establece que, una vez autorizado el teletrabajo y con carácter previo a su inicio, el teletrabajador debe recibir una formación específica en materia de prevención de riesgos laborales, incidiendo particularmente en la forma de adaptar su puesto de trabajo y en los riesgos derivados de las pantallas de visualización de datos. Esta formación tiene carácter obligatorio.

Finalmente, cabe destacar que en el artículo 11 del Decreto 1/2018 se establece que, con carácter previo al inicio del teletrabajo, el servicio de prevención valorará el entorno laboral y emitirá un informe sobre sus condiciones. Únicamente se realizará una valoración presencial cuando así lo solicite el teletrabajador o cuando el propio servicio de prevención lo considere necesario, y siempre previa comunicación al teletrabajador. Si el servicio de prevención recomienda adoptar medidas correctoras en el puesto de trabajo, su implantación es responsabilidad del teletrabajador. La falta de implantación puede dar lugar a la revisión de la autorización de teletrabajo[15].

6) En la Comunidad Autónoma de Castilla-La Mancha, el Decreto 57/2013 también trata la cuestión de la prevención de riesgos laborales; así se prevé que:

a) Los teletrabajadores tienen derecho a una adecuada protección en materia de seguridad y salud, resultado de aplicación, en todo caso, lo que se establece en la Ley de Prevención de Riesgos Laborales, y en su normativa de desarrollo[16].

Y, b) como en otras Comunidades Autónomas, uno de los requisitos de acceso al teletrabajo es que el lugar desde el que se vaya a realizar cumpla con la normativa vigente en materia de seguridad y salud laborales.

7) En el caso de Aragón[17] solo se recoge la obligación de garantizar las condiciones exigides en materia de prevención de riesgos laborales, así como la obligación de formación en relación con las medidas necesarias de protección de la salud y prevención de riesgos laborales en el puesto de trabajo.

8) En Galicia, la Orden de 20 de diciembre de 2013, establece que deben garantizarse las condiciones exigidas en materia de prevención de riesgos laborales[18]; añadiéndose que a la correspondiente solicitud debe acompañarse un formulario en materia de prevención de riesgos laborales[19]. Y también se señala

15. Artículo 19.2.e) del Decreto 1/2018.
16. Artículo 4.2.
17. Instrucción de 6 de agosto de 2014.
18. Artículo 13.
19. Artículo 15.1.

que la Escuela Gallega de Administración Pública debe facilitar la formación necesaria en materia de prevención de riesgos laborales[20].

9) En el ámbito de las Islas Baleares, el Decreto 36/2013, prevé que existe la obligación de garantizar el cumplimiento de las condiciones exigidas en materia de prevención de riesgos laborales. Y que debe informarse al teletrabajador de la política en materia de seguridad y salud laboral, especialmente sobre las exigencias relativas a las pantallas de datos. El trabajador autorizado para teletrabajar debe rellenar un cuestionario de auto-comprobación en materia de prevención de riesgos laborales facilitado por el servicio competente[21].

Y, junto a ello, la Escuela Balear de Administración Pública debe acreditar, cuando corresponda, que el teletrabajador ha cumplimentado de forma correcta un cuestionario sobre, entre otras materias, la prevención de riesgos laborales. Previamente debe ponerse a disposición del teletrabajador un manual de teletrabajo con el contenido necesario.

Y, 10) finalmente, la materia de prevención de riesgos laborales también se recoge en la normativa autonómica catalana. Así, el Decreto 77/2020, de 4 de agosto, establece que en el plan personal de trabajo del teletrabajador debe constar expresamente el compromiso de respetar y aplicar la normativa y las medidas específicas que se determinen en materia de prevención de riesgos laborales[22]. Y el artículo 9.1 prevé que los teletrabajadores y sus supervisores deben recibir formación, entre otras materias, en prevención de riesgos laborales.

En conclusión, tanto en el sector público como privado las normas ofrecen las pautas necesarias para que se garantice la protección de los teletrabajadores frente a los riesgos laborales; pautas que se completan con lo previsto en la Ley de Prevención de Riesgos Laborales y su normativa de desarrollo. A nuestro entender, ese marco legal es suficiente y adecuado; la cuestión esencial, como en el caso del trabajo presencial, es cómo se concreta en la práctica dicha normativa y su grado de incumplimiento, presentándose en este ámbito un reto adicional, como es el hecho de que el teletrabajo se desarrolla, normalmente, en el propio domicilio del teletrabajador. Domicilio protegido por el reconocimiento constitucional de su inviolabilidad.

20. Artículo 16.
21. Artículo 11.5.
22. Artículo 6.3.a).

3. LA REGULACIÓN DE LA PREVENCIÓN DE RIESGOS LABORALES EN LA NEGOCIACIÓN COLECTIVA QUE ABORDA EL TELETRABAJO

3.1. El sector privado

En el sector privado, la prevención de riesgos laborales en el marco del teletrabajo tiene un cierto interés para la negociación colectiva, si bien algunos convenios colectivos se limitan a señalar, desde una perspectiva genérica, que se cumplirá lo que se prevé en la Ley de Prevención de Riesgos Laborales y en la normativa que la desarrolla en cada momento. Y también se añade que se mantendrá la cobertura por accidente de trabajo y enfermedad profesional[23].

En cambio, otros convenios colectivos recogen una regulación más específica, lo que es totalmente recomendable, dada la transcendencia de la materia que nos ocupa; así, a modo de ejemplo:

a) Se prevé que el desarrollo del teletrabajo en el domicilio solo será posible cuando el espacio resulta adecuado a las exigencias de la seguridad y salud en el trabajo. La empresa debe informar al trabajador sobre su política en materia de seguridad y salud laboral, especialmente sobre las exigencias relativas a las pantallas de visualización. El teletrabajador debe aplicar correctamente esa política y la empresa es responsable de su protección. Para verificar la correcta aplicación de las normas, la empresa y la representación de los trabajadores solo podrán acceder al domicilio del teletrabajador previa notificación y consentimiento por parte de este. La empresa debe adoptar medidas para prevenir el aislamiento del teletrabajador en relación con otras personas de la empresa[24].

b) Se señala que el lugar de teletrabajo debe contar con una serie de condiciones que garanticen que se podrá desarrollar el trabajo habitual en un entorno adecuado. Además de los requisitos que garanticen la conexión, debe contarse con un espacio que cumpla las condiciones mínimas en materia de prevención, seguridad y salud de un puesto de trabajo tipo. Estas condiciones mínimas constarán en el acuerdo individual de teletrabajo. Para comprobar estas condiciones, el teletrabajador se compromete a aceptar una visita de evaluación de riesgos, la fecha y la hora de la cual se concertará personalmente con cada teletrabajador[25].

c) Se establece que la empresa facilitará a los teletrabajadores y a los representantes de los trabajadores información sobre las condiciones de seguridad y salud laboral en que deba prestarse el teletrabajo. Y también se afirma que: 1) la empresa informará al teletrabajador de su política en materia de salud y se-

23. CC de la empresa Thales España GRP (BOE de 11 de julio de 2020). També, CC de Repsol comercial de productos petrolíferos (BOE de 23 de noviembre de 2018).

24. CC estatal de perfumería y afines (BOE de 20 de agosto de 2019).

25. CC de Repsol comercial de productos petrolíferos (BOE de 23 de noviembre de 2018).

guridad en el trabajo, especialmente sobre las exigencias relativas a las pantallas de datos; 2) el teletrabajador aplicará correctamente esta política; 3) el desarrollo del teletrabajo en el domicilio del trabajador solo será posible cuando este espacio resulte adecuado a las exigencias de seguridad y salud en el trabajo; 4) la empresa debe adoptar las medidas necesarias para prevenir el aislamiento del teletrabajador en relación con el resto de los trabajadores de la empresa; y, 5) para poder verificar la correcta aplicación de las medidas de seguridad, la empresa y los representantes de los trabajadores solo podrán acceder al domicilio del teletrabajador previa notificación y con su consentimiento previo[26].

Y, d) especialmente es el II CC de empresas vinculadas Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU, que recoge una completa regulación en materia de prevención de riesgos laborales; así se establece que:

1) Para evitar situaciones de aislamiento o de no pertenencia, es necesario establecer con carácter obligatorio reuniones de contacto bien con el equipo de trabajo del teletrabajador, con los colaboradores o con el responsable directo. Estas reuniones tendrán lugar con una periodicidad semanal, garantizando al menos una jornada de trabajo presencial.

Y, 2) se incluyen una serie de recomendaciones relacionadas con los puestos de trabajo con pantallas de visualización de datos, que necesariamente tienen que cumplir los teletrabajadores; así:

— El puesto de trabajo debe tener unas dimensiones suficientes para permitir los cambios de postura y movimientos de trabajo.
— El usuario de terminales con pantalla tiene que poder ajustar fácilmente la luminosidad y el contraste entre los caracteres y el fondo de pantalla, y adaptarlos fácilmente a las condiciones del entorno.
— Los caracteres tienen que poderse apreciar fácil y nítidamente a una distancia entre 40 y 60 cm y tienen que ser estables, sin vibraciones ni parpadeos.
— La altura ideal de la pantalla es aquella que permite visualizarla dentro del espacio comprendido entre la línea de visión horizontal y la trazada a 60 grados bajo la horizontal.
— Es conveniente, sobre todo en los trabajos de entrada de datos en base a listados o cualquier otro tipo de documentos, la instalación de un portadocumentos junto a la pantalla y a su misma altura para evitar posturas incorrectas, puesto que el movimiento del cuello cuando se mira a la pantalla y a los documentos se realiza en un plano horizontal que es menos perjudicial que el vertical.
— Es muy importante dejar espacio suficiente ante el teclado para que el usuario pueda apoyar los brazos y las manos,
— El asiento tiene que ser giratorio y graduable en altura. El apoyo tiene que ser inclinable, regulable en altura o en su defecto con ajuste lumbar.

26. CC general de la industria química (BOE 8 de agosto de 2018).

— Los puestos de trabajo tienen que instalarse de tal forma que las fuentes de luz como por ejemplo ventanas y otras aperturas, tabiques y equipos no provoquen deslumbramiento directo ni reflejos en la pantalla.
— La empresa realizará la vigilancia de la salud (reconocimientos médicos) a intervalos periódicos.
— A fin de eliminar el riesgo eléctrico se tomarán una serie de precauciones elementales como, por ejemplo: no sobrecargar las tomas de los enchufes, no depositar líquidos en las proximidades de los equipos en general y los teclados en particular y abstenerse de abrir, manipular o introducir objetos por la parte posterior de las pantallas.
— Queda expresamente autorizada la empresa para que mediante los técnicos y/o delegados de prevención pueda acceder al domicilio del teletrabajador para las comprobaciones que estime oportunas, previa notificación al teletrabajador con 48 horas de antelación al menos y con su autorización, y con respecto a las garantías constitucionales de inviolabilidad del domicilio, con la observancia de las comunicaciones legales oportunas.
— Periódicamente se realizarán estudios y controles de salud para determinar la incidencia del teletrabajo en la salud laboral, informándose a la representación de los trabajadores de su evolución.
— Y, finalmente, se dará a los teletrabajadores una formación adecuada y de calidad sobre el uso de las herramientas básicas del teletrabajo, centrándose en las cuestiones psico-sociales necesarias para una correcta adecuación al nuevo entorno laboral.

3.2. El caso de las Administraciones Públicas

Aunque pueda sorprender, la negociación colectiva desarrollada en las Administraciones Públicas —tanto respecto del personal funcionario como del personal laboral—, muestra poco interés respecto al teletrabajo. Y, muy probablemente, ello se debe a que, como vimos, la regulación de esta materia se está llevando a cabo a través de acuerdos concretos en las diversas Administraciones.

Partiendo de ello, a modo de ejemplo, algún convenio colectivo que regula el teletrabajo se limita a fijar una franja de disponibilidad obligatoria de teletrabajo —de 9 a 14 horas—, sin perjuicio de las previsiones en materia de descanso dentro de la jornada, descanso entre jornadas y descanso semanal. No aborda la cuestión de la prevención de riesgos laborales[27].

27. Convenio colectivo del Consejo Comarcal del Maresme 2023-2026 (BOP de Barcelona de 20 de julio de 2023).

4. RECOMENDACIONES SOBRE LA FORMA DE GESTIONAR LA PREVENCIÓN DE RIESGOS LABORALES EN EL MARCO DEL TELETRABAJO

Una vez analizados los textos que tratan sobre la prevención de riesgos laborales en el marco del teletrabajo, tanto a nivel de la Unión Europea como estatal y autonómico, así como la reciente negociación colectiva de los sectores público y privado, es posible realizar algunas consideraciones respecto a cómo sería conveniente abordar las cuestiones relacionadas con la prevención de riesgos laborales en dicho ámbito; consideraciones que son aplicables tanto en el marco de las Administraciones Públicas como en las empresas privadas, al tratarse de una "cuestión común". Así:

1) Como señalamos, la Ley de Prevención de Riesgos Laborales y sus normas de desarrollo resultan aplicables en el marco del teletrabajo, y, en consecuencia, el empleador público o privado, según el artículo 14 de aquella, tiene la obligación de "garantizar la seguridad y salud de los trabajadores a su servicio en todos los aspectos relacionados con el trabajo", y, con tal fin, adoptará todas las medidas de prevención necesarias. Este deber general de protección también se aplica al teletrabajo, con independencia de donde se desarrolle este.

Y junto a esto, el empleador (público o privado), en el caso del teletrabajo, también está obligado a:

a) La evaluación de los riesgos laborales[28].

b) La planificación y facilitación de los equipos de trabajo y medios de protección individuales (artículos 17 y 23.1.b) de la Ley de Prevención de Riesgos Laborales).

c) A informar y formar a los teletrabajadores sobre los riesgos existentes en su puesto de trabajo[29]. También debe formarlos sobre las peculiaridades de la prestación de servicios vía teletrabajo.

d) A ejercer la vigilancia de la salud de los teletrabajadores[30].

Y, e) en su caso, también está obligado a la protección de la maternidad, los menores, los trabajadores temporales y de empresas de trabajo temporal y de los trabajadores especialmente sensibles a determinados riesgos[31].

Por otro lado, aunque, como decíamos, la Ley de Prevención de Riesgos Laborales y sus normas de desarrollo resultan aplicables íntegramente en el marco del teletrabajo, esto no impide afirmar que esta aplicación no siempre resulta fácil, principalmente cuando la prestación de servicios se desarrolla en el domicilio del teletrabajador (que es lo más habitual en la práctica).

28. Artículos 16 y 23.1.a) y c) de la Ley de Prevención de Riesgos Laborales.
29. Artículos 18 y 19 de la Ley de Prevención de Riesgos Laborales.
30. Artículos 22 y 23 de la Ley de Prevención de Riesgos Laborales.
31. Artículos 25 a 28 de la Ley de Prevención de Riesgos Laborales.

A lo que cabe añadir que algunas normas reglamentarias de desarrollo de la Ley de Prevención de Riesgos Laborales tienen una especial trascendencia en el marco del teletrabajo; es el caso de:

a) Real Decreto 488/1997, de 14 de abril, sobre disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización. Lo analizaremos más adelante.

Y, b) Real Decreto 299/2016, de 22 de julio, sobre la protección de la salud y la seguridad de los trabajadores contra los riesgos relacionados con la exposición a campos electromagnéticos. En este Real Decreto se incluye la obligación del empleador de elaborar y aplicar un plan de acción que tiene que incluir medidas técnicas y de organización dirigidas a evitar que la exposición a estos campos electromagnéticos sea superior a ciertos límites, se establece una obligación de evaluación y, en su caso, la realización de mediciones o cálculos de los niveles de exposición en los campos electromagnéticos, etc.

Y desde otras perspectivas, también cabe tener presente, aunque no tienen valor normativo, la Nota Técnica Preventiva 412 sobre Teletrabajo: criterios para su implantación, aprobada por el Instituto Nacional de Seguridad e higiene en el Trabajo en 1996, y la Guía de actuación de la Inspección de Trabajo en relación con las condiciones laborales y de seguridad y salud en el teletrabajo de 2002.

La Nota Técnica Preventiva 412 puede resultar útil en la hora de concretar las características y actitudes que debería poseer una persona candidata al teletrabajo (flexibilidad, adaptabilidad, confianza, autonomía…), así como las características que deberían cumplir los mandos y gestores vinculados al mismo (deseo de participar en el proyecto de teletrabajo, confianza en sus subordinados, capacidad para organizar el trabajo…).

Y, en fin, como hemos visto, la negociación colectiva también puede regular esta materia, respetando, lógicamente, lo previsto en las normas.

2) Todas las organizaciones, con independencia de su dimensión y actividad, y de su carácter público o privado, tienen la obligación de incorporar el teletrabajo (y a los teletrabajadores) en su plan de prevención de riesgos laborales[32]. Respecto a los contenidos de este plan de prevención de riesgos laborales en relación con el teletrabajo, cabe destacar los siguientes: evaluación de riesgos, medidas de protección y equipos de trabajo, información, formación y participación de los trabajadores, medidas de emergencia y situaciones de riesgo grave e inminente, vigilancia de la salud, coordinación de actividades, protección de colectivos especialmente sensibles, organización de la actividad preventiva y obligaciones de los trabajadores.

3) Desde la perspectiva de la prevención de riesgos laborales, el domicilio del teletrabajador es un centro de trabajo, con todos los efectos asociados (obligación de evaluación, adopción de medidas de prevención…). Sin embargo, no podemos olvidar que el artículo 18.2 de la Constitución reconoce la inviolabili-

32. Artículo 16 de la Ley de Prevención de Riesgos Laborales.

dad del domicilio particular, incluyendo también otros espacios equiparables (la habitación de un hotel o un hostal, el coche particular…). En todos estos casos, la entrada requiere el consentimiento de su titular o una resolución judicial.

Cabe tener presente, sin embargo, que, con las consiguientes garantías, podría establecerse en el acuerdo de autorización del teletrabajo la posibilidad de acceder en el domicilio del teletrabajador por motivos de prevención de riesgos laborales, aunque, como hemos visto, esta no es la opción por la cual se decanta actualmente la normativa autonómica y local. Y ese acuerdo no excluiría que la decisión última seguiría correspondiendo al teletrabajador[33]. La misma posibilidad se podría recoger a la negociación colectiva, tal como hacen algunos de los convenios analizados en este trabajo, así, es el caso, por ejemplo, del II CC de empresas vinculadas Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones, SAU[34].

Pero, como hemos visto, en los documentos analizados la regla general es que cualquier entrada de los miembros del servicio de prevención en el puesto de trabajo del teletrabajador requiere la petición previa de este o bien su consentimiento.

En este ámbito también es importante destacar que el puesto de trabajo —la oficina a distancia, en los términos de algunos de los documentos analizados—, tiene que fijarse expresa y obligatoriamente en el acuerdo de teletrabajo y este lugar no puede variarse por parte del teletrabajador, puesto que el mismo tiene que cumplir las medidas necesarias en materia de prevención de riesgos laborales. Cualquier cambio tiene que ser comunicado y autorizado previamente por el órgano competente. Así mismo, entendemos que, por causas justificadas, la organización podría limitar el lugar o lugares donde puede ejercerse el teletrabajo.

Finalmente, en este ámbito cabe señalar que la consideración del domicilio como puesto de trabajo a efectos preventivos comporta la aplicación del Real Decreto 485/1997, de 14 de abril, sobre disposiciones mínimas en materia de señalización de seguridad y salud en el trabajo y del Real Decreto 486/1997, de 14 de abril, por el cual se establecen las disposiciones mínimas de seguridad y salud en los puestos de trabajo.

4) En concordancia con el señalado, el empleador tiene la obligación de realizar una evaluación de riesgos laborales respecto del domicilio del teletrabajador, pero solo respecto del espacio habilitado para teletrabajar.

Por otro lado, si se permite que el teletrabajador preste sus servicios en un telecentro, el empleador también tiene la obligación de proceder a la correspondiente evaluación de riesgos laborales. Y, en fin, en los casos de teletrabajo móvil, que implica dejar al teletrabajador la libertad de elegir el lugar de pres-

33. Tal y como ha reconocido la sentencia de la Audiencia Nacional de 22 de marzo, al respecto Rojo Torrecilla, E. (2022). Trabajo a distancia (teletrabajo). Fijación de claros límites a la discrecionalidad del empleador para regular las condiciones de trabajo. Notas a la importante sentencia de la AN de 22 de marzo de 2022. Blog.

34. BOE de 13 de noviembre de 2019.

tación de servicios en cada momento (una biblioteca, un hotel, las instalaciones del cliente, un hotel o cafetería…), la evaluación de riesgos se limitaría a los riesgos derivados de la propia manera de prestar los servicios (riesgos ergonómicos y psicosociales), sin afectar el puesto de trabajo, puesto que este es móvil y libremente elegido por el teletrabajador en cada momento.

Respecto a la manera de llevar a cabo esta evaluación de riesgos cuando se trata de teletrabajo en el domicilio, cabe destacar que, si bien una inspección física del puesto de trabajo es lo más recomendable, no es obligatoria, pudiéndose sustituir —como hemos visto— por un completo cuestionario de autocomprobación facilitado por el servicio de prevención que debe rellenar el teletrabajador y la posterior valoración de las respuestas por parte de este servicio. Y obviamente, con carácter previo, es necesario que el teletrabajador cuente con la formación suficiente en materia de prevención de riesgos laborales.

Por tanto, desde una perspectiva temporal, en primer lugar, tiene que darse la formación, posteriormente el teletrabajador cumplimenta el correspondiente auto-cuestionario adaptado a las características de su puesto de trabajo y, finalmente, el servicio de prevención lo evalúa. Si no existe esta formación o no es adecuada para el puesto de trabajo, obviamente la empresa o Administración Pública habrá incumplido la obligación de evaluar los riesgos laborales.

No podemos olvidar tampoco que la Ley de Prevención de Riesgos Laborales articula la obligación de evaluar los riesgos como una obligación dinámica, no estática, y, por lo tanto, de ser necesario, tendrán que realizarse evaluaciones periódicas. Aquí hay que recordar que el artículo 6.1 del Real Decreto 39/1997, de 17 de enero, que regula los servicios de prevención, establece que tienen que articularse mecanismos eficaces de revisión de la evaluación en aquellos lugares en los que se detecten daños para la salud de los trabajadores o en aquellos otros en los que se haya apreciado que las actividades de prevención planificadas son inadecuadas o insuficientes. A lo que cabe añadir que lo que se evalúa es el puesto de trabajo no las condiciones personales del teletrabajador.

Respecto a los riesgos laborales vinculados al teletrabajo que la empresa o Administración Pública tienen que evaluar necesariamente, cabe señalar que son de dos tipos: a) riesgos asociados al puesto de trabajo (riesgos genéricos; riesgos ergonómicos, incluyendo específicamente los trastornos de tipos musculoesqueléticos; y riesgos derivados de agentes físicos, incluyendo la fatiga visual); y, b) riesgos organizacionales y psicosociales (estrés laboral, tecnoestrés, aislamiento, adicción al trabajo,…). También cabe tener presente el riesgo de incendio o las medidas de emergencia[35].

En primer lugar, en relación con los riesgos genéricos del puesto de trabajo, es posible identificar como medidas de prevención para hacerles frente las siguientes:

a) Es conveniente que el espacio de trabajo tenga luz natural y que el ruido —interno o externo— sea lo más reducido posible.

35. Artículo 20 de la Ley de Prevención de Riesgos Laborales.

b) Es conveniente que el teletrabajador cuente con un espacio de trabajo independiente dentro de su domicilio, y que, además, sea suficiente para contener los equipos y materiales necesarios. El cableado eléctrico y telefónico tiene que estar instalado de manera correcta, para evitar posibles accidentes.

c) El puesto de trabajo tiene que contar con la ventilación necesaria y la temperatura adecuada según la época del año.

Y, d) para prevenir los trastornos musculoesqueléticos —vinculados muchas veces al mantenimiento de posturas estáticas (típicas del teletrabajo) y los movimientos repetitivos— es necesario un buen diseño ergonómico del puesto de trabajo. Esto implica, como mínimo, que:

1) La mesa de trabajo debe tener el espacio suficiente para situar la pantalla y el teclado del ordenador, documentos, materiales, etc. El material tiene que evitar reflejos y la mesa ser regulable en altura.

2) Se debe tener una silla ergonómica, regulable en altura, con reposabrazos y refuerzo en la zona lumbar.

3) El teclado del ordenador tiene que ser inclinable e independiente de la pantalla. Los ordenadores portátiles —por sus dimensiones y tipos de teclado— pueden causar lesiones musculoesqueléticas. Se recomienda conectar el ordenador portátil a una pantalla y teclado independientes.

4) Se debe tener un reposapiés regulable y antideslizante. También es recomendable utilizar reposamuñecas.

Y, 5) la pantalla del ordenador debe evitar reflejos y los caracteres deben tener la dimensión necesaria para facilitar su lectura. Para evitar la fatiga visual, la pantalla tiene que colocarse de manera perpendicular a las ventanas, para evitar deslumbramientos. Así mismo, siguiendo lo previsto en el Real Decreto 488/1997, se requiere que:

— La imagen de la pantalla sea estable, sin destellos u otras formas de inestabilidad.
— Debe ser posible ajustar fácilmente la luminosidad y el contraste para adaptarlos a las características del entorno.
— La pantalla debe ser orientable e inclinable para evitar los reflejos.
— La pantalla debe estar situada a una altura adecuada (dentro del espacio comprendido entre la línea de visión horizontal y la que se encuentra en 60 grados por debajo de la misma).
— Colocar la pantalla, el teclado y los documentos en una distancia similar de los ojos para evitar la fatiga visual y los giros de la cabeza y el cuello. La distancia recomendada de lectura de la pantalla respecto a los ojos es de entre 40 y 55 cm.
— Y, en fin, también es conveniente realizar pausas para descansar y reducir el tiempo máximo de trabajo ante una pantalla de ordenador.

En segundo lugar, respecto a los riesgos organizacionales y psicosociales, cabe destacar que estos se concretan principalmente, como señalábamos anteriormente, en el aislamiento, la adición al trabajo o el tecnoestrés.

El primero deriva del hecho que el teletrabajador trabaja en su propio domicilio, en solitario, lo que limita claramente el contacto personal con otros com-

pañeros, clientes o usuarios —el contacto se lleva a cabo a través de correo electrónico, telefónicamente, vía WhatsApp…—. La adición al trabajo puede surgir ante jornadas largas de trabajo en las que no hay control del empleador, lo que puede llevar a una auto-explotación por parte del propio teletrabajador.

Y, en fin, más específico todavía, el tecnoestrés puede presentar tres variantes: a) la tecnofatiga, que consiste en la fatiga mental derivada del uso prolongado y continuado de las nuevas tecnologías; b) la tecno adicción, que implica una incontrolable compulsión a utilizar las nuevas tecnologías durante largos periodos de tiempos; y, c) la tecnofobia, que deriva del sobreesfuerzo para adaptarse a las nuevas tecnologías.

Respecto a las medidas preventivas en relación con este tipo de riesgos, hay que señalar que:

a) Para evitar o reducir el aislamiento resulta conveniente, al margen de la fórmula del teletrabajo a tiempo parcial, convocar reuniones periódicas entre el teletrabajador y sus compañeros o supervisores, actividades formativas, etc.

b) Para prevenir la sobreexplotación, el estrés laboral o la adicción al trabajo es necesario arbitrar limitaciones de la jornada, pausas y descansos. A esto ayuda el control y el registro de la jornada de trabajo, aplicable tanto en el sector privado como en las Administraciones Públicas.

c) Y, finalmente, para evitar o reducir el tecnoestrés es esencial la formación sobre un buen uso de las nuevas tecnologías, así como el establecimiento de un servicio de apoyo para la resolución de posibles problemas. En el caso de la tecno adicción también es esencial el control de la jornada de trabajo, para evitar extralimitaciones.

Y, en todos los casos, la formación de los teletrabajadores sobre las medidas a tomar para evitar estos riesgos es esencial. Formación que es obligatoria y que debería renovarse o actualizarse cada vez que resulte necesario.

5) Si bien la evaluación de los riesgos laborales se centra exclusivamente en el puesto de trabajo y no en las características personales del teletrabajador, cabe tener presente que no todas las personas tienen las habilidades y competencias necesarias por el teletrabajo (flexibilidad, adaptabilidad, confianza, capacidad de organización…), en la línea apuntada por la, antes citada, Nota Técnica Preventiva 412 del Instituto Nacional de Seguridad e higiene en el Trabajo. Esto implica que, aunque las funciones del puesto de trabajo sean susceptibles de ser ejercidas a través del teletrabajo, no todo solicitante de teletrabajo será apto para teletrabajar. Y autorizar para el teletrabajo a una persona no apta puede comportar un riesgo para su seguridad y salud laboral, y dar lugar a las correspondientes responsabilidades a cargo de la empresa o Administración Pública (recargo de prestaciones, pago de indemnizaciones…).

6) Cabe plantearse qué pasa cuando el empleador no cumple con su obligación de evaluación de los riesgos o lo hace de manera defectuosa. En este caso, como vimos, el Acuerdo Marco Europeo sobre Teletrabajo reconoce al teletrabajador la posibilidad de solicitar a su empleador una inspección. También se abre, en su caso, la posibilidad de presentar una denuncia ante la Inspección de Trabajo y Seguridad Social.

7) Se ha apuntado que el teletrabajo tiene como inconvenientes el incremento de hábitos como el tabaco, el alcohol o el café, o un mayor sedentarismo, puesto que el espacio de trabajo se encuentra en el propio domicilio. Desde una perspectiva general, resulta recomendable que la empresa o Administración Pública fomente hábitos saludables entre su plantilla.

8) Obviamente, el teletrabajador debe contar con una información suficiente sobre los riesgos específicos de su puesto de trabajo —tanto los asociados al puesto de trabajo como los de carácter organizacional y psicosocial—, así como de las medidas de protección y prevención aplicables. Resulta aplicable el artículo 18.1 de la Ley de Prevención de Riesgos Laborales, donde se prevé que: "A fin de dar cumplimiento al deber de protección… el empresario adoptará las medidas adecuadas para que los trabajadores reciban todas las informaciones necesarias en relación con: a) Los riesgos para la seguridad y la salud de los trabajadores en el trabajo, tanto aquellos que afecten la empresa en su conjunto como cada tipo de puesto de trabajo o función. b) Las medidas y actividades de protección y prevención aplicables a los riesgos señalados en el apartado anterior. c) Las medidas adoptadas en conformidad con lo dispuesto en el artículo 20 de la presente Ley. En las empresas que cuenten con representantes de los trabajadores, la información… se facilitará por el empresario a los trabajadores a través de estos representantes; sin embargo, tendrá que informarse directamente a cada trabajador de los riesgos específicos que afecten su puesto de trabajo o función y de las medidas de protección y prevención aplicables a estos riesgos".

9) Tal y como también se deriva de los documentos analizados páginas atrás, la formación en materia de prevención de riesgos laborales es un elemento clave en el marco del teletrabajo. A tal efecto, el artículo 19 de la Ley de Prevención de Riesgos Laborales establece que el empleador —privado o público— tiene que garantizar que cada trabajador reciba una formación teórica y práctica, suficiente y adecuada, en materia preventiva, tanto en el momento de su contratación, cualquiera que sea la modalidad o duración de esta, como cuando se produzcan cambios en las funciones que ejerza o se introduzcan nuevas tecnologías o cambios en los equipos de trabajo.

La formación debe estar centrada específicamente en el puesto de trabajo o función de cada trabajador, adaptarse a la evolución de los riesgos y a la aparición de otros nuevos y repetirse periódicamente, si fuera necesario (por ejemplo, cuando se constata la presencia de conductas imprudentes o se considera que no se aplican adecuadamente las medidas preventivas). En definitiva, antes de la incorporación al teletrabajo, el teletrabajador debe haber sido formado adecuadamente, con independencia de que se trate de un trabajador temporal o fijo, y esta formación debe actualizarse en el momento en que se produzcan cambios en sus funciones, se introduzcan nuevos métodos de trabajo, nuevos equipos de trabajo o nuevas tecnologías. Esta formación, tal y como afirmamos anteriormente, se tiene que evaluar para garantizar que el teletrabajador la ha interiorizado.

Esta formación tiene que impartirse, siempre que sea posible, dentro de la jornada y en horario de trabajo o, en su defecto, en otras horas, con el recono-

cimiento, en este último caso, del tiempo de descanso compensatorio equivalente retribuido (el coste temporal de esta formación obligatoria va siempre a cargo de la empresa o Administración Pública). La formación puede impartirse con medios propios o bien concertándola con servicios ajenos y su coste no recaerá, en ningún caso, sobre el trabajador.

Todo esto implica que el teletrabajador tiene que recibir una formación adecuada a su puesto de trabajo y sus riesgos, lo que implica que la formación debe incluir los riesgos inherentes en el puesto de trabajo ocupado y los riesgos derivados de las características de la modalidad de trabajo que se ejerce (organización de la jornada, trabajo a resultados, autonomía en la organización del trabajo, resolución de problemas informáticos, medidas para evitar el aislamiento,…), así como la formación necesaria para un uso adecuado del correspondiente equipo informático.

Por otro lado, en el ámbito del teletrabajo esta formación es todavía más importante, teniendo presente que muy difícilmente la organización podrá comprobar directamente que el teletrabajador cumple con las medidas preventivas. Obviamente, esta formación es obligatoria, y si no se realiza y supera adecuadamente, no se puede autorizar el teletrabajo.

Finalmente, en este marco hay que recordar que el Acuerdo Marco Europeo sobre Teletrabajo establece que los superiores jerárquicos y compañeros de trabajo directos del teletrabajador deben recibir formación en aquellas cuestiones que tengan incidencia directa sobre la prevención de riesgos laborales, como por ejemplo: la gestión del trabajo por objetivos o proyectos, el registro de la jornada, la garantía de la desconexión digital, una organización saludable del tiempo de trabajo, formas de reducir el estrés y el aislamiento, etc.

10) Como también pasa en el trabajo presencial, el teletrabajador debe cumplir ciertas obligaciones en materia de prevención de riesgos laborales, conforme a lo que se establece en el artículo 29 de la Ley de Prevención de Riesgos Laborales; así:

a) Tiene que velar por su propia seguridad y salud, así como la de aquellas otras personas a las que pueda afectar su trabajo (el resto de los convivientes del domicilio, por ejemplo).

b) Debe utilizar adecuadamente los instrumentos de trabajo, los medios y equipos de protección, los mecanismos de seguridad, etc.

c) Tiene que informar inmediatamente su superior jerárquico o al servicio de prevención sobre cualquier posible situación de riesgo.

d) Tiene que cooperar con el empleador para garantizar que sus condiciones de trabajo sean seguras y contribuir a que se cumplan todas las obligaciones preventivas previstas legalmente.

Cabe recordar que, tal como establece el propio artículo 29.3 de la Ley de Prevención de Riesgos Laborales, el incumplimiento de las obligaciones preventivas por parte del trabajador —también del teletrabajador— es considerado un incumplimiento laboral o una falta a efectos disciplinarios, pudiéndose iniciar el correspondiente procedimiento disciplinario. Es más, la propia situación particular que ostenta el teletrabajador —trabaja en su propio domicilio— hace que

estas obligaciones en materia preventiva adquieran, incluso, una mayor relevancia.

Por otro lado, en el convenio colectivo o acuerdo sobre teletrabajo tendría que constar expresamente que es causa de revocación del teletrabajo no adoptar las medidas preventivas y correctoras recomendadas por el servicio de prevención de riesgos laborales.

11) Como ya señalamos, la empresa o la Administración Pública tiene que cumplir con un deber de vigilancia de la salud del teletrabajador, conforme a lo que se prevé en el artículo 22 de la Ley de Prevención de Riesgos Laborales.

En este precepto se establece que, como regla general, la vigilancia de la salud solo podrá llevarse a cabo cuando el trabajador preste su consentimiento, con tres excepciones: a) cuando un reconocimiento médico es imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud del trabajador; b) cuando es necesario verificar si el estado de salud del trabajador puede constituir un peligro para él mismo, por los otros trabajadores, o para otras personas relacionadas con la empresa o Administración; y, c) cuando lo establece una disposición normativa, en atención a la protección de riesgos específicos y actividades de especial peligrosidad (enfermedades profesionales, trabajadores nocturnos, exposición al ruido, utilización de pantallas de visualización, agentes cancerígenos...).

Es evidente que el teletrabajo se vincula al uso de pantallas de visualización, y por eso el Real Decreto 488/1997 recoge la obligación de los trabajadores afectados por el mismo a someterse a la vigilancia de la salud. Así, en su artículo 4 se establece la obligación del empleador de garantizar a los trabajadores una vigilancia adecuada de su salud teniendo en cuenta en particular los riesgos para la vista y los problemas físicos y de carga mental, el posible efecto añadido o combinado de estos, y la eventual patología acompañante. Por tanto, se tendrán en cuenta los riesgos ergonómicos y psicosociales-organizacionales (carga de trabajo, forma de gestionar el tiempo, posible estrés, aislamiento, etc.), y la vigilancia la llevará a cabo personal sanitario especializado.

Esta vigilancia de la salud tiene que producirse antes de iniciar la actividad laboral, con posterioridad de manera adecuada al nivel de riesgo, y cuando aparezcan trastornos que pudieran derivarse del trabajo. Como en otros ámbitos, el empleador está obligado a facilitar los medios de protección necesarios.

Los reconocimientos médicos vinculados con esta obligación de vigilancia de la salud son obligatorios para los teletrabajadores y, por lo tanto, en caso de negativa, se podría llegar a abrir un procedimiento disciplinario. En cambio, los reconocimientos médicos no ligados a los riesgos derivados del uso de pantallas de visualización son voluntarios. Se tiene que informar previamente al teletrabajador de las pruebas que se llevarán a cabo, la información que se obtendrá con las pruebas y la conexión que existe entre aquellas y los riesgos.

Por otro lado, si la vigilancia de la salud detecta que el teletrabajo afecta la salud del teletrabajador, se deberán poner en marcha las medidas necesarias, que pueden ser simplemente una adaptación o modificación de los equipos de trabajo (mesa, silla, teclado, reposapiés, pantalla…), o de la organización del

trabajo o del tiempo de trabajo (más pausas para descansar, control de la jornada, desconexión digital efectiva…). Si no son suficientes las medidas correctoras, habría que pensar en un cambio de funciones, de puesto de trabajo, e incluso, en una reversión del teletrabajo, volviendo al trabajo presencial a tiempo completo.

12) No podemos olvidar que un control efectivo por parte del empleador de la jornada y de los descansos —registro de la jornada— tiene una gran relevancia en el marco de la prevención de los riesgos laborales, puesto que puede evitar o reducir los riesgos psicosociales vinculados al teletrabajo (adicción al trabajo, fatiga mental, tecnoestrés en sus diversas variantes).

Y obviamente, los mecanismos de control, que pueden ser telemáticos, deben ser respetuosos con el derecho a la intimidad y vida privada del teletrabajador y guardar la proporcionalidad requerida. Se pueden utilizar varios mecanismos de control: sistemas de grabación o video vigilancia, sistemas biométricos, controles sobre el propio ordenador (monitorizando el uso del correo electrónico y de internet…). Las posibilidades son amplias. En todo caso, como decíamos antes, se tienen que respetar los principios de justificación, idoneidad y proporcionalidad del sistema empleado y se tiene que informar al teletrabajador de cómo se llevará a cabo el control.

13) Cabe tener presente que la normativa sobre prevención de riesgos laborales otorga un trato especial al trabajo nocturno, añadiendo obligaciones adicionales por razones evidentes de protección de la salud. Y, lógicamente, el teletrabajo facilita el trabajo en horario nocturno, puesto que, precisamente la flexibilidad horaria es uno de sus rasgos más relevantes. Por lo tanto, a nuestro entender, el empleador puede prohibir el teletrabajo en horario nocturno; esta prohibición se puede incluir en el correspondiente acuerdo de teletrabajo y en caso de que el teletrabajador no la cumpla se podría revocar el teletrabajo y la organización quedaría eximida de cualquier responsabilidad.

14) Tal como prevé la Ley de Prevención de Riesgos Laborales, el empleador —público o privado— tiene la obligación de controlar el cumplimiento de las normas en materia de prevención de riesgos laborales por parte de sus trabajadores y, en el caso del teletrabajo el reto principal deriva del hecho de que la actividad se desarrolla generalmente en el propio domicilio.

En esta cuestión cabe reiterar que, aunque la mejor forma de control sería inspeccionar directamente el puesto de trabajo del teletrabajador, el carácter inviolable del domicilio exige siempre su consentimiento y una notificación previa con tiempo suficiente. Y si este no se da, la responsabilidad de aplicar adecuadamente las medidas requeridas para hacer frente a los riesgos recae en el propio teletrabajador.

15) Lógicamente, cabe tener presente que, tanto los delegados de prevención como el comité de seguridad y salud, tienen que estar atentos a la situación y a los riesgos específicos derivados del teletrabajo, con la dificultad adicional que comporta el hecho que los teletrabajadores ejercen sus funciones en su domicilio particular. No se podrá acceder en el domicilio sin el consentimiento del teletrabajador.

Tiene que informarse periódicamente al Comité de Seguridad y Salud sobre los aspectos esenciales del teletrabajo (número de empleados teletrabajando, perfil, posibles incidencias, situaciones particulares, informes de los supervisores o gestores…).

16) Cabe destacar que, en algún caso excepcional, el teletrabajo se podría imponer a un trabajador cuando surge una necesidad desde la perspectiva de la prevención de riesgos laborales. Sería el caso, por ejemplo, en que existiendo una situación conflictiva en la organización a nivel colectivo o individual (vinculada a riesgos psicosociales) que exige no pasar a la persona a una baja médica, al considerar que podría agraviarse su estado, se decide el paso temporal al teletrabajo en su domicilio, al considerarse que con esto se facilitaría su recuperación. Se trataría, en todo caso, de una situación temporal y excepcional.

17) Sin entrar a fondo en el tema, también cabe recordar que, desde la perspectiva de la prevención de riesgos laborales y para garantizar la salud, es esencial que se garantice el derecho a la desconexión digital de los teletrabajadores, teniendo presente aquello previsto en el artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre.

La empresa o Administración Pública debe tener una política interna sobre esta materia que, además, trate de forma particular la situación de los teletrabajadores, con el objetivo, entre otros, de garantizarles los descansos, el respeto de la jornada máxima y cualquier otro límite en materia de tiempo de trabajo derivado de la normativa vigente.

Y también, desde una perspectiva preventiva, es necesario desarrollar acciones de formación y sensibilización de los teletrabajadores sobre la necesidad de hacer un uso responsable de las herramientas informáticas que evite los riesgos psicosociales, particularmente la fatiga informática y el tecnoestrés.

Y, 18) finalmente, cabe recordar que, como en el caso del trabajo presencial, en el teletrabajo existe el riesgo de ser acosado, ya sea sexualmente, por razón de sexo, por causas discriminatorias o psicológicamente. Por lo tanto, es necesario que en los protocolos que regulen el acoso, tanto en las empresas como en las Administraciones Públicas, se incluya la figura del teletrabajo y se adopten las medidas pertinentes para evitar que los teletrabajadores sean acosados.

BIBLIOGRAFÍA

De Las Heras García, A. (2016) *El teletrabajo en España: un análisis crítico de normas y prácticas.* CEF.

Curull, M., Maynou, L. y Farré, L. (2024), *Teletrabajo después de la pandemia. Análisis desde la perspectiva del trabajador.* Fundación La Caixa.

García Calvente, Y (2020). Avances y desafíos del teletrabajo en la regulación del teletrabajo: reflexiones del ingreso y el gasto público en un contexto de pandemia. *Nueva Fiscalidad*, n.º 3.

Lousada Arochena, J.F., y Ron Latas, R.P. (2015), Una mirada periférica al teletrabajo, el trabajo a domicilio y el trabajo a distancia en el derecho

español, en, MELLA MÉNDEZ, L. (ed.), *Trabajo a Distancia y Teletrabajo*. Thomson Reuters Aranzadi.

MAURI MAJÓS, J. (2020), La reglamentación del teletrabajo en las administraciones locales. *Seminario sobre Relaciones Colectivas*. FMC.

MELLA MÉNDEZ, L (2015). Configuración general del trabajo a distancia en el derecho español, en Mella Méndez, L. (Dir.*), El teletrabajo en España: aspectos teórico-prácticos de interés*. Wolters Kluwer.

ROJO TORRECILLA, E. (2022). Trabajo a distancia (teletrabajo). Fijación de claros límites a la discrecionalidad del empleador para regular las condiciones de trabajo. Notas a la importante sentencia de la AN de 22 de marzo de 2022. Blog.

SIERRA BENÍTEZ, E.M. (2011). *El contenido de la relación laboral en el teletrabajo*. CES Andalucía.

THIBAULT ARANDA, J. (2010), *El teletrabajo*. CES.

I. Empresa y organización interna

La constitución en línea de sociedades de responsabilidad limitada. La incorporación al Derecho español de la Directiva 2019/1151 y la Propuesta de reforma de la normativa europea

Jorge Miquel Rodríguez
Profesor Titular de Derecho Mercantil
Universidad Autónoma de Barcelona

ABSTRACT:
Directive 2019/1151, known as the "Company Digitalization Directive" was incorporated into the Spanish legislation by Law 11/2023, which represents an important advance in the online constitution of limited liability companies (private companies only) that, except in a duly justified exception, may be established without the need to physically appear at the notary's office. This procedure is only possible if the contributions are monetary. In addition, throughout the life of the company, procedures can be maintained electronically. The procedure also applies to branches. We will also examine the Proposal to reform the Directive

Keywords: Private companies, online constitution, Proposal to reform the Directive

Palabras clave: sociedades limitadas, constitución en línea, reforma de la Directiva

SUMARIO:

1. INTRODUCCIÓN

La constitución en línea de sociedades de responsabilidad limitada ha experimentado un notable impulso en los últimos años, como consecuencia principalmente de a Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo de 20 de junio de 2019 por la que se modifica la Directiva (UE) 2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades[1]. Con carácter previo también podemos advertir que no es la primera regulación en nuestro ordenamiento referida a la constitución de sociedades por vía telemática, que se remonta a 20 años atrás con la Ley 7/2003, de 1 de abril, de la sociedad limitada Nueva Empresa, derogada por la Ley 18/2022, de 28 de septiembre y diversa regulación posterior.

La Directiva 2019/1151 fue incorporada a nuestro ordenamiento con un retraso considerable, pues el plazo de adaptación terminaba el 1 de agosto de 2021 y en cambio se introdujo con la Ley 11/2023, de 8 de mayo, de transposición de Directivas de la Unión Europea en materia de accesibilidad de determinados productos y servicios, migración de personas altamente cualificadas, tributaria y digitalización de actuaciones notariales y registrales; y por la que se modifica la Ley 12/2011, de 27 de mayo, sobre responsabilidad civil por daños nucleares o producidos por materiales radiactivos. Del propio título se desprende que se trata de una Ley muy extensa, pues incorpora nada menos que seis Directivas. Ha transcurrido más de un año desde su promulgación y precisamente con ese plazo se ha completado un periodo transitorio hasta estar plenamente desarrollada. La primera parte de nuestro estudio se dedicará a repasar los aspectos más relevantes de la Directiva, así como su incorporación a nuestro ordenamiento.

Nos dedicaremos con mayor atención a esbozar las novedades previstas para un futuro previsiblemente próximo, en lo que a las reformas del Derecho de la Unión Europea se refiere, que implicará también ulteriores modificaciones en nuestro ordenamiento. Teniendo en cuenta que ha habido elecciones al Parlamento Europeo y que por tanto esos trabajos preparatorios han interrumpido su curso normal, y que debamos siempre advertirlo de manera cautelar, parece claro que más allá de cambios de detalle que pueda haber, las líneas maestras

1. Sin perjuicio de las menciones a la redacción originaria de la Primera Directiva, la norma de referencia es por tanto la Directiva (UE) 2017/1132 2009/101/CE del Parlamento Europeo y del Consejo, de 14 de junio de 2017 sobre determinados aspectos del Derecho de sociedades (versión codificada) (DOUE-L-2017-81254).

de las reformas proyectadas no deberían separarse mucho de lo que se ha aprobado ya.

En concreto, esos trabajos preparatorios están avanzados y han cristalizado en el anuncio por parte del Consejo de la UE en febrero de 2024 de la adopción de una posición única que implica un mandato de negociación para avanzar en los cambios necesarios para profundizar en la digitalización en el Derecho de sociedades y acompañando una Propuesta de Directiva. Se trabaja esencialmente en torno a la Propuesta de Directiva de marzo de 2023 del Parlamento Europeo y del Consejo por la que se modifican las Directivas 2009/102/CE y (UE) 2017/1132 en lo que respecta a la ampliación y mejora del uso de herramientas y procesos digitales en el ámbito del Derecho de sociedades, y también se actualiza la Directiva de 2019 sobre el uso de herramientas y procesos digitales en el derecho de sociedades[2].

La Propuesta, que examinaremos con detalle, manifiesta de manera clara la intención de avanzar en los logros ya conseguidos, con la finalidad principal de conseguir una mayor competitividad en las empresas de la UE. Se aumentará la disponibilidad de la información disponible además de una mejora en la transparencia y por otro lado se busca una mayor conexión en las administraciones públicas que también suponga una reducción de los trámites y la burocracia en general, incluyendo los referidos al empleo de la información de otros registros mercantiles en situaciones transfronterizas.

Esos objetivos se concretan con medidas de refuerzo del Sistema de Interconexión de Registros Mercantiles (BRIS). Se pretende garantizar que los datos de las empresas en los registros mercantiles sean precisos, fiables y estén actualizados. Se refuerza el principio "una sola vez" que ya está presente en la norma-

2. Existe ya una literatura abundante, entre los trabajos recientes de carácter general que podemos mencionar, sin perjuicio de otras referencias ulteriores relativas a cuestiones concretas, puede verse: MADRID PARRA, A., (2023) "La constitución telemática de sociedades mercantiles: Opciones de política legislativa", en AAVV (coord. MJ PEÑAS MOYANO), *Estudios de Derecho de sociedades y de Derecho concursal: libro en homenaje al profesor Jesús Quijano González,* Valladolid, pp. 459 y ss., MIQUEL RODRÍGUEZ, J. (2023), La constitución en línea de Sociedades de Responsabilidad Limitada. Transposición de la Directiva 2019/1151 y reforma de la Ley de Sociedades de Capital, en La Ley mercantil, núm. 103, FUENTES NAHARRO, M., (2023) *La digitalización del derecho de sociedades, La Directiva 2019/1151 y su trasposición al Derecho español*, Pamplona 2023, la obra colectiva NIETO CAROL, U (dir.) (2023) *La digitalización en el derecho de sociedades*, Valencia y dentro de ella, especialmente relevantes en el contexto de nuestras páginas, EMBID IRUJO, J.M., "La digitalización del Derecho de Sociedades", pp. 17 y ss. y NIETO CAROL, U., "Constitución en línea de sociedades limitadas", pp. 73 y ss. y CABANAS TREJO, R. y RIVAS RUÍZ, A., (2024) *La constitución de la sociedad de responsabilidad limitada tras las últimas reformas legales y la reciente doctrina registral: Procedimientos telemáticos y redacción de estatutos*, Barcelona. También podemos mencionar ALVAREZ ROYO-VILLANOVA, S (2021) "Propuesta de adaptación de la directiva de digitalización 2019/1151 a la vista del derecho comparado", Revista Lex Mercatoria, núm 18, BOQUERA MATARREDONA, J. (2021), "La digitalización de las sociedades de capital españolas tras las Directivas europeas sobre la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades", RDM 320, HERNANDO CEBRIA, L. (2022)" Modelos societarios y digitalización en la movilidad transfronteriza intracomunitaria", RdS, núm 65.

tiva actual y la legislación interna que la incorpora a los diversos ordenamientos, pero se proponen también medidas específicas, como eliminar la necesidad de una apostilla en determinadas situaciones o la introducción de un certificado de empresa de la UE multilingüe, también para esas situaciones transfronterizas. El mandato de negociación del Consejo comparte los principales objetivos de la Propuesta de Directiva, pero va más allá en algunas cuestiones, Así, por mencionar algunos, se desarrolla el principio "una sola vez" en casos de filiales o sucursales transfronterizas y se pretende también incidir en la reducción de trámites en casos de grupos de sociedades.

2. LA DIRECTIVA 2019/1151

La Directiva 2019/1151 ya incorporada a nuestro Derecho ya ha sido objeto de estudio y atención entre nosotros, de manera que me voy a limitar a recordar algunas ideas esenciales que nos sean de utilidad en el marco de las presentes reflexiones.

La primera idea es que se trata de una Directiva de mínimos, que impone como obligación principal y casi única que los Estados miembros regulen un sistema de constitución de las sociedades de capital íntegramente en línea, sin necesidad de que los solicitantes comparezcan en persona, contemplándose como excepcional la posibilidad de requerir la presencia física en determinadas circunstancias que efectivamente han sido recogidas por el legislador español.

El segundo principio fundamental que podemos destacar especialmente es que el procedimiento no alcanza solamente a la constitución, sino que se extiende a toda la vida de la sociedad: en eso precisamente consiste el principio "solo una vez", que es un eje esencial de todo el sistema.

En tercer lugar, debe insistirse en que el procedimiento es también aplicable al registro de sucursales, que tiene una extensión notable en la Directiva y que con carácter general se trata de una materia que tiene una importante trascendencia práctica que no viene siempre acompañada de un tratamiento legislativo acorde con esa importancia[3].

El extenso Preámbulo de la Ley 11/2023 explica con todo detalle los antecedentes tanto a nivel europeo como interno en lo referido a la modernización del Derecho de sociedades en la parte relativa a la digitalización. Existen distintos momentos que se pueden identificar como impulsores de los cambios en esta dirección, principalmente a lo largo de todo el siglo XXI y de manera particular durante la pasada década. En clave registral, es particularmente relevante la puesta en marcha del Sistema de Interconexión de Registros centrales, mercantiles y de sociedades de todos los Estados miembros (SIRM o BRIS acrónimo de

3. Específicamente, FERNÁNDEZ DEL POZO, L. (2020) "La publicidad registral de las sucursales tras la publicación de la Directiva (UE) 2019/1151 de herramientas digitales", La Ley Mercantil núm 67, FUENTES NAHARRO, *La digitalización, cit.*, pp. 46 y ss.

Business Registers Interconnection System), materializado en la Directiva 2012/17 y otra normativa posterior. También podemos referirnos como un antecedente reciente de la Directiva a la comunicación de la Comisión Europea de 6 de mayo de 2015 "Una Estrategia para el Mercado Único Digital de Europa", cuyas líneas maestras son visibles en la Directiva 2019/1151, destacando de manera significativa el principio de "solo una vez"[4]. La Directiva ocupa un total de 25 páginas del Diario Oficial, es decir que tiene una extensión relativamente amplia. En cambio, su transposición al Derecho español se ha realizado con cierta contención, como veremos a continuación.

A pesar de tratarse de una Directiva de mínimos conviene señalar alguna opción de la Directiva que el legislador español ha decidido no acoger. La primera destacable es que en el caso español solamente se dirige a las sociedades de responsabilidad limitada. Naturalmente, sería posible extender este sistema al procedimiento de constitución de sociedades anónimas. Así lo determina expresamente el artículo 13 octies 1 segundo párrafo, cuando advierte que *los Estados miembros podrán decidir no ofrecer procedimientos de constitución en línea para otros tipos de sociedades que no sean los enumerados en el anexo II BIS*. El legislador español ha optado por no extenderlo más allá de las sociedades de responsabilidad limitada y esa es también la opción que predomina de manera generalizada en los países de nuestro entorno. De otro lado, la Directiva 2019/1151 también permite que los Estados Miembros regulen este procedimiento de manera única y exclusiva para el caso de que las aportaciones sean dinerarias: así lo señala el artículo 13 octies 4 d) *la exclusión de la constitución en línea en aquellos casos en que el capital social de la sociedad se suscriba mediante contribuciones en especie*. En las jurisdicciones que tienen mayor tradición e influencia entre nosotros, como por ejemplo Alemania o Italia se ha optado por la misma solución, tanto en la limitación tipológica, como en su aplicación exclusiva a las aportaciones dinerarias

Desde un punto de vista sustancial, el artículo 13 octies de la Directiva es el que merece una mayor atención. En ese precepto podemos encontrar las claves de la reforma, basada en una serie de principios esenciales que deben incorporar a sus ordenamientos los Estados miembros. El primero de ellos, que la constitución de sociedades pueda realizarse de manera telemática —en línea— de manera íntegra, sin necesidad de comparecencia en persona por parte de los interesados. Se menciona de manera explícita que se incluye aquí el otorgamiento de la escritura de constitución de una sociedad, si bien se advierte de la po-

4. Para una visión general de esta evolución, cfr. por todos, GÓRRIZ LÓPEZ, C., *Derecho originario: principio de libre establecimiento. Derecho secundario: armonización y derecho uniforme*, en AAVV (coord. MIQUEL RODRIGUEZ, J. y PÉREZ TROYA, A.), *Derecho de sociedades europeo*, Madrid, 2019, pp. 27 y ss. De manera específica con un exhaustivo repaso a la Directiva, cfr. en la misma obra, CABANAS TREJO, R., *Procedimiento en línea (constitución, registro y presentación de documentos e información), publicidad y registro*, en *Derecho de sociedades europeo,* cit., pp. 79 y ss.

sible excepción prevista en el artículo 13 ter, apartado 4 y en el artículo 13 octies apartado 8[5].

La Directiva también hace referencia específica a la necesaria existencia de modelos estandarizados (con mayor precisión se regula la cuestión en el artículo 13 nonies), señalando el artículo 13 octies 2 que los Estados miembros establecerán normas detalladas para la constitución en línea de sociedades, mientras que el artículo 13 octies 3 entra en cuestiones muy detalladas que han sido recogidas también —como veremos— por nuestro legislador. En concreto, se exigen de manera necesaria hasta seis aspectos distintos: los procedimientos para garantizar que los solicitantes tienen la capacidad jurídica necesaria y el poder para representar a la sociedad; los medios para comprobar la identidad de los solicitantes de conformidad con el artículo 13 ter; los requisitos aplicables a los solicitantes para la utilización de los servicios de confianza a que se refiere el Reglamento (UE) no. 910/2014; los procedimientos para comprobar la legalidad del objeto —también de la denominación— de la sociedad en la medida en que dichos controles estén previstos en Derecho nacional y finalmente los procedimientos para comprobar el nombramiento de los administradores.

Asimismo, según el artículo 13 octies 4, de manera opcional determina una serie de cuestiones que podrán establecer los Estados miembros. De una parte, menciona los procedimientos para garantizar la legalidad de la escritura de constitución de la sociedad, en particular la verificación del correcto uso de los modelos y también la función del notario o de cualquier otra persona u organismo habilitado en virtud del Derecho nacional para tratar cualquier aspecto de la constitución en línea de una sociedad.

De otro lado, menciona dos aspectos a los que nos referiremos de manera específica porque nuestro legislador ha decidido incorporarlos. Se trata de las *consecuencias de la inhabilitación de un administrador por la autoridad competente de cualquier Estado miembro* y también la *posibilidad de exclusión de la*

---

5. El artículo 13 ter 4 ha sido incorporado a nuestro ordenamiento de manera muy fiel. *Cuando se justifique por razón de interés público en impedir el uso indebido o la alteración de identidad, los Estados miembros podrán, a los efectos de comprobar la identidad de un solicitante, adoptar medidas que requieran la presencia física de ese solicitante ante cualquier autoridad, persona u organismo habilitado en virtud del Derecho nacional para tratar cualquier aspecto de los procedimientos en línea a que se refiere el presente capítulo, incluido el otorgamiento de la escritura de constitución de una sociedad. Los Estados miembros se asegurarán de que solo pueda exigirse la presencia física de un solicitante caso por caso cuando existan razones para sospechar una falsificación de identidad, y de que cualquier otra fase del procedimiento pueda completarse en línea.*

El artículo 13 octies apartado 8 incide en la misma cuestión: *Cuando se justifique por razón de interés público en garantizar el cumplimiento de las normas sobre capacidad jurídica y sobre el poder de los solicitantes para representar a una sociedad, cualquier autoridad o persona u organismo habilitado en virtud del Derecho nacional para tratar cualquier aspecto de la constitución en línea de una sociedad, incluido el otorgamiento de la escritura de constitución, podrá solicitar la presencia física del solicitante. Los Estados miembros se asegurarán de que, en tales casos, solo pueda exigirse la presencia física de un solicitante caso por caso cuando existan motivos para sospechar que se han incumplido las normas contempladas en el apartado 3, letra a). Los Estados miembros garantizarán que cualquier otra fase del procedimiento pueda no obstante completarse en línea.*

constitución en línea en aquellos casos en que el capital social de la sociedad se suscriba mediante contribuciones en especie.

Esa apretada síntesis de la Directiva pretende dejar claro el punto de partida para la reforma prevista, ya anunciada y con algunos frutos en el año 2023 y continuada en 2024[6]. El crecimiento exponencial en el empleo de la digitalización en todos los sectores obliga a replantear algunas premisas de la Directiva, en el sentido de ampliar y actualizar su ámbito de aplicación, según señala la propia Comisión.

3. LA LEY 11/2023

Como se ha advertido, la Ley 11/23 de 8 de mayo incorpora diversas Directivas. En lo que a nosotros nos ocupa, se dedicó el título IV, compuesto de seis artículos, del 34 al 39, en el que se modifican diferentes normas. En concreto, la Ley del Notariado de 1862, el Código de Comercio de 1885, la Ley Hipotecaria de 1946; también sendas Leyes de Medidas fiscales, administrativas y del orden social (de 2000 y 2001) y finalmente el Texto Refundido de la Ley de Sociedades de Capital de 2010. La Ley 11/2023, de 8 de mayo se completa con el *Real Decreto 442/2023, de 13 de junio, por el que se modifica el Reglamento del Registro Mercantil, aprobado por el Real Decreto 1784/1996, de 19 de julio, y por el que se traspone parcialmente la Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se modifica la Directiva (UE) 2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades* al que haremos referencia posteriormente. Es imprescindible, por tanto, tener presente que existen otras modificaciones relevantes que tienen un amplio alcance en lo referido a la práctica notarial y registral, que van más allá del objeto de estas líneas, las novedades en la LSC. La entrada en vigor de la Ley en la parte que nos ocupa se produjo al día siguiente de su publicación en el BOE, aunque en su conjunto ha tardado un año entero en entrar en vigor plenamente.

Como se recuerda en el propio Preámbulo y ya hemos advertido, no es la primera regulación en nuestro ordenamiento referida a la constitución de sociedades por vía telemática, que se remonta a 20 años atrás, en concreto con la Ley 7/2003, de 1 de abril, de la sociedad limitada Nueva Empresa, figura derogada desde la Ley 18/2022, de 28 de septiembre. Existe en esa misma dirección diversa regulación posterior en los años 2010, 2013 y 2015. Puede observarse que toda esta normativa interna —pero también la Directiva 2019/1151— es anterior a la COVID, que precisamente supuso un punto de inflexión muy notable por el crecimiento exponencial en cuanto al empleo de la digitalización en las socieda-

6. De manera más extensa, *infra*. IV. Cfr. asimismo el Programa de trabajo de la Comisión para 2023: COM(2022) 548 final y sus anexos. Puede verse un resumen en el comunicado de prensa de 18-10-2022: https://ec.europa.eu/commission/presscorner/detail/es/IP_22_6224

des de capital —por ejemplo, en lo referido a las juntas—. A pesar de esa regulación previa, no se cumplían plenamente las exigencias de la Directiva, de ahí la necesidad de introducir algunas modificaciones, dirigidas principalmente, como veremos a continuación, a garantizar la constitución íntegramente en línea, el mantenimiento a lo largo de la vida de la sociedad y la extensión al régimen de las sucursales. Debe recordarse que el procedimiento se aplica solamente a sociedades de responsabilidad limitada y únicamente en los casos en que las aportaciones sean dinerarias.

La reforma es bastante concisa, tanto en lo que se refiere al número de artículos introducidos como a su extensión. En concreto son seis nuevos preceptos los que se incorporan a la Ley de Sociedades de Capital. Se trata, en particular, de los artículos 20 bis, 22 bis, 40 bis, 40 ter, 40 quater y 40 quinquies. La incorporación de la Directiva en lo que a modificaciones de la LSC se refiere, se limita solamente a ellos y a un apartado 3 añadido al artículo 213 LSC. Procederemos a comentarlos de manera individual advirtiendo desde ahora que su trascendencia desde un punto de vista sustantivo me parece desigual. Se mezcla algún precepto dedicado íntegramente a definiciones, con otro que deja todo su contenido a un desarrollo reglamentario ulterior y también alguno más en el que predominan aspectos notariales y registrales. Debemos insistir en que la incorporación de la Directiva también afecta con carácter general a otra normativa de mayor alcance, como la Ley del Notariado o la Ley Hipotecaria. Veamos de manera individual las novedades que afectan a cada uno de los artículos. De manera sistemática, las dos primeras modificaciones (20 bis y 22 bis) se encuadran en el Título I (*La constitución de las sociedades de capital*) Capítulos I (*Disposiciones generales*) y II (*Constitución de sociedades*). Por su parte, los artículos 40 bis a 40 quinquies se encuadran en un nuevo Capítulo III bis, que lleva por título *La constitución electrónica de la sociedad de responsabilidad limitada (constitución en línea)*. Por último, el artículo 213.3 está situado en el Título VI *La administración de la sociedad,* Capítulo II *Los administradores*.

En primer lugar, el nuevo artículo 20 bis LSC se dedica exclusivamente a definiciones: *Medio de identificación electrónica, Sistema de identificación electrónica, Medios electrónicos, Constitución, Registro de una sucursal* y *Modelo*. Personalmente, echo en falta una referencia concreta al significado de la frase *instrumento de pago electrónico de amplia disposición en la Unión Europea*, cuyo significado y alcance específico me parece que debe buscarse en alguna norma externa, tanto a la Ley de Sociedades de Capital, como a la propia Ley 11/2023. En mi opinión, y sobre todo teniendo en cuenta la estructura del artículo 20 bis, hubiera sido oportuna esa aclaración, como se hace por ejemplo en los apartados 1) y 2), "medio de identificación electrónica" y "sistema de identificación electrónica" y en cambio me parecen menos necesarias —aunque tampoco estén de más— las referencias de los apartados 4, 5 y 6.

Aparece aquí la única mención al registro de sucursal en la reforma de la Ley de Sociedades de capital: *"Registro de una sucursal"; el proceso que conduce a la publicidad de documentos e información relativos a una sucursal de nueva apertura en un Estado miembro*.

El artículo 22 bis bajo la rúbrica *Constitución de sociedades en línea* establece unas cuantas ideas clave. Primero, naturalmente que se trata de un procedimiento facultativo que no afecta a la posibilidad de acudir a cualquier otro. Asimismo, se proclama que las referencias afectan tanto al momento de la constitución como al resto de la vida de la sociedad. Se establece, no obstante, una matización muy relevante: no podrá utilizarse el procedimiento íntegramente en línea cuando la aportación de los socios al capital social se realice mediante aportaciones que no sean dinerarias.

Los artículos 40 bis a 40 quinquies se encuadran en un nuevo capítulo de la Ley, el capítulo III bis, bajo la rúbrica *La constitución electrónica de la sociedad de responsabilidad limitada (constitución en línea)*.

La Ley meramente deja para un desarrollo ulterior lo establecido en el artículo 40 bis, titulado *Modelos electrónicos para la constitución electrónica*, pues habrá que introducir modificaciones en el Documento Único Electrónico, estatutos tipo y escritura pública estandarizada. Se prevé que esos documentos deberán ser accesibles a través de la pasarela digital única europea y en la línea con la conexión con otra normativa que va más allá de la regulación de la LSC deberá además contemplar *un nudo de comunicación con la plataforma notarial.*

Se requiere que los documentos señalados estén redactados en español, en las lenguas cooficiales y en inglés. Además, de nuevo en una referencia ajena a la LSC se advierte que el otorgamiento de la escritura pública y su inscripción se realizarán conforme a la normativa correspondiente notarial y registral.

El artículo 40 ter, referido a las aportaciones —siempre dinerarias— determina que "serán efectuadas mediante un instrumento de pago electrónico de amplia disposición en la Unión Europea" y permita la identificación de la persona que realizó el pago. Se establece también que la documentación, valoración y transmisión de las aportaciones dinerarias serán instrumentadas electrónicamente, si bien el notario comprobará cuando sea necesario, que se ha acreditado la realidad y, en su caso, la valoración de las aportaciones efectuadas al capital social de la sociedad. Asimismo, remitiendo al 62.2 LSC, se advierte que no será necesario acreditar la realidad de las aportaciones dinerarias en la constitución de sociedades de responsabilidad limitada si los fundadores manifiestan en la escritura que responderán solidariamente frente a la sociedad y frente a los acreedores sociales de la realidad de las mismas.

El artículo 40 quater establece que el Registro Mercantil competente para recibir la escritura pública de constitución y sus anexos documentales electrónicos será el del domicilio social de la sociedad que se constituya y se establecen unos plazos muy breves en el caso de empleo de escrituras en formato estandarizado con campos codificados y estatutos tipo (seis horas hábiles contadas desde el día siguiente al de la fecha del asiento de presentación o, en su caso, al de la fecha de devolución del documento retirado) o en los demás casos un máximo de cinco días laborables (contados desde el siguiente al de la fecha del asiento de presentación o, en su caso, al de la fecha de devolución del documento retirado). Se admite, sin embargo, que pueda haber causa justificada por razones técnicas o por especial complejidad del asunto que impida el cumpli-

mento de dicho plazo, en cuyo caso el Registrador mercantil deberá notificar esta circunstancia al interesado.

Por último, el artículo 40 quinquies establece la posibilidad de que existan excepciones a la constitución íntegramente en línea y sin necesidad de comparecencia presencial ante el notario, excepciones que en cualquier caso se referirían al momento inicial y no a la vida posterior de la sociedad. Esas dos excepciones, que como se ha advertido antes, están expresamente contempladas por la Directiva, son de una parte dirigidas a "evitar cualquier falsificación de identidad" y a "comprobar la identidad exacta del fundador" y de otro lado, para proceder a la "completa comprobación de la capacidad del otorgante y, en su caso, sus efectivos poderes de representación". Se requiere en estos casos que se anexen a la escritura los motivos por los que se ha exigido la presencia de los comparecientes.

Las novedades en la LSC al incorporar la Directiva 2019/1151 se concretan como hemos visto en la introducción de nuevos preceptos que tienen en común que giran en torno a la constitución en línea, con los requisitos que hemos visto.

Un añadido ulterior en un contexto algo diferente es el previsto en el nuevo 213.3 LSC, que establece los siguiente: *A los efectos de lo dispuesto en este artículo, podrá tomarse en consideración cualquier inhabilitación o información pertinente a efectos de inhabilitación vigente en otro Estado miembro de la Unión Europea.*

En el contexto del contenido de esta reforma, puede llamar la atención este nuevo inciso, pues se encuentra ubicado sistemáticamente en un lugar distinto, en concreto en el marco de las prohibiciones para ser administrador que con carácter general contempla el artículo 213 LSC. Por citar algunos ejemplos, los menores de edad no emancipados, los judicialmente incapacitados, personas inhabilitadas conforme a la Ley Concursal, condenados por delitos contra la libertad, contra el patrimonio o contra el orden socioeconómico, contra la seguridad colectiva, contra la Administración de Justicia o por cualquier clase de falsedad, así como aquéllos que por razón de su cargo no puedan ejercer el comercio entre otros.

El artículo 213.3 LSC trae causa de la previsión del artículo 13 decies de la Directiva, precepto extenso que es incorporado a nuestro ordenamiento de manera muy sucinta[7].

La finalidad del artículo de la Directiva y consecuentemente del nuevo 213.3 LSC es doble: favorecer la realización de actividades transfronterizas, pero también permitir que pueda prevenirse algún eventual abuso. Por ese motivo, se facilita el intercambio de información relativa a una posible inhabilitación para ser administrador, de modo que un Estado miembro pueda rechazar el nombramiento de una persona inhabilitada en otro Estado miembro. Sin embargo, esto

7. En este sentido, sobre el precepto de la Directiva, cfr., CABANAS TREJO, *op. cit.,* pp. 97-99 y ampliamente FUENTES NAHARRO, *La digitalización, cit*., pp. 113 y ss.

no es una obligación, por lo que no existe la obligación de solicitar dicha información de manera sistemática.

Por lo que se refiere a las sucursales, en el marco de la reforma de la Ley de Sociedades de Capital con motivo de la incorporación de la Directiva a nuestro ordenamiento, las menciones concretas a las sucursales son muy escasas. Sin embargo, como ya se ha advertido, la Directiva 2019/1151 sí le dedica una atención notable a la sucursal. Como recuerda el Preámbulo de la Ley 11/2023, todo el procedimiento realizado íntegramente en línea se extiende al registro de sucursales, pues la Directiva pretende que sea posible abrir y registrar una sucursal en otro Estado miembro de manera enteramente telemática, y exige que los Estados miembros se informen mutuamente a través del sistema BRIS acerca de los cierres de sucursales o las modificaciones de razón social o de domicilio social, en sintonía con el principio "solo una vez".

En la Ley 11/2023 las referencias concretas a las sucursales son pocas. Más allá de lo que dice el Preámbulo, que acabamos de sintetizar, podemos citar la escueta mención en el artículo 20 bis LSC, ya comentado, como única referencia específica a ella. En el marco de la incorporación de la Directiva hay que referirse entonces a la modificación del Código de comercio, en concreto en su apartado 17.5 que sí realiza una extensa referencia a la sucursal y que de alguna manera supone, aquí sí, la recepción de la Directiva, completada luego con el RD 442/2023 modificando el Reglamento del Registro Mercantil[8].

También llama la atención que dentro de las diversas Directivas que se incorporan en la Ley 11/2023, hay una referencia a las sucursales en una modificación de la *Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y*

8. Dice ahora el artículo 17.5 del Código de comercio que *el Registro Mercantil asegurará la interconexión con la plataforma central europea en la forma que se determine por las normas de la Unión Europea y las normas reglamentarias que las desarrollen. El intercambio de información a través del sistema de interconexión facilitará gratuitamente información sobre las indicaciones referentes a:*

a) La denominación y forma jurídica de la sociedad, su domicilio social, el Estado miembro en el que estuviera registrada, su número de registro y su Identificador Único Europeo (EUID).

b) Detalles del sitio web de la sociedad, cuando consten en el Registro.

c) Estado de la sociedad, como si ha sido cerrada, suprimida del Registro, disuelta, liquidada o está económicamente activa o inactiva.

d) Objeto de la sociedad.

e) Datos de las personas que, como órgano o como miembros de tal órgano, estén actualmente autorizadas por la sociedad para representarla en las relaciones con terceros y en los procedimientos jurídicos, y si las personas autorizadas a representar a la sociedad pueden hacerlo por sí solas o deben actuar conjuntamente.

f) Información sobre cualquier sucursal de la sociedad en otro Estado miembro, que incluya la denominación, el número de registro EUID y el Estado miembro en que esté registrada la sucursal.

El Registro Mercantil facilitará igualmente de manera gratuita información sobre las indicaciones antes señaladas, bien de manera directa o bien redirigiendo al interesado a la plataforma central europea.»

su internacionalización, y de manera específica de su artículo 22.1[9], que se realiza en el marco de la transposición (parcial) de la *Directiva (UE) 2021/1883 del Parlamento Europeo y del Consejo, de 20 de octubre de 2021, relativa a las condiciones de entrada y residencia de nacionales de terceros países con fines de empleo alta cualificación y por el que se deroga la Directiva 2009/50/CE del Consejo*.

La transposición de la Directiva en esta materia se completa con el RD 442/2023, cuya entrada en vigor se pospuso, como se ha advertido ya, para coincidir con la del artículo 38 de la Ley 11/2023, es decir, en mayo de 2024 un año después de la publicación en el BOE. El RD 442/2023 reforma solamente el Reglamento del Registro Mercantil. No realiza modificaciones en los artículos existentes, y en cambio se introducen nuevos preceptos: un artículo 94 bis[10] y los artículos 308 bis a 308 septies cuyas rúbricas nos dan una idea de su contenido. Los tres primeros, *creación en línea de sucursales de una sociedad establecida en otro estado miembro de la Unión Europea*, *documentación a presentar para la creación en línea de una* sucursal y *cierre en línea de una sucursal*. Los tres siguientes, aunque situados inmediatamente después, están ubicados en una nueva Sección 3.ª llamada *Información societaria europea y su acceso mediante la plataforma central europea y el Identificador Único Europeo (EUID): Información societaria europea*, *información sobre sucursales de sociedades europeas* y

---

9. *«Artículo 22. Servicios de los Puntos de Atención al Emprendedor.*

1. Las personas físicas y jurídicas podrán realizar a través de los Puntos de Atención al Emprendedor todos los trámites administrativos necesarios para el cese de la actividad de empresarios individuales y para la extinción y cese de la actividad de sociedades mercantiles.

En particular, podrá encargarse la realización de los siguientes trámites:

a) Las actividades relativas a la constitución de sociedades y otros actos posteriores.

b) La solicitud de la inscripción al Registro Mercantil de la disolución, liquidación y extinción de la sociedad, del nombramiento de los liquidadores, del cierre de sucursales y, en general, cancelación del resto de asientos registrales.

c) La comunicación de la extinción de la empresa o el cese definitivo de su actividad y baja de los trabajadores a su servicio a la Dirección Provincial de la Tesorería General de la Seguridad Social.

d) La declaración de baja en el Censo de Empresarios, Profesionales y Retenedores y declaración de baja en el Impuesto de Actividades Económicas.

e) La comunicación de la baja en los Registros sectoriales estatales, autonómicos y municipales en los que se hubiese inscrito la empresa o sus instalaciones.

f) La comunicación de cese de actividad a las autoridades estatales, autonómicas y municipales cuando ésta sea preceptiva.

g) En caso de empresarios de responsabilidad limitada, la solicitud de cancelación de las inscripciones que resulten necesarias en el Registro Mercantil, en el Registro de la Propiedad, de Bienes Muebles y en cualesquiera otros Registros en los que estuvieren inmatriculados los bienes inembargables por deudas empresariales o profesionales.

10. *Se asignará a las sociedades de capital y a las sucursales de sociedades de otros Estados miembros un identificador único europeo (EUID), que permita identificarlas inequívocamente en las comunicaciones entre los registros a través del sistema de interconexión de registros mercantiles. Dicho identificador único europeo se compone de prefijo del país (ES); código del Registro Mercantil seguido de un punto; identificador único de sociedad o sucursal y, en su caso, un dígito de verificación que permita evitar errores de identificación*

modificación registral de datos de sucursales transfronterizas intracomunitarias.

Por último, creo de interés mencionar que en la Disposición final séptima se establece que se podrá disponer gratuitamente, a través del sistema de interconexión de Registros, de una información y una serie de documentos que enumera en su apartado 2 letras a) a h)[11].

4. LA PROPUESTA DE MODIFICACIÓN DE LA DIRECTIVA

Por motivos diversos, la normativa sobre constitución en línea y en general sobre otros aspectos de la digitalización de sociedades debe ser revisada con vistas a avanzar y llegar aún más lejos de lo que se ha conseguido hasta ahora. Esas razones se sintetizan en tener en cuenta la situación actual tanto en lo referido a las posibilidades técnicas como de empleo y difusión general de los mecanismos de comunicación a distancia, como al hecho de que hay sectores en los que el objetivo es ya no el de profundizar, sino simplemente iniciar nuevos caminos[12]. Nos referiremos a los aspectos recientemente publicados, tal como se encuentran en el estado actual los trabajos preparatorios, pero no podemos obviar otros aspectos generales, de contexto general. Así, los referidos a la nueva etapa legislativa que se inicia en la Unión Europea y que a pesar de estar ante cuestiones que no parecen objeto de discrepancia, sí es posible que pueda haber una preferencia por impulsar una normativa determinada lo que en ocasiones se traduce en un menor interés por desarrollar otra. Como ha sucedido siempre en lo que a trabajos preparatorios en el marco de la UE se refiere —y también en nuestro propio contexto interno tenemos ejemplos— normas que parece que van a ser aprobadas, en un momento determinado se abandona su tramitación. En este caso, sin embargo y sin perjuicio de que determinadas cuestiones pueden quedar fuera del eventual resultado final sí tengo la impresión de que la

---

11. *Denominación o denominaciones y forma jurídica de la sociedad, domicilio social de la sociedad y Estado miembro en el que está registrada, número de registro de la sociedad y su EUID, detalles del sitio web de la sociedad, cuando consten en el Registro nacional, estado de la sociedad, como si ha sido cerrada, suprimida del registro, disuelta, liquidada o está económicamente activa o inactiva, tal como se determine en el Derecho nacional y cuando conste esta información en los Registros nacionales, objeto de la sociedad, cuando conste en el Registro nacional, datos de las personas que, como órgano o como miembros de tal órgano, estén actualmente autorizadas por la sociedad para representarla en las relaciones con terceros y en los procedimientos judiciales, y si las personas autorizadas a representar a la sociedad pueden hacerlo por sí solas o deben actuar conjuntamente, Información sobre cualquier sucursal de la sociedad en otro Estado miembro, que incluya la denominación, el número de registro EUID y el Estado miembro en que esté registrada la sucursal.*

12. Con mayor detalle, el documento *Revision of Directive 2019/1151/EU on digital tools and processes in company law* de abril de 2023, (EPRS, *European Parlamentary Research Service*, elaborado por HUEMER, M-A): https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)740247#:~:text=Directive%202019%2F1151%2FEU%20on%20the%20use%20of%20digital%20tools,documents%20for%20limited%20liability%20companies

aprobación de algunos de los puntos que se comentarán a continuación va a ser poco menos que inevitable, por una cuestión de necesidad.

Como es frecuente en el ámbito de la normativa que se impulsa en la Unión Europea, se dan explicaciones muy completas sobre el estado de los trabajos, lo que se pretende conseguir y las vías que se utilizarán para hacerlo. De ese modo, se informa con detalle del acuerdo alcanzado por el Consejo y el Parlamento para ampliar el uso de herramientas digitales en el Derecho de sociedades de la UE[13]. Siendo exactos, el título del epígrafe referido a la Propuesta de modificación de la Directiva es una simplificación, puesto que en realidad su alcance va más allá y la modificación de la Directiva 2019/1151 es solamente una parte de toda la Propuesta. Podemos resumir los objetivos que se pretende conseguir en una idea central: hacer más accesibles un mayor número de datos societarios que contribuirán a aumentar la confianza y la transparencia en las empresas de los Estados miembros, además de crear unas administraciones públicas más conectadas y conseguir reducir y simplificar los trámites, para las propias empresas, pero también para otros interesados, esencialmente en situaciones de carácter transfronterizo. De ese modo se seguirá avanzando en un mercado único que tendrá una mayor integración y digitalización para las empresas.

La Comisión publicó en marzo de 2023 una propuesta de Directiva para la ampliación y mejora del uso de herramientas y procesos digitales en el ámbito del Derecho de sociedades. El Consejo adoptó su mandato de negociación en febrero de 2024. La propuesta contribuirá a los objetivos establecidos en las diversas Comunicaciones que van en esa dirección: *Brújula Digital 2030*, *La digitalización de la justicia en la UE*, *Actualización del nuevo modelo de industria de 2020* y *Una estrategia para las pymes en pro de una Europa sostenible y digital*. La idea de la Comisión es profundizar en los objetivos de conseguir una información societaria exacta, fiable y actualizada, que pueda ser consultada por los interesados a través del sistema BRIS de interconexión de los registros empresariales. La reducción de trámites burocráticos antes mencionada se consigue a través de la eliminación de determinados trámites, así como la creación de un poder de digital para toda la UE, y también un certificado de sociedad de la UE, multilingüe. El acuerdo entre el Parlamento y el Congreso profundiza aún más en las intenciones de la Comisión, y se introducen todavía algunas modificaciones que pretenden precisamente avanzar en la simplificación, pero también en la reducción de cargas. Del examen de la Propuesta de Directiva en su versión actualizada hemos detectado una serie de elementos de interés que creemos oportuno destacar, insistiendo en que, a pesar del estado actual como trabajos preparatorios, parece bastante claro que algunos de ellos formarán parte en un futuro relativamente próximo de nuestro panorama societario. Hay identificados

13. En ese sentido, el Comunicado de prensa, de fecha 13 de marzo de 2024 es muy completo: cfr., https://www.consilium.europa.eu/es/press/press-releases/2024/03/13/council-and-parliament-strike-a-deal-to-expand-the-use-of-digital-tools-in-eu-company-law/

diversos puntos, que hemos tratado de sistematizar, aunque ciertamente los diez aspectos podrían ser perfectamente siete o doce, pues muchos de ellos están estrechamente relacionados entre sí y otros también podrían incluso individualizarse aún más.

4.1. Disparidad

Una primera cuestión que claramente preocupa al legislador comunitario es la disparidad, especialmente destacable en los Considerandos 7, 8 y 9 de la Propuesta de Directiva. En ese sentido, se advierte que aunque todos los Estados miembros llevan a cabo controles previos de los diversos documentos y la información societaria antes de que sean inscritos en el Registro Mercantil correspondiente, no hay coincidencia en relación la intensidad de los controles, los procedimientos aplicables o también la persona u órgano encargado de verificar la información.

Por ese motivo, se destaca la importancia de asegurar que existan en todos los Estados miembros unos controles que puedan garantizar un elevado nivel de exactitud y fiabilidad de la información, sin que al mismo tiempo se dejen de respetar las tradiciones de los distintos Estados miembros. Además, es necesario que dichos controles sean obligatorios y se insiste en que en este caso no solamente estaríamos en el marco de la constitución de sociedades íntegramente en línea, sino también con carácter general para cualquier otra forma de constitución de sociedades.

También en esa misma dirección se advierte que se debe garantizar en todos los Estados miembros un control, ya sea administrativo, judicial o notarial preventivo, o cualquier combinación de estos, que respete las tradiciones de los Estados miembros.

4.2. Reducción de costes y cargas administrativas

Me ha parecido oportuno visualizar esta reducción de costes y cargas administrativas a las que se refiere el Considerando 11 de manera individualizada, pues aunque está conectada con la siguiente idea y con la referencia explícita al principio "solo una vez" esta es un objetivo que por sí mismo tiene peso suficiente en toda la política de la Comisión y es plenamente asumida por el Parlamento y el Consejo. Precisamente, se estima que para reducir en mayor medida todavía los costes y las cargas administrativas relacionados con la constitución de sociedades y de manera específica en lo que hace referencia a la duración de los trámites y procedimientos, y también con la intención de facilitar la expansión principalmente de las PYMES en el mercado único, el principio «solo una vez», que ya tienen una importancia notable, debe ampliarse aún más.

4.3. "Solo una vez"

Precisamente, el principio "solo una vez" desarrollado principalmente en los Considerandos 12 y 13 parte de una idea asentada ya y que forma parte de la esencia de la Directiva 2019/115 y en el caso de su incorporación a nuestro Derecho de las reformas introducidas por la Ley 11/2023. Como ya se ha advertido con detalle, la aplicación del principio de «solo una vez» supone para las sociedades no tener que presentar la misma información a las administraciones públicas más de una vez. Pero este principio no solamente debe predicarse de las administraciones públicas, pues supone que haya que volver a presentar esos documentos o esa información a ninguna autoridad, organismo o persona, ya que esas autoridades deben acceder directamente a la información a disposición del público mediante el sistema de interconexión de registros a través del Portal Europeo de e-Justicia.

4.4. La cantidad de información societaria disponible

En el Considerando 14 se destaca que es fundamental aumentar la cantidad de información societaria que esté disponible en toda la Unión, pero también garantizar que esta sea comparable y más fácilmente accesible. En definitiva, la cantidad y calidad de información societaria se convierte en un eje importante de la Propuesta de modificación, aunque en este punto tal vez sea oportuno recordar que no siempre tener mucha información es la mejor opción, puesto que se corre el riesgo de exigir un exceso de información que no sea realmente relevante y en la práctica permita que haya cuestiones importantes sobre las que se pueda dar una información de menor calidad que pase desapercibida por la abundancia de otra de interés escaso a los efectos que se pretende conseguir.

4.5. Referencias a las sociedades personalistas

El Considerando 15 introduce una interesante —por lo novedosa— referencia a las sociedades personalistas. Se abre aquí una vía hasta ahora apenas explorada en el Derecho de sociedades europeo, que es el de la extensión a las llamadas sociedades mercantiles personalistas de todo el aparato previsto para el resto de las sociedades relativo a la transparencia y acceso transfronterizo a la información, con la finalidad de tutelar los intereses de terceros y aumentar la confianza en las operaciones comerciales con diferentes tipos de sociedades en el mercado único. Se trata de uno de los aspectos que ahora mismo me generan más dudas, pues la falta de tradición al respecto en el marco de la UE indica que el camino a recorrer puede ser aquí más largo. También es cierto que algunas sentencias muy importantes del TJUE han tenido por objeto sociedades de distinta índole algunas de ellas precisamente de ese estilo (por ejemplo, el

caso *Cartesios)*. Se abre en este punto una vía interesante, tanto si se avanza en ella ahora como en caso de una mayor lentitud. Es también un buen ejemplo de que las miras se amplían en ese sentido el hecho de que el acuerdo al que nos hemos referido antes entre Consejo y Parlamento Europeo incluye la posibilidad de una revisión futura para incluir a las cooperativas en la Directiva sobre el Derecho de sociedades.

4.6. Número de empleados

Es sobradamente conocido que el número de empleados de una sociedad es información importante para terceros, pues es uno de los indicadores que nos dan una idea acerca de la dimensión de la sociedad y todo lo que ello comporta. En este caso, y en una aplicación interesante de la conexión entre diversas normas, se dice que los Estados miembros podrán utilizar esta información ya existente sobre el número medio de empleados y ponerla a disposición del público de forma gratuita a través del sistema de interconexión de registros. Se trata de una información que debe ser incluida por las sociedades en los estados financieros de conformidad con la Directiva 2013/34 y en el futuro esos datos se extraerán de allí para ponerlos a disposición de los interesados

4.7. Información sobre grupos

Los considerandos 18 a 21 tienen una interesante referencia a los grupos de sociedades, que tradicionalmente han sido (y siguen siendo) una materia complicada de abordar por parte del legislador. Se trata de uno de los aspectos que ahora mismo me suscita una mayor curiosidad en cuanto a su desarrollo futuro. Es cierto que no se dice nada que pueda ser discutido, pues la previsión sobre la cuestión me parece muy sensata. Pero en el estado actual de la Propuesta veo que algunas de las definiciones del texto articulado son susceptibles de mejora. En todo caso, el punto de partida es que la información sobre los grupos societarios es de notable importancia para promover la transparencia y aumentar la confianza en el entorno empresarial, pero también lo es para contribuir a la detección eficaz de prácticas fraudulentas o abusivas que desde luego son perjudiciales para el mercado en general. En ese contexto, es oportuno poner a disposición de los interesados información sobre las estructuras de los grupos, en una medida que no solamente debe afectar a los grupos transfronterizos sino también a los de ámbito estrictamente doméstico. Es conocido que los grupos de sociedades pueden tener estructuras relativamente sencillas, pero también que pueden ser complejas. A esos efectos, destaca la exigencia de un retrato, lo que denomina la Propuesta de Directiva un esquema visual de la estructura del grupo, cuya finalidad y efecto sea la de reflejar la cadena de control. De ese modo, se contribuiría a mejorar la comprensión del funcionamiento del grupo, facilitado a través del sistema de interconexión de registros, ofrecería una visión

global del grupo fácil de usar, fácilmente accesible y completa, y favorecería una mejor comprensión del funcionamiento del grupo en su conjunto y en relación con sus miembros de manera individualizada. En este contexto la propia Propuesta de Directiva inicia unos esbozos de regulación futura, pues se señala que ese esquema visual no se exige, pero sí se "anima" (literalmente) a los Estados miembros a que avancen en esa dirección. Se admite que se debe evaluar con un mayor detalle toda la referencia a esta cuestión.

4.8. Información actualizada

Me parece interesante la insistencia en un aspecto que puede parecer menor pero que plantea problemas, y es el de garantizar que la información del registro se mantenga actualizada. En este sentido, hay una remisión expresa a la recomendación 24 del Grupo de Acción Financiera Internacional, titulada «Transparencia y titularidad real de las personas jurídicas», revisada en marzo de 2022, en la que se incluyen diversos requisitos para que la información societaria que consta en los registros mercantiles sea exacta y se mantenga actualizada.

4.9. Certificado de la sociedad de la UE armonizado

Es relevante la previsión relativa a la creación de un certificado armonizado de sociedad de la UE, que desde luego recuerda a otros documentos identificativos que tienen un reconocimiento sencillo desde hace tiempo (pensemos por ejemplo en un permiso de conducir). De ese modo las sociedades podrán demostrar de manera sencilla pero también fiable, pues es doble siempre el objetivo, que están legalmente constituidas en un Estado miembro.

4.10. Poder de representación digital de la UE

En fin, uno de los aspectos que consideramos más interesantes de todas las medidas propuestas es el que se trata en el Considerando 27, que es nada menos que el establecimiento de un poder de representación digital que sea válido para toda la UE, cuya finalidad ahora mismo se concreta en facilitar aún más los procedimientos transfronterizos para las sociedades y simplificar y reducir determinados trámites, como la apostilla o la traducción. Sobre ese poder de representación digital se anuncia que habrá un modelo común europeo multilingüe que las sociedades van a poder utilizar para autorizar a una persona a representarlas en procedimientos específicos que tengan dimensión transfronteriza cuando caigan bajo el ámbito de aplicación de la Directiva.

BIBLIOGRAFÍA

ÁLVAREZ ROYO-VILLANOVA, S. (2021) "Propuesta de adaptación de la directiva de digitalización 2019/1151 a la vista del derecho comparado", Revista Lex Mercatoria, núm 18

BOQUERA MATARREDONA, J. (2021), "La digitalización de las sociedades de capital españolas tras las Directivas europeas sobre la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades", RDM 320

CABANAS TREJO, R. y RIVAS RUÍZ, A., (2024) *La constitución de la sociedad de responsabilidad limitada tras las últimas reformas legales y la reciente doctrina registral: Procedimientos telemáticos y redacción de estatutos*, Barcelona

CABANAS TREJO, R., (2019) *Procedimiento en línea (constitución, registro y presentación de documentos e información), publicidad y registro*, en *Derecho de sociedades europeo,* AAVV (coord. Miquel Rodriguez, J. y Pérez Troya, A.), *Derecho de sociedades europeo*, Madrid, pp. 79 y ss.

EMBID IRUJO, J.M., (2023) "La digitalización del Derecho de Sociedades", en Nieto Carol, U (dir.) *La digitalización en el derecho de sociedades*, Valencia, pp. 17 y ss. y

FERNÁNDEZ DEL POZO, L. (2020) "La publicidad registral de las sucursales tras la publicación de la Directiva (UE) 2019/1151 de herramientas digitales", La Ley Mercantil núm 67

FUENTES NAHARRO, M., (2023) *La digitalización del derecho de sociedades, La Directiva 2019/1151 y su trasposición al Derecho español*, Pamplona 2023, la obra colectiva

GÓRRIZ LÓPEZ, C. (2019), *Derecho originario: principio de libre establecimiento. Derecho secundario: armonización y derecho uniforme*, en AAVV (coord. Miquel Rodríguez, J. y Pérez Troya, A.), *Derecho de sociedades europeo*, Madrid, pp. 27 y ss.

HERNANDO CEBRIA, L. (2022)" Modelos societarios y digitalización en la movilidad transfronteriza intracomunitaria", RdS, núm 65.

MADRID PARRA, A., (2023) "La constitución telemática de sociedades mercantiles: Opciones de política legislativa", en AAVV (coord. MJ Peñas Moyano), *Estudios de Derecho de sociedades y de Derecho concursal: libro en homenaje al profesor Jesús Quijano González,* Valladolid, pp. 459 y ss.

MIQUEL RODRÍGUEZ, J. (2023), La constitución en línea de Sociedades de Responsabilidad Limitada. Transposición de la Directiva 2019/1151 y reforma de la Ley de Sociedades de Capital, en La Ley mercantil, núm. 103

NIETO CAROL, U. (2023), "Constitución en línea de sociedades limitadas", en Nieto Carol, U (dir.) *La digitalización en el derecho de sociedades*, Valencia, pp. 73 y ss.

II. Empresa y ubicación territorial

El principio del estado de origen entre la directiva de comercio electrónico, el reglamento general de protección de datos y el reglamento de servicios digitales

Miguel Gardeñes Santiago
Profesor Titular de Derecho internacional privado
Universitat Autònoma de Barcelona

ABSTRACT:
The so-called "country of origin principle", enshrined in article 3 of the E-commerce Directive, approved in 2000, has been a powerful tool for the integration of the information society services market in the EU. However, its multifaceted or multipurpose nature has led to some problems when interpreting it or applying it. The aim of this paper is to explain the reasons for such problems and to propose solutions for overcoming them. At the same time, this paper analyses if the country of origin principle has a role to play in two Regulations particularly important for the digital market of the EU: the General Data Protection Regulation and the Digital Services Act.

Keywords: mutual recognition. Country of Origin Principle. E-commerce Directive. General Data Protection Regulation (GDPA). Digital Services Act (DSA).

Palabras clave: reconocimiento mutuo. Principio del Estado de origen. Directiva de comercio electrónico. Reglamento General de Protección de Datos (RGPD). Reglamento de Servicios Digitales (RSD).

SUMARIO:

1. INTRODUCCIÓN Y OBJETO DEL TRABAJO.

Ya hace casi veinticinco años que se aprobó la Directiva 2000/31, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, y en particular del comercio electrónico en el mercado interior (en adelante, DCE)[1], que constituyó en aquel momento un texto legal de suma importancia para la adaptación del Derecho de la Unión Europea (en adelante, UE) al entorno digital. A pesar del tiempo transcurrido desde entonces, de la rápida evolución tecnológica y del importante desarrollo legislativo para tener en cuenta dicha evolución, la DCE sigue siendo una pieza maestra del sistema. Una de sus aportaciones más destacables, y que fue objeto de no pocas discusiones en el momento en que se gestó el texto, fue la introducción en su artículo 3, bajo el título de "mercado interior", del principio del Estado de origen, en cuya virtud se atribuía la responsabilidad reguladora y supervisora de los prestadores de los servicios de la sociedad de la información al Estado miembro

1. DOCE L 178, de 17-7-2000; incorporada en España mediante la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante, LSSI).

de la UE en el que estuvieran establecidos. Ya en aquel momento, se suscitaron dudas de cuál debiera ser el alcance del mencionado principio del país de origen. Tras más de dos décadas, existe ya un considerable acervo jurisprudencial al respecto, que ha resuelto algunas de las cuestiones que se planteaban, pero, en mi opinión, también ha dado lugar a interpretaciones problemáticas que debieran ser revisadas.

El objeto de este trabajo será, por una parte, analizar cómo ha evolucionado la interpretación del principio del Estado de origen previsto en la DCE en los últimos veinticinco años; por otra parte, y habida cuenta del tiempo transcurrido, analizaremos cómo y en qué medida el principio del Estado de origen se ha incorporado a otros textos de Derecho derivado de la UE reguladores del entorno digital. A este respecto, y por su singular trascendencia, he seleccionado dos: el Reglamento 2016/679, de 27 de abril de 2016, de protección de datos de carácter personal (en adelante, RGPD)[2] y el Reglamento 2022/2065, de 19 de octubre de 2022, de servicios digitales (en adelante, RSD)[3]. Ambos se diferencian de la DCE en un importante aspecto: mientras que esta última era un texto claramente pensado para el comercio de servicios de la sociedad de la información en el mercado interior europeo[4], los citados Reglamentos disponen una regulación europea con una clara vocación de aplicarse también a sujetos establecidos en Estado terceros, en la medida en que se den los criterios de vinculación con la UE que los propios Reglamentos prevén[5]. Sin embargo, aquí no me ocuparé de este aspecto *ad extra*, sino de la dimensión *ad intra*, relativa al comercio de servicios dentro del mercado interior europeo, es decir, en el contexto del comercio transfronterizo de servicios entre Estados miembros de la UE. En dicho contexto, resulta oportuno analizar si el principio de control por el Estado de origen desempeña algún papel, y cuáles serían sus límites.

2. ALGUNAS PRECISIONES CONCEPTUALES PREVIAS

Antes de adentrarnos en el tema objeto de estudio, resulta conveniente hacer alguna precisión previa. Frecuentemente se habla de la "regla del país de origen" en un sentido muy amplio, que incluiría también la regla de reconocimiento mutuo derivada de las normas del TFUE relativas a las libertades de circulación

2. DOUE L 119, de 4-5-2016.

3. DOUE L 277, de 27-10-2022.

4. Véase, en este sentido, el considerando 58 de la DCE, que establece que la Directiva no se aplicará a los servicios procedentes de prestadores establecidos en Estados terceros.

5. En este sentido, comparando la DCE y el RSD, Goñi Urriza, N. (2023), *La libre circulación de servicios en la Unión Europea: El régimen de la libertad de establecimiento y la libre prestación de servicios y su aplicación por los tribunales españoles*. Bosch (p. 183). En cuanto al ámbito de aplicación territorial del RGPD, De Miguel Asensio, P. (2022). *Derecho privado de Internet*. Thomson Reuters (6ª ed.) (pp. 410-418).

en el mercado interior[6]. En mi opinión, sin embargo, es preciso distinguir dicha regla del principio del Estado de origen. La regla de reconocimiento mutuo deriva de la jurisprudencia del TJUE en el contexto de la aplicación de las normas del Tratado relativas a las libertades de circulación, primero en el ámbito del comercio de mercancías[7], y más tarde, sobre todo a partir de principios de los años noventa del siglo pasado, también en el resto de libertades, y muy especialmente la de prestación de servicios[8]. Tal como ya tuve ocasión de exponer con mayor detenimiento en otro lugar[9], en virtud del reconocimiento mutuo el Estado miembro de importación o destino de los productos o servicios no estaría realmente obligado a "aplicar" la normativa del Estado miembro de origen, sino simplemente a tomarla en consideración, para valorar si alcanza o no un resultado equivalente al de la normativa del Estado de destino en cuanto al nivel de protección de determinados intereses públicos, como por ejemplo la salvaguarda de la seguridad pública o de los intereses de los consumidores. Por tanto, el reconocimiento mutuo supone aplicar el principio tradicional según el cual los productos o servicios deben adaptarse a las reglas del Estado de destino (*host country rule*), aunque se trataría de una aplicación flexible o matizada, porque, al aplicar sus propias normas, la autoridad del Estado de destino debiera evaluar si los objetivos que estas persiguen se alcanzan o no mediante la aplicación al productor o prestador de otro Estado miembro del régimen jurídico vigente en su Estado de origen. Con ello se evitaría la doble o múltiple regulación injustificada.

En cuanto al principio del Estado de origen, ciertamente participa de la misma finalidad de evitar la carga que para el comercio transfronterizo supone la doble regulación injustificada, y de hecho se inspira en la doctrina del reconocimiento mutuo, que de este modo sería su antecedente. Sin embargo, en mi opinión, existiría una importante diferencia: su aplicación no derivaría de las disposiciones del Tratado relativas a las libertades de circulación, sino de los actos de Derecho derivado en los que el legislador de la Unión lo hubiera incorporado. Es decir, la diferencia fundamental estaría en que no sería una regla de interpretación aplicable con carácter general en el marco del Derecho primario relativo a la libre circulación, sino un principio de regulación que el legislador de la UE puede utilizar, o no, en determinados actos de Derecho derivado,

6. Entre otros, Thomale C. y Weller, M.-P. (2017). Country of origin rule. Basedow. J et al. (ed.). *Encyclopaedia of Private International Law*. Elgar (pp. 479-483).

7. Inaugurada con el célebre asunto *Cassis de Dijon*, de 20-2-1979 (as. C-120/78, ECLI:EU:C:1979:42).

8. Sobre el "transplante" de la jurisprudencia *Cassis de Dijon* al sector de los servicios, véase, entre otros, Mattera, A. (1991). Les principes de proportionnalité et de reconnaissance mutuelle en matière de libre circulation de personnes et des services: de l'arrêt Thieffry aux arrêts Vlassoupoulou, Mediawet et Dennemayer. *Revue du Marché Unique Européen,* núm. 4 (pp. 191-203).

9. Gardeñes Santiago, M. (2019). El reconocimiento mutuo en la Unión Europea: su naturaleza jurídica a la luz de las técnicas o métodos del Derecho internacional privado. Agudo González, J. (dir.). *Relaciones jurídicas transnacionales y reconocimiento mutuo*. Aranzadi (pp. 138-148).

modulando en cada caso su alcance y efectos[10]. De ello se desprende que pueden existir diferencias en la plasmación del principio del Estado de origen en cada acto legislativo concreto, en función del alcance que el legislador haya querido otorgarle. Ahora bien, tales diferencias no impedirían que pudiera detectarse un fundamento común: se trata de un principio basado en la idea de "centralizar" el estatuto jurídico del operador económico en su Estado de establecimiento, con la finalidad de evitarle la carga de la doble o múltiple regulación. Pero, como señalaba, partiendo de esta idea básica, el principio del Estado de origen puede adoptar diversas modalidades, según lo que prevea el legislador en cada caso: puede dar lugar a una norma para determinar el régimen jurídico aplicable al operador económico, o a una determinada faceta de su actividad, o a una norma que prevea el reconocimiento de resoluciones administrativas (por ejemplo, las que condicionan el acceso a una determinada actividad regulada), o bien puede utilizarse como criterio para atribuir competencia preferente a la autoridad administrativa de un Estado. No se trataría, por tanto, de un tipo concreto de "regla", sino de un principio de regulación encaminado a facilitar la circulación y el comercio transnacionales, cuyo uso, entonces, depende de una decisión política. Veamos, pues, como se ha plasmado en la DCE.

3. NATURALEZA JURÍDICA DEL PRINCIPIO DEL ESTADO DE ORIGEN EN LA DCE

3.1. Elementos en tensión de un modelo indeterminado: los artículos 3 y 1.4

El artículo 3 ("mercado interior") establece en su apartado 1 que "todo Estado miembro velará por que los servicios de la sociedad de la información facilitados por un prestador de servicios establecido en su territorio respeten las disposiciones nacionales aplicables en dicho Estado miembro que formen parte del ámbito coordinado." Correlativamente, el apartado 2 del mismo artículo impide a los Estados miembros "restringir la libertad de prestación de servicios de la sociedad de la información de otro Estado miembro por razones inherentes al ámbito coordinado." Como puede observarse, la citada disposición efectuaría una remisión al Estado de establecimiento del prestador del servicio[11], en cuya

10. Desde una perspectiva más general, se deprende claramente de la jurisprudencia del TJUE la diferente situación que pueda darse, en el ámbito gobernado por las libertades de circulación del mercado interior, dependiendo de si resultan o no aplicables normas armonizadas de Derecho derivado; por ejemplo, en la sentencia de 30-5-2024 (as. C-662/22 y C-667/22, ECLI:EU:C:2024:432) afirmó que "mediante un acto de Derecho derivado, el legislador de la Unión puede concretar una libertad fundamental recogida en el Tratado FUE creando condiciones aún más favorables para el correcto funcionamiento del mercado interior que las resultantes del Derecho primario…" (ap. 67).

11. Para determinar el lugar de "establecimiento", véanse los criterios del considerando 19; véase también el art. 2 de la LSSI.

virtud este quedaría sometido a la regulación del mismo y, al mismo tiempo, dispensado de cumplir con la regulación de los demás Estados miembros a los que dirigiera su actividad. Tal remisión al Estado miembro de establecimiento (*home country rule*) tendría la apariencia de una norma de conflicto de leyes, aunque de un carácter *sui generis*, dado su amplísimo ámbito de aplicación material. Ello puede verse, por ejemplo, en la transposición española: así, cuando el artículo 2 de la LSSI establece, en su apartado 1, que dicha ley (en su totalidad) será de aplicación a los prestadores de servicios establecidos en España y a los servicios prestados por los mismos, añadiéndose en el apartado 4 que tales prestadores "estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen…". Desde luego, esta remisión en bloque al "ordenamiento jurídico español" contrasta con las soluciones especializadas propias de las normas de conflicto de leyes en cuanto a la determinación de su ámbito de aplicación material, que suele delimitarse cuidadosamente, en función de las distintas instituciones o categorías jurídicas concernidas[12]. Desde esta perspectiva, podría decirse que mientras que las normas de conflicto de leyes utilizan una técnica "de pincel", el principio del Estado de origen utilizaría una "de brocha gorda"[13].

---

12. En este sentido, Hellner, M (2004) ha destacado, a propósito del art. 3 de la DCE, que una norma de conflicto de leyes genérica que remitiera a la ley del Estado de origen supondría un retroceso con respecto a las normas de conflicto de leyes vigentes en los Estados miembros, que han evolucionado en el sentido de una mayor especialización para adaptarse a las especificidades de la distintas instituciones, teniendo en cuenta los intereses en presencia y la seguridad jurídica (The Country of Origin Principle in the E-commerce Directive: A Conflict with Conflict of Laws? Fuchs, A., Muir Watt, H. y Pataut, E. (dirs). *Les conflits de lois et le système juridique communautaire*. Dalloz (pp. 223-224).

13. Ahora bien, y al margen de la problemática específica de la DCE, nada impide que el legislador de la UE pueda optar por incluir normas de conflicto de leyes de carácter especializado inspiradas en el principio del Estado de origen en determinados actos del Derecho de la Unión. A este respecto, disponemos de ejemplos interesantes en el ámbito de la propiedad intelectual. El primero de ellos sería el de la Directiva 93/83, de 27-9-1993, sobre derechos de autor y afines en el sector de la radiodifusión vía satélite y de la distribución por cable, de cuyo art. 1, apartados 1 y 2, complementados por los considerandos 14, 15 y 18, se desprende que los derechos de radiodifusión se rigen por la ley del Estado donde se produjera la "comunicación al público vía satélite", y que se reputa que dicho país será aquel en que se inicien las señales portadoras del programa. Otro ejemplo sería el de la Directiva 2019/789, de 17-4-2019, relativa al ejercicio de los derechos de autor y afines aplicables a determinadas transmisiones en línea de los organismos de radiodifusión y a las retransmisiones de programas de radio y televisión, cuyo art. 3 (complementado por el considerando 9) establece el principio del "país de origen" en lo que se refiere a los servicios accesorios en línea, puesto que, a los efectos del ejercicio de los derechos de autor y afines, considera que el acto de comunicación al público se localiza únicamente en el Estado miembro en el que el organismo de radiodifusión tenga su establecimiento principal; sobre estas Directivas, Ballesta Martí, L. (2023). *The Communication to the Public of Musical Works Online in the European Union's Legislation: Striving for a Fair Balance*. Tesis doctoral, Universitat Autònoma de Barcelona (pp. 83, 86-87). Tanto en uno como en otro texto se percibe claramente que la intención del legislador es evitar la aplicación simultánea de varias leyes a un mismo acto de comunicación, por lo que "centraliza" su régimen legal mediante la "localización jurídica" del mismo en el Estado de origen. Ahora bien, cabe destacar una importante diferencia: mientras que la Directiva 93/83 considera que el Estado de origen es el de inicio de la señal, la Directiva 2019/789

Por ello, el impacto que la referencia al país de origen contenida en el artículo 3 pudiera tener en las normas de conflicto de leyes, particularmente en materia de obligaciones contractuales y extracontractuales, suscitó bastante preocupación y controversia, y por ello se incluyó el artículo 1.4 en la DCE, a cuyo tenor: "La presente Directiva no establece normas adicionales de Derecho internacional privado ni afecta a la jurisdicción de los tribunales de justicia." Se alcanzaba así una solución de compromiso, que en apariencia preservaba las normas de Derecho internacional privado, pero que en realidad abocaba a un modelo abierto o indeterminado.

3.2. Su determinación judicial: la jurisprudencia eDate

Cuando el legislador configura un modelo abierto, ello supone dejar en manos del juzgador la concreción o determinación del mismo. Y el TJUE recogió ese guante. Su resolución básica al respecto es la sentencia *eDate Adverstising*, de 25 de octubre de 2011[14]. Versaba sobre dos asuntos acumulados en los que sujetos residentes en Estados miembros (Alemania y Francia respectivamente) plantearon demandas por intromisión en los derechos de la personalidad contra editores de contenidos en páginas de Internet establecidos en otros Estados miembros (Austria y, en aquel momento, también el Reino Unido). Las cuestiones prejudiciales se referían a la competencia judicial (sobre la base del artículo 5.3 del Reglamento 44/2001, equivalente el actual 7.2 del Reglamento 1215/2012) y, por lo que aquí interesa, en el terreno del Derecho aplicable al fondo, a la incidencia del artículo 3 de la DCE en la determinación de dicho Derecho. En concreto, el Tribunal Supremo alemán preguntó si la norma del artículo 3 tiene el carácter de norma de conflicto de leyes (es de suponer que de carácter bilateral) aplicable a las materias de Derecho civil, o si únicamente supone un correctivo al Derecho que resulte aplicable según las normas de conflicto de leyes, para modificar su tenor con arreglo a las exigencias del país de origen. En apretada síntesis, el TJUE resolvió la tensión entre los artículos 3 y 1.4 de la DCE con una fórmula de compromiso: por un lado, admite claramente que la referencia al Estado de origen contenida en el artículo 3 incluye también las cuestiones de Derecho civil; sin embargo, y por otro lado, sostiene que el hecho de que se produzca semejante referencia no determina necesariamente su calificación como norma de conflicto de leyes, y de ello deduce que los Estados miembros no estarían obligados a transponer la citada disposición en forma de norma de conflicto de leyes (debe entenderse que se está refiriendo a norma de conflicto de leyes de carácter bilateral). Ahora bien, y ello es de suma importancia, afirma que lo dispuesto en el precitado artículo 3, apartados 1 y 2, "debe interpretarse

opta, creo que con mejor criterio, por una localización más significativa desde el punto de vista económico, como es la del establecimiento principal de la entidad radiodifusora.

14. Asuntos acumulados C-509/09 y C-161/10. ECLI:EU:C:2011:685.

de modo que se garantice que el enfoque de coordinación seguido por el legislador de la Unión permita efectivamente asegurar la libre circulación de los servicios de la sociedad de la información entre los Estados miembros[15]". De ello deduciría que, en el ámbito coordinado, los Estados miembros debieran garantizar que, dejando a salvo las excepciones previstas por la Directiva, el prestador del servicio no quedara sujeto a requisitos más estrictos que los que previera la ley de su Estado de establecimiento[16].

La solución alcanzada por el TJUE se alinearía aparentemente con determinadas construcciones doctrinales en clave de "correctivo material" que, supuestamente, permitirían conciliar la tensión —por no decir contradicción— entre los citados artículos 3 y 1.4[17]. Según estos planteamientos, las normas de conflicto de leyes se aplicarían con normalidad y, solo si el Derecho nacional que resultara aplicable según ellas fuera más restrictivo que el del Estado de origen del prestador, entonces intervendría el principio de país de origen para "corregir" el resultado alcanzado por la norma de conflicto, en favor del régimen menos oneroso para el prestador del servicio[18]. Semejante construcción resulta contradictoria, puesto si se reconoce que el artículo 3 de la DCE tiene una función de "coordinación" entre sistemas legales, entonces está claro que es una norma de Derecho internacional privado. Es más, el argumento de que el principio del Estado de origen constituiría únicamente un "correctivo" al Derecho material aplicable según la norma de conflicto de leyes sería un argumento falaz, por una sencilla razón: la regla del artículo 3 de la DCE no es una regla de carácter material que se "superponga" a otras, sino que es una norma que define el ámbito de aplicación territorial de determinadas normas materiales, las del Estado de origen del prestador. Por ello, en vez de una interpretación en clave de "correctivo material", en mi opinión resulta más ajustada una interpretación en clave conflictual o de coordinación de sistemas, como la que propuso Basedow en los años 90 del siglo XX a propósito del reconocimiento mutuo. Como se recordará, el maestro alemán se refería al "contenido normativo-conflictual" de la referencia

15. Apartado 64.

16. Apartado 68; sobre la doctrina establecida en el caso *eDate*, Forner Delaygua, J.J. (2013), "Ley aplicable y ley respetable". Forner Delaygua et al. *Entre Bruselas y La Haya. Estudios sobre la unificación internacional y regional del Derecho internacional privado. Liber amicorum Alegría Borrás*, Marcial Pons (pp. 417-427); De Miguel Asensio (2022, cit., pp. 206-207); El Hage, Y. (2022). *Le droit international privé à l'épreuve de l'Internet*. L.G.D.J. (pp. 308-314).

17. Para una excelente síntesis de las críticas formuladas a la jurisprudencia *eDate*, particularmente por la doctrina francesa y belga, en el sentido de atribuirle un carácter artificioso, la voluntad de establecer un sistema "dual y escondido" de reglas de conflicto, o por sus supuestas dificultades de manejo, derivadas de la necesidad de tener que comparar el contenido de dos ordenamientos, véase El Hage, Y. (2022, cit., pp. 311-314).

18. A decir verdad, este planteamiento no era nuevo. Una formulación muy clara del mismo puede encontrarse en la obra de Tebbens, cuando afirmó que el reconocimiento mutuo derivado de las libertades de circulación no actuaría *en amont* (es decir, en el nivel de las normas de conflicto de leyes), sino *en aval* (en el nivel del Derecho material designado por tales normas de conflicto de leyes); Tebbens, H.D. (1994) Les conflits de lois en matière de publicité déloyale à l'épreuve du droit communautaire. *Revue critique de droit international privé* (p. 480).

al Estado de origen que, a su juicio, sería el siguiente: el supuesto de hecho de la norma sería la comercialización de productos o servicios, el punto de conexión sería el país de origen de los mismos y la consecuencia jurídica sería la aplicación de una de las dos leyes —la del Estado de origen o la del Estado destino de los productos o servicios—, en función de cuál de ellas fuera más favorable al operador económico. Sería, por tanto, un criterio de designación del Derecho aplicable basado en el principio de favorecer la actividad del empresario que operara en el mercado interior (principio al que llamó "*favor offerentis*")[19]. Entiendo que, de hecho, la interpretación del artículo 3 de la DCE que hoy deriva de la jurisprudencia *eDate*, reiterada en casos posteriores[20], encajaría bastante bien en este planteamiento[21].

Por último, cabe añadir que una posible explicación de la aparentemente alambicada solución del caso *eDate* es que el TJUE se vio obligado a hacer de "equilibrista"[22] para sortear la contradicción inherente a los arts. 3 y 1.4 de la DCE. Ahora bien, también podría haber otra explicación: se trata de disposiciones de una Directiva, que necesitan de un acto de transposición en los Derechos nacionales, a diferencia de lo que ocurre con los Reglamentos. Por tanto, tiene sentido que el TJUE no quisiera adoptar una posición excesivamente restrictiva

19. Basedow, J. (1995). Der kollisionrechtliche Gehalt der Produktfreiheiten im europäischen Binnenmarkt. *Rabels Z.* (pp. 1-55).

20. Así, por ejemplo, en la sentencia *A contra Daniel B y otros*, de 1-10-2020 (as. C-49/18, ECLI:EU:C:2020:764), se trataba de una farmacia holandesa que dirigía publicidad a potenciales clientes residentes en Francia, y que fue objeto de una acción por daños derivados de actos de competencia desleal, ejercitada por competidores franceses. Según el Reglamento 864/2007, sobre la ley aplicable a las obligaciones extracontractuales, el Derecho aplicable en este caso sería el francés, dado que el artículo 6 del citado Reglamento establece que, para los daños derivados de actos de competencia desleal, la ley aplicable será la del mercado afectado. A pesar de ello, el TJUE admite que el prestador pueda valerse de la ley de su Estado de establecimiento, a no ser que el Estado de destino de los servicios pueda invocar alguna de las excepciones que prevé la DCE.

21. A este respecto, en su brillante análisis de la doctrina sentada en la jurisprudencia *eDate*, afirma el profesor Forner que el TJUE configura claramente la referencia al Estado de origen como una referencia a sus normas de Derecho material, que por tanto no incluiría sus normas de conflicto de leyes. De este modo decretaría *de facto* una "unificación conflictual" que el propio legislador no pudo alcanzar cuando adoptó el Reglamento 864/2007, sobre ley aplicable a las obligaciones extracontractuales, puesto que su art. 1.2.g) excluye de su ámbito de aplicación las obligaciones extracontractuales derivadas de vulneraciones del derecho a la intimidad y demás derechos de la personalidad, que era precisamente el tipo de responsabilidad de la que se trataba en este caso. En virtud de la regla establecida por el TJUE, el prestador quedaría sujeto a la ley aplicable según la norma de conflicto, únicamente en la medida en que no fuera más restrictiva que la ley de su Estado de establecimiento. En consecuencia, de entre las dos leyes, el prestador quedaría sujeto a aquella cuyo régimen material le fuera más favorable. Por ello, distingue, creo intuir que con una cierta dosis de humor, entre la "ley aplicable", que sería la determinada en cada caso por la norma de conflicto de leyes, y la "ley respetable", que se impondría a la primera siempre que su resultado material fuera más favorable al prestador. En su opinión, y particularmente en el área de las vulneraciones de los derechos de la personalidad, semejante mecanismo daría lugar a un resultado injusto, puesto que la determinación de la ley aplicable acaba dependiendo de un factor que se encuentra únicamente bajo el control del prestador; Forner Delaygua, J.J. (2013, cit., p. 422).

22. Expresión que tomo prestada de Yves Le Hage (2022, cit., p. 312).

del margen de decisión que corresponde a los Estados miembros al adoptar las normas de transposición. Es decir, lo único que exigiría la Directiva es que, en los textos estatales de transposición, la función de coordinación de sistemas legales que desempeña el artículo 3 de la DCE quede garantizada, sin predeterminar la técnica normativa concreta que cada Estado considere más apropiada. Por consiguiente, no se les forzaría a incorporar el texto en su ordenamiento mediante una norma de conflicto "savignyiana" o de carácter bilateral. Podrían hacerlo mediante normas de conflicto de carácter unilateral, tal como habría hecho el legislador español en la LSSI[23]. Ahora bien, que el artículo 3 de la DCE no obligue a los Estados miembros a incorporarlo a sus ordenamientos mediante una norma de conflicto bilateral no significa que les impida que lo hagan, si lo consideran oportuno, tal como habría hecho el legislador francés[24].

4. CONDICIONANTES DE LA APLICACIÓN DEL PRINCIPIO DEL ESTADO DE ORIGEN EN LA DCE

Como ha podido observarse, la referencia al Estado de origen del artículo 3 DCE puede resultar problemática por su amplísimo alcance. Por ello, no es extraño que el legislador europeo intentara acotar, con la máxima precisión posible, el ámbito de aplicación de dicha referencia y sus excepciones. Los analizaremos en los párrafos que siguen.

4.1. Los "servicios de la sociedad de la información"

Hay que tener en cuenta que la DCE, aunque adoptada en el contexto más general de la libre prestación de servicios en la UE, constituye una *lex specialis* que se aplica únicamente a los llamados "servicios de la sociedad de la información"[25] (en adelante, SSI). La definición general de este concepto hoy se encuentra en el artículo 1.1 de la Directiva 2015/1535, de 9 de septiembre de

23. A este respecto, y con mayor detenimiento, mi trabajo anteriormente citado (2019, pp. 151-154).

24. La Ley 2004-575, de 21 de junio de 2004, incorpora en el artículo 17, primer párrafo, una norma que claramente responde al patrón de una norma de conflicto bilateral. Su texto es el siguiente: "*L'activité définie à l'article 14 est soumise à la loi de l'Etat membre sur le territoire duquel la personne qui l'exerce est établie, sous réserve de la commune intention de cette personne et de celle à qui sont destinés les biens ou services*."; sobre la transposición francesa, El Hage (2022, cit., pp. 314-318). A este respecto, señalaba Forner Delaygua, J.J. que, puestos a transponer el art. 3 de la DCE en la forma de una norma de conflicto de leyes bilateral para la relaciones intracomunitarias o *ad intra*, los Estados miembros tendrían la opción de establecer una norma que remitiera unívocamente a la ley del Estado de establecimiento del prestador, o bien adoptar una que dijera que el prestador de servicios pudiera invocar la ley de dicho Estado siempre que le fuera más favorable (2013, cit., p. 426).

25. Expresión que, debo confesarlo, siempre me ha parecido algo pomposa.

2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas sobre servicios de la sociedad de la información, a cuyo tenor constituye un SSI "todo servicio normalmente prestado a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios."

Para la concreción de esta figura puede recurrirse, además de a las aclaraciones del considerando 18 de la DCE, a la ya abundante jurisprudencia sobre el tema: a título de ejemplo, serían SSI los servicios de un periódico que ofrezca información en línea[26], los servicios de publicidad en línea[27], los servicios de alojamiento de datos[28], los servicios de intermediación, mediante una plataforma electrónica, entre arrendatarios y arrendadores, profesionales o no profesionales, que propongan servicios de alojamiento de corta duración y que, además, ofrezcan prestaciones accesorias a dicho servicio de intermediación[29], los servicios de acceso a Internet o a una red de comunicación[30], los servicios de venta en línea de medicamentos no sujetos a prescripción médica[31], o los servicios de intermediación, mediante una aplicación para móviles, entre taxistas y clientes[32].

En la práctica, los supuestos que han planteado mayores problemas de delimitación son los de los servicios de puesta en contacto o intermediación relacionados con servicios que no se prestan por vía electrónica, como sería el caso de los de transporte. A este respecto, es bien conocido el supuesto de la sentencia *Asociación Profesional Élite Taxi*, de 20 de diciembre de 2017[33], en la que, a propósito de los servicios prestados por Uber en España, consistentes en una aplicación para móviles que permitía, a cambio de una remuneración, conectar a conductores no profesionales que utilizaban su propio vehículo con personas que deseaban realizar desplazamientos urbanos, el TJUE afirmó que, por las modalidades concretas de organización del servicio considerado, no se trataba de un SSI, sino de un servicio de transporte, y ello porque el servicio prestado por Uber estaba indisociablemente vinculado a un servicio de transporte. En cambio, en el antes citado asunto *Airbnb Ireland*, de 19 de diciembre de 2019, consideró que, tal como estaba organizado, el servicio de intermediación entre arrendadores y arrendatarios que prestaba *Airbnb* era suficientemente autónomo o distinguible de los servicios de arrendamiento subyacentes. Se trata, por tanto, de una aproximación casuística, en función de las características del concreto servicio que ofrezca cada prestador. A este respecto, los asuntos *Star Taxi*, ya

26. STJUE Papasavvas, de 11-9-2014, as. C-291/13, ECLI:EU:C:2014:2209.
27. STJUE *Vanderborght*, de 4-5-2017, as. C-339/15, ECLI:EU:C :2017:335.
28. STJUE *Eva Glawishnig-Piesczek c. Facebook Ireland*, de 3-10-2019, as. C-18/18, ECLI:EU:C:2019:821.
29. STJUE *Airbnb Ireland*, de 19-12-2019, as. C-390/18, ECLI:EU:C:1112.
30. STJUE *La Quadrature du Net,* de 6-10-2020, as. C-511/18 y otros, ECLI:EU:C:2020 :791.
31. La ya citada STJUE *A contra Daniel B y otros*, de 2020.
32. STJUE *Star Taxi App,* de 3-12-2020, as. C-62/19, ECLI:EU:C:2020:980.
33. As. C-434/15, ECLI:EU:C:2017:981.

citado y *Doctipharma*, de 29 de febrero de 2024[34], también han aportado precisiones útiles: cuando se trate de servicios que tengan por objeto poner en contacto a clientes y a prestadores de servicios de "diferente naturaleza" (como podría ser, por ejemplo, el transporte de personas), el servicio de puesta en contacto solo podrá considerarse un SSI si el servicio ofrecido es realmente distinto del referido servicio "de diferente naturaleza". En cambio, si el servicio de puesta en contacto formara "parte integrante" de un servicio global cuyo elemento principal fuera una actividad o servicio distinto de un SSI, en tal caso tal intermediación no podría considerarse un SSI[35]. El criterio decisivo sería, pues, que el servicio de puesta en contacto fuera distinto o distinguible del servicio "intermediado". Para valorarlo, pueden tenerse en cuenta diversos aspectos, y en particular el de la existencia o no de control por parte del prestador del servicio electrónico sobre el servicio "material" subyacente. En el caso de *Uber*, por ejemplo, se consideró que dicha empresa ejercía una influencia decisiva sobre las condiciones de prestación del transporte, incluyendo la determinación del precio máximo de la carrera. En cambio, en el caso *Airbnb*, se consideró que el prestador no ejercía un control comparable sobre las condiciones de los arrendamientos y, por tanto, el servicio de intermediación que prestaba era un SSI, al poder diferenciarse del arrendamiento[36].

4.2. Necesidad de establecimiento en la UE del prestador del servicio

Al ser la DCE una norma dictada con el objeto de facilitar la libre prestación de los servicios que contempla en el mercado interior, siendo entonces una norma de desarrollo de la libertad contemplada en el artículo 56 del TFUE, es del todo lógico que su aplicabilidad se circunscriba a los prestadores establecidos en los Estados miembros, y que por tanto queden excluidos los establecidos en Estados terceros, tal como recuerda el considerando 58 de la DCE. Es más, tal como se ha señalado acertadamente[37], a los SSI regulados en la DCE hoy podría aplicárseles también la Directiva 2006/123, de 12 de diciembre de 2006, de servicios en el mercado interior, aunque en virtud del artículo 3.1 de la segunda, en caso de conflicto prevalecerían las disposiciones de la norma especial, en este caso la DCE.

34. As. C-606/21, ECLI:EU:C:2024:179.

35. Al respecto, ap. 35 de la última sentencia citada. En el caso concreto, consideró que era un SSI un servicio de puesta en contacto, mediante un sitio de Internet, de clientes y farmacéuticos suscritos a dicho servicio de intermediación, que permitía que los farmacéuticos vendieran, desde sus propios sitios de Internet, medicamentos no sujetos a receta médica.

36. A este respecto, conclusiones del Abogado General M. Szpunar en el asunto *Airbnb*, presentadas el 30-4-2019, ap. 18-91.

37. Goñi Urriza, N. (2023, cit., p. 117).

Por su parte, la jurisprudencia tampoco ha tenido dudas al respecto. Por ejemplo, en la sentencia *Viagogo AG*, de 27 de abril de 2023[38], se suscitó la cuestión de si un prestador de SSI establecido en Suiza podía ampararse en la DCE para dirigir su actividad a Estados miembros de la UE, a lo que el TJUE dio una respuesta negativa[39]. Obviamente, ello no significa que un prestador establecido en un Estado tercero no pueda dirigir sus servicios a clientes situados en Estados miembros de la UE, lo que significa es que, en lo relativo al ejercicio de dicha actividad, deberá cumplir la normativa del Estado miembro de destino de los servicios, sin poder valerse del principio del Estado de origen y, por tanto, de las normas aplicables en su Estado de establecimiento. Cabe añadir que, tal como precisó el TJUE en la sentencia *de Visser*, de 15 de marzo de 2012, el artículo 3, apartados 1 y 2, tampoco se aplicará en el supuesto de prestadores cuyo lugar de establecimiento sea desconocido, puesto que la aplicación del citado precepto se supedita a la identificación del Estado miembro en cuyo territorio esté efectivamente establecido el prestador de SSI[40].

4.3. Las exclusiones del ámbito de la DCE

Desde el punto de vista de su ámbito de aplicación material, la aplicación del principio del Estado de origen en el comercio de servicios en el mercado interior sufre importantes limitaciones. Las primeras se refieren a las cuestiones excluidas expresamente del ámbito de aplicación material de la DCE, y que se indican en su artículo 1.5. En primer lugar, se excluye lo relativo a la fiscalidad. La DCE, por tanto, no afectaría al régimen del IVA aplicable a los servicios. Pero, evidentemente, las normas sobre el IVA no serían las únicas normas tributarias afectadas por la exclusión. Así, por ejemplo, en la sentencia *Airbnb Ireland y Airbnb Payments UK*, de 22 de diciembre de 2022, el Tribunal recuerda que la exclusión "en materia de fiscalidad" es amplia e incluiría todos los aspectos relativos a la misma. En el caso concreto, se trataba de la normativa italiana que obligaba al intermediario a recoger y comunicar a la Administración tributaria nacional los datos de los arrendamientos celebrados mediante su intermediación, así como, en caso de que hubiera intervenido también en el cobro de la renta, la obligación de retener una parte de la cantidad pagada por el arrendatario e ingresarla a la Administración[41]. En segundo lugar, se excluyen las cuestiones referidas a la protección de datos de carácter personal y a la confidencialidad de las comunicaciones, cuestiones que se regirían por su normativa específica[42]. En tercer lugar, la DCE no se aplica a los acuerdos o prácticas

38. As. C-70/22, ECLI:EU:C:2023:350.
39. Apartados 29 a 31 de la sentencia.
40. As. C-292/10, ECLI:EU:C:2012:142, ap. 69-72.
41. As. C-83/21, ECLI:EU:C:2022:1018, ap. 25.
42. Así lo recordó el TJUE en el precitado asunto *La Quadrature du Net*, de 2020, y que la DCE no se aplicaría a tales cuestiones.

contemplados por las normas del Derecho de la competencia, lo que obviamente significa que los criterios de aplicación territorial de las normas *antitrust* para nada se ven afectados por la DCE. Por último, también se excluyen las actividades de los notarios o figuras equivalentes, en la medida en que su actividad implique una conexión directa y específica con el ejercicio de la autoridad pública, la representación y defensa de clientes ante los tribunales, y las actividades de juego que impliquen apuestas de valor monetario.

4.4. La delimitación del "ámbito coordinado" por la Directiva

La delimitación del "ámbito coordinado" es un elemento de capital importancia para conocer el alcance del principio del Estado de origen, puesto que el artículo 3.1 de la DCE establece claramente que se aplica únicamente dentro de los confines de dicho ámbito coordinado. Pero tales confines son muy amplios, a tenor de la delimitación que lleva a cabo el artículo 2.h): para empezar, se incluyen tanto los requisitos aplicables a "los prestadores" como a los "servicios", tanto si se trata de normas específicamente aplicables a los prestadores de SSI y a los propios SSI, como si se trata de normas "de tipo general", lo que supondría una remisión en bloque al conjunto de normas, del tipo que sean, a las que esté sometido el prestador en su Estado de establecimiento. Tanto se incluyen los requisitos relativos al "inicio de la actividad" como a su "ejercicio"; entre estos últimos, se incluyen los relativos al "comportamiento" del prestador, los que se refieran a la "calidad o el contenido" del servicio, incluidos los aplicables a la publicidad y a los contratos, así como las exigencias en materia de responsabilidad del prestador. Se trata sin duda de un vastísimo ámbito de aplicación material, que incluiría importantes aspectos del régimen de Derecho privado aplicable al prestador (como demostraría por ejemplo la ya citada sentencia *Papasavvas*, de 11 de septiembre de 2014, en la que el TJUE confirmó, siguiendo el camino trazado por la jurisprudencia *eDate*, que un régimen de responsabilidad civil por difamación se incluiría en el ámbito coordinado), pero que también incluiría los aspectos de Derecho público, como se desprende claramente de la sentencia *Google Ireland*, de 9 de noviembre de 2023[43]. Ello nos devuelve al problema ya mencionado anteriormente[44], que es el del carácter extraordinariamente amplio del supuesto de hecho de la referencia al Estado de origen derivada del artículo 3.1 de la DCE, amplitud que supera con mucho la que hoy día es habitual en las normas de conflicto de leyes, normalmente mucho más especializadas. Como se verá más adelante, ello puede favorecer que se produzcan errores o excesos en la interpretación del mecanismo previsto en el citado artículo 3. Cabe señalar también que esta extraordinaria amplitud del "ámbito coor-

43. As C-376/22, ECLI:EU:C:2023:835, dictada a propósito de un contencioso administrativo del que era parte la autoridad administrativa de supervisión austríaca.

44. *Supra*, apartado 3.1.

dinado" explica que alcance a muchas cuestiones que no son objeto de armonización por la DCE[45], y por tanto las materias cuya aplicación la Directiva "coordina" superan con mucho a las que armoniza.

Por último, cabe añadir que quedan excluidos del ámbito coordinado los requisitos aplicables a las mercancías en sí, a la entrega de las mismas y a los servicios no prestados por medios electrónicos. La evidente lógica de esta exclusión es la de dejar fuera del ámbito coordinado las exigencias relativas a los productos o a los servicios que deban prestarse fuera de la red[46]. Así, por ejemplo, el hecho de que una mercancía haya sido ofrecida o publicitada a través de Internet, o el hecho de que el vendedor o el fabricante ofrecieran servicios adicionales por Internet (asesoramiento, servicios post venta…) para nada impediría que la mercancía en cuestión tuviera que cumplir las reglamentaciones técnicas (armonizadas a nivel de la UE o nacionales) que en cada caso le resultaran aplicables. Ahora bien, cabe plantearse si determinados requisitos de información obligatoria en el contexto del comercio en línea de mercancías podrían enjuiciarse en el marco del art. 34 TFUE. La pregunta no es ociosa, porque es bien sabido que en ocasiones el TJUE ha enjuiciado reglamentaciones nacionales sobre formas de publicidad, técnicas de venta o requisitos aplicables al comercio minorista bajo la óptica del artículo 34 del TFUE[47]. En cambio, tras la aprobación de la ya citada Directiva 2006/123, sobre servicios en el mercado interior, el TJUE ha encontrado un nuevo punto de apoyo, que le ha permitido considerar la venta minorista de mercancías como un "servicio"[48].

A la vista de estas fluctuaciones jurisprudenciales, no cabe excluir que determinados aspectos de las ventas en línea puedan enjuiciarse, en unas ocasiones a partir de las normas sobre servicios, y en particular la DCE, y en otras desde la perspectiva de la libre circulación de mercancías, o incluso de ambas conjuntamente[49]. En la jurisprudencia reciente hay algún precedente que avalaría este parecer. En efecto, en la sentencia *Booky.fi Oy*, de 23 de marzo de 2023[50], se analizó la compatibilidad con el Derecho de la UE de la normativa finlandesa

45. En este sentido, De Miguel Asensio, P. A. (2023). *Manual de Derecho de las nuevas tecnologías*. Aranzadi (p. 59).

46. *Ibid*. (p. 59).

47. De hecho, los supuestos "excesos" que a este respecto el TJUE habría cometido en el pasado condujeron a la rectificación jurisprudencial que supuso la sentencia *Keck*, de 24 de noviembre de 1993 (as. C-267/91 y C-268/91, ECLI:EU:C:1993:905).

48. Por ejemplo, así lo hizo en la sentencia de 30-1-2018 (as. C-360/15 y C-31/16), ECLI:EU:C:2018:44). Este viraje del ámbito de las mercancías hacia el de los servicios probablemente le haya sido útil al TFUE para desembarazarse indirectamente de la doctrina establecida en la precitada sentencia *Keck*, que, aunque no ha sido abiertamente desautorizada, ha sido gradualmente relegada por el TJUE.

49. Ciertamente, cabe recordar que, aunque no sea lo más habitual, en ocasiones el TJUE ha analizado determinadas disposiciones de los Derechos nacionales a la luz de más de una de las libertades de circulación (véase, por ejemplo, la sentencia *Austria c. Alemania*, de 18-6-2019, as. C-591/17. ECLI:EU:C:2019:504).

50. As. C-662/21, ECLI:EU:C:2023:239.

sobre programas audiovisuales a la luz del artículo 34 del TFUE, en el caso de un comerciante que vendía los citados programas grabados en soportes físicos como DVD y Blu-ray, a través de una tienda *on line*, y al que se le reprochaba no haber cumplido la normativa finlandesa sobre clasificación y etiquetado de grabaciones audiovisuales por razones de protección de los menores. A este respecto, debe recordarse que, tratándose de la distribución comercial de música o películas, la posición tradicional del TJUE ha sido que si las grabaciones musicales o cinematográficas se incorporan a un soporte físico, como por ejemplo los discos, en tal caso se aplican las normas del TFUE sobre mercancías; en cambio, si tales grabaciones se difunden por medios como la radio o la televisión, la actividad entraría en el ámbito de las normas sobre servicios. Volviendo al caso *Booky.fi*, resulta evidente que la obligación de indicar en el producto la clasificación por edades correspondiente sería una norma técnica relativa al mismo, y por ello excluida del ámbito coordinado por la DCE. Ahora bien, también cabría deducir de esta sentencia que el TJUE habría enjuiciado determinadas obligaciones relativas a la información que el vendedor debía facilitar en línea, antes de la compra, desde la perspectiva de las normas sobre mercancías en vez de las relativas a los servicios. En concreto, la ley finlandesa exigía que la indicación de la edad aconsejada debía facilitarse, junto con la información del producto, en el mismo momento en que el soporte se pusiera a la venta en línea[51], y el TJUE admite que dicha medida podría justificarse por razones de protección de menores, y que no sería desproporcionado exigir que tal información estuviera disponible antes de efectuarse la compra, para que el comprador pudiera determinar, con conocimiento de causa, si el contenido del programa resulta adecuado para los menores de los que fuera responsable[52]. Es evidente, por tanto, que en el contexto de las ventas de una tienda en línea, tal información previa a la compra solo puede ofrecerse a través de la página de Internet de la tienda en cuestión, y que el TJUE evaluó la necesidad y proporcionalidad de la medida a la luz del art. 34 TFUE, y no a la de las normas de la DCE. Por ello, no cabe excluir que, con respecto a normas de este tipo, pueda darse una cierta superposición parcial de las reglas relativas a distintas libertades de circulación.

4.5. Cuestiones excluidas de la aplicación del principio del Estado de origen

Existen determinadas materias que se incluyen en el "ámbito coordinado" que define la DCE a las que, a pesar de ello, no se les aplica el principio del Estado de origen, puesto que así lo indica expresamente el artículo 3.3 de la DCE, que remite a la lista contenida en su anexo. A título de ejemplo, y sin

51. Ap. 29.
52. Véase, especialmente, el ap. 61.

ánimo de exhaustividad, en la lista de materias a las que no se aplica el principio del Estado de origen se incluyen los derechos de propiedad intelectual e industrial[53], la licitud de las comunicaciones comerciales no solicitadas por correo electrónico, la libertad de elección de la ley aplicable al contrato, las obligaciones relativas a contratos con consumidores, o la validez formal de los contratos por los que se creen o transfieran derechos en materia de propiedad inmobiliaria, si dichos contratos están sometidos a requisitos formales obligatorios en virtud de la ley del Estado de situación del inmueble.

Por tanto, en los ámbitos indicados, las normas de Derecho internacional privado operarán sin estar sujetas al "correctivo" del principio de origen, lo que en muchas ocasiones conducirá a que se aplique el principio contrario, esto es, el del "Estado de destino" (*host country rule*). Por ejemplo, esto ocurriría claramente con respecto a los contratos con consumidores, en el que el principio es el de la aplicación de la ley del Estado de residencia habitual del consumidor, siempre que el empresario hubiera dirigido su actividad comercial a dicho Estado[54]. Es más, tal y como aclara el considerando 56 de la DCE, la excepción de los contratos con consumidores incluye "la información sobre elementos esenciales del contenido del contrato, incluidos les derechos del consumidor, que tengan una influencia determinante sobre la decisión de celebrarlo." Análogamente, la excepción relativa a los derechos de autor y afines también estaría orientada a preservar la aplicación de la ley del Estado de destino de los servicios, esta vez en virtud de la aplicación del principio de protección territorial propio de la propiedad intelectual[55]. En cambio, la aclaración de que la DCE para nada afecta al derecho de las partes a elegir la ley aplicable a su contrato obedecería a una lógica distinta, de la que se desprendería la presunción de que la aplicación de un régimen legal acordado por las partes difícilmente supondrá un obstáculo al comercio, más bien al contrario, tenderá a facilitarlo.

4.6. La posible incidencia de otras normas limitadoras de los SSI

Para finalizar este apartado correspondiente a los condicionantes de la aplicación del principio del Estado de origen en el contexto de los SSI, resulta oportuno referirse a otra posibilidad, que es que determinados SSI —que entren en el ámbito coordinado por la DCE y que tampoco se vean afectados por la

53. Aunque debe recordarse que, como se ha señalado anteriormente (*supra*, nota 13), existen disposiciones de la UE que regulan determinadas modalidades de los derechos de autor y afines que se basan precisamente en el principio del Estado de origen.

54. Art. 6 del Reglamento 593/2008, de 17 de junio de 2008, relativo a la ley aplicable a las obligaciones contractuales; considerando 55 de la DCE.

55. No hay que olvidar, sin embargo, que determinados textos del Derecho de la UE relativos a los derechos de autor y afines abrazan el principio del país de origen con respecto a ciertos actos de comunicación al público de las obras protegidas (*supra*, nota 13).

exclusión del ámbito de aplicación del principio del país de origen establecida en el artículo 3.3—, a pesar de ello puedan verse limitados por otras disposiciones del Derecho de la UE. Contamos con un excelente ejemplo de ello en la reciente y ya citada sentencia *Doctipharma*, de 2024. Como se recordará, se trataba de un servicio de puesta en contacto, a través de Internet, de farmacéuticos y clientes, para la venta de medicamentos no sujetos a receta médica. El TJUE no tuvo inconveniente en reconocer el carácter de SSI de tal servicio, contemplado por tanto por la DCE, que en principio podría beneficiarse de la aplicación del principio del país de origen. Ahora bien, tratándose de la comercialización de medicamentos, es obvio que debía tenerse en cuenta también la normativa específica sobre dichos productos, para comprobar si establecía límites adicionales a tales SSI; en este caso, se trataría de la Directiva 2001/83, de 6 de noviembre de 2001, por la que se adoptó un código comunitario para medicamentos de uso humano. Pues bien, el artículo 85 *quater* de dicha Directiva establece que, sin perjuicio de la legislación nacional que prohíba la oferta al público mediante SSI de medicamentos sujetos a receta médica, los Estados miembros velarán para que los medicamentos puedan ofrecerse por venta a distancia mediante SSI, siempre que se cumplan determinadas condiciones. En particular, los Estados miembros pueden determinar las personas físicas o jurídicas autorizadas a realizar tales ventas. En uso de esta habilitación, la ley francesa establecía que solo podrían llevarlas a cabo quienes tuvieran la condición de farmacéutico. En consecuencia, considera el TJUE que el legislador francés solo podría prohibir la actividad de servicio de puesta en contacto entre clientes y farmacéuticos para la venta de medicamentos no sujetos a receta médica si la plataforma o intermediario en cuestión, que no ostentara la condición de farmacéutico, interviniera en la venta de tales medicamentos. En cambio, no podría prohibirla si el servicio se limitara a la pura puesta en contacto con los farmacéuticos, siendo estos quienes vendieran los medicamentos a través de sus propias páginas de Internet.

5. LA APLICACIÓN DEL PRINCIPIO DEL ESTADO DE ORIGEN

5.1. El marco normativo del artículo 3 de la DCE y la función del Estado miembro de destino de los servicios

En los apartados anteriores hemos visto que corresponde al Estado de origen o establecimiento del prestador de los SSI la responsabilidad de regularlos (art. 3, ap. 1). Es más, la remisión al Estado de origen contenida en dicha disposición no se referiría únicamente al Derecho o "ley" aplicable, como es habitual en las nomas de conflicto de leyes, sino también a los actos de aplicación por sus autoridades, particularmente en el ámbito administrativo. Ello explicaría la laxitud y diversidad terminológica que envuelve al principio del país de origen, como por ejemplo cuando no referimos a él como principio de "control" por el país de origen (*home country control*), poniendo así el acento más en la actividad

supervisora que en la propia ley o norma jurídica[56]. Ello permitiría distinguir el principio del Estado de origen de las normas de conflicto en el ámbito del Derecho internacional privado o, dicho de otro modo, poner de relieve la versatilidad o polivalencia del principio del Estado de origen: en contextos de Derecho privado, como los que hemos examinado (reclamaciones de responsabilidad civil derivadas de daños al honor y a los derechos de la personalidad, acciones por competencia desleal…), dicho principio podría funcionar como una norma de conflicto de leyes; en cambio, en otros contextos, y particularmente en los regulados por el Derecho público, su funcionamiento sería distinto: en múltiples ocasiones el elemento clave no sería tanto la "ley" del Estado de origen como las actuaciones de sus autoridades administrativas[57].

Por lo que se refiere al rol del Estado de destino de los SSI, se vería limitado de manera importante: como se recordará, el apartado 2 del artículo 3 de la DCE dice que los Estados miembros "no podrán restringir" la libertad de prestación de SSI procedentes de otro Estado miembro por razones inherentes al ámbito coordinado. Sin embargo, el apartado 4 del mismo artículo permite hacer excepciones al apartado 2 con respecto a "un determinado servicio", bajo dos tipos de condiciones[58]: las primeras (letra a) serían de carácter sustantivo o de fondo, y exigirían que la medida estuviera justificada por razones de orden público (incluyendo la protección de menores y el respeto de la dignidad humana), la salud pública, la seguridad pública o la protección de los consumidores (incluyendo los inversores). Las segundas (letra b) hacen referencia a obligaciones de carácter procedimental, en los siguientes términos: antes de adoptar medidas restrictivas frente a un determinado SSI procedente de otro Estado miembro, el Estado de destino deberá pedir al Estado de establecimiento del prestador que tome las medidas necesarias. Si el Estado de establecimiento no hubiera tomado tales medidas, o las que hubiera tomado resultaran insuficientes, en tal caso el Estado de destino podría tomar medidas, tras haber informado de su intención de adoptarlas al Estado de establecimiento del prestador y a la Comisión. Únicamente en

---

56. Se ha puesto de relieve, por ello, en referencia al reconocimiento mutuo, que se parecería más al "método de referencia al ordenamiento jurídico competente" que al método conflictual clásico; Picone, P. (2004). Diritto internazionale privato comunitario e pluralità dei metodi di coordinamento tra ordenamenti. Picone, P. (ed.). *Diritto internazionale privato e diritto comunitario*. Cedam (pp. 485-525).

57. En España resultan de gran interés a este respecto los trabajos del administrativista Jorge Agudo González. Dicho autor basa su planteamiento en la existencia de diversas "variantes" del reconocimiento mutuo. La referencia al Estado de origen supondría un "reenvío" al "ordenamiento jurídico" de origen, que permitiría, bien el reconocimiento de la regulación de otro Estado miembro, bien de los actos dictados al amparo de la misma. Es decir, se trataría de admitir en el territorio del Estado de acogida o de destino los efectos generados por un ordenamiento extranjero, generalmente materializados en un "acto de aplicación" en el caso concreto; Agudo González, J. (2019). La articulación de las relaciones jurídicas transnacionales mediante las variantes del reconocimiento mutuo. Agudo González, J. (dir.). *Relaciones jurídicas transnacionales y reconocimiento mutuo*. Aranzadi (esp. pp. 233-235, 264-274 y 289-297).

58. Sobre el art. 3.4, entre otros, Goñi Urriza, N. (2023, cit., pp. 197-200).

caso de urgencia, se permite al Estado de destino prescindir de las obligaciones de comunicación establecidas en la letra b), aunque entonces deberán notificarse a la Comisión y al Estado miembro de establecimiento las medidas adoptadas, indicando los motivos de la urgencia (art. 3.5 de la DCE). En cualquier caso, la Comisión examinará las medidas notificadas o adoptadas por el Estado de destino del SSI, y si considera que son incompatibles con el Derecho de la UE, solicitará a dicho Estado que no las adopte o que las retire, según los casos (art. 3, ap. 6 de la DCE).

En definitiva, la competencia del Estado receptor o de destino de los SSI tendría un carácter subsidiario, en el sentido de que solo podría adoptar medidas restrictivas, en virtud del artículo 3.4, si el Estado de origen o establecimiento del prestador, cuya competencia sería preferente, no lo hubiera hecho satisfactoriamente, debiendo cumplir además las obligaciones de notificación recién explicadas. Ello conduce a matizar alguna afirmación, a mi juicio excesiva, de la jurisprudencia. Así, en la antes citada sentencia *Google Ireland*, de 9 de noviembre de 2023, el TJUE dijo que el Estado de destino de los SSI no puede adoptar "medidas de carácter general y abstracto referidas a una categoría de servicios de la sociedad de la información descrita genéricamente[59]." Como se ha destacado acertadamente, semejante afirmación debe entenderse en el sentido, no de que no pueda adoptar tales disposiciones, sino que no puede aplicarlas a SSI procedentes de otros Estados miembros[60]. Por mi parte, creo que habría que añadir algo más: también podría aplicarlas a un prestador de SSI establecido en otro Estado miembro, pero únicamente a título subsidiario, si el Estado de origen no hubiera cumplido con su función supervisora, y con pleno respeto de las obligaciones de notificación del artículo 3.4.b). Otro claro ejemplo de los límites que se imponen al Estado miembro de destino de los SSI lo encontramos en tres recientísimas sentencias, todas ellas de 30 de mayo de 2024[61]. Versaban sobre las obligaciones de carácter administrativo que imponía la legislación italiana a los proveedores de servicios de intermediación en línea que prestaran sus servicios en Italia, aunque estuvieran establecidos en otros Estados miembros. En concreto, se les obligaba a inscribirse en un registro administrativo en Italia, a facilitar periódicamente a la autoridad de supervisión italiana información detallada sobre la organización de la empresa proveedora, y a abonarle una contribución económica para sufragar los gastos de la actividad supervisora. Retomando la doctrina establecida en el caso *Google Ireland*, el TJUE dictamina que el intento de aplicar dichas obligaciones a prestadores establecidos en otros Esta-

59. Ap. 34, véase también el ap. 47.

60. En este sentido, Feliu Álvarez de Sotomayor, S. (2024). Ámbito territorial y aplicación del principio de control en origen en el Reglamento (UE) de servicios digitales. Castelló Pastor, J.J. (dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*. Aranzadi (p. 62).

61. Se trata de los asuntos *Airbnb Ireland UC* y *Amazon Services Europe Sarl* (as. C-662/22 y C-677/22, ECLI:EU:C:2024:432), *Google Ireland* y *Eg Vacation Rentals Ireland* (as. C-664/22 y C-666/22, ECLI:EU:C:2024:434) y *Amazon Services Europe* (as. C-665/22, ECLI:EU:C:2024:435).

dos miembros resultaría contrario al artículo 3.1 de la DCE y, en las circunstancias de los casos concretos, las restricciones impuestas no podrían ampararse en la excepción del artículo 3.4 de la DCE[62].

5.2. Las obligaciones de procedimiento y la muy discutible aportación de la jurisprudencia Airbnb de 2019

Las obligaciones de información y comunicación establecidas en la letra b) del artículo 3.4 del Reglamento, que acaban de examinarse, estarían pensadas para los supuestos de aplicación de la DCE por autoridades administrativas, engrosando así una legión de textos europeos relativos al mercado interior que establecen mecanismos de cooperación administrativa entre las autoridades de los Estados miembros. No parecen pensadas, en cambio, para un contexto de aplicación judicial, y ello se deduciría de la propia letra b) cuando establece las obligaciones de notificación, aunque "sin perjuicio de los procesos judiciales, incluidas las actuaciones preliminares y los actos realizados en el marco de una investigación criminal". Esta exclusión sería del todo lógica, y también muy habitual en los textos de Derecho secundario de la UE relativos al mercado interior, por la sencilla razón de que los principios en que se basa la cooperación administrativa no pueden extrapolarse sin más al ámbito de la asistencia y cooperación entre autoridades judiciales de diferentes países que conozcan de controversias de carácter civil o penal, cooperación que como es bien sabido se rige por su normativa específica. No creo que la alusión, en los considerandos 25 y 26, a que las medidas restrictivas deban tomarse de conformidad con las condiciones establecidas en la DCE pueda interpretarse en sentido contrario[63]. Las "condiciones" a las que aluden ambos considerandos no pueden ser otras que las de carácter sustantivo, basadas por tanto en los motivos de interés general que puedan justificar una restricción, pero en cambio no creo que se refieran a los requisitos procedimentales del artículo 3.4.b), puesto que, como ya he indicado, dicha disposición se cuida de especificar que se aplicará "sin perjuicio de los procesos judiciales", con la evidente intención de no interferir en los mismos ni entorpecer su tramitación.

62. Véase el comentario de estas sentencias de De Miguel Asensio, P.A. (2024). Criterio de origen de la Directiva sobre comercio electrónico y límites a las medidas de aplicación del Reglamento (UE) 2019/1150 sobre servicios de intermediación en línea. Blog de Pedro De Miguel Asensio (post de 30-5-2024), accesible en: https://pedrodemiguelasensio.blogspot.com/2024/05/criterio-de-origen-de-la-directiva.html

63. Complementariamente, el considerando 26 reconoce el derecho de los Estados miembros a aplicar sus normas de Derecho penal y enjuiciamiento criminal, sin que sea necesario notificarlas a la Comisión; por su parte, el considerando 25 establece que los tribunales nacionales que conozcan de controversias de Derecho privado pueden adoptar medidas restrictivas de los SSI, de conformidad con las condiciones establecidas en la DCE.

Dicho esto, y a pesar de ello, la ya citada sentencia *Airbnb*, de 19 de diciembre de 2019, ha llegado, a mi juicio, a resultados sorprendentes. Como se recordará, se trataba de una acción penal en Francia, con ejercicio accesorio de la acción civil, contra la filial irlandesa de *Airbnb*, por supuestamente haber ejercido en Francia funciones de agente inmobiliario sin poseer la tarjeta profesional correspondiente. Desde luego, existían dudas razonables de hasta qué punto la actividad de *Airbnb* desde su establecimiento en Irlanda debía verse afectada por la ley francesa de 1970 sobre actividades de intermediación inmobiliaria (conocida como "Ley Hoguet"), pero ello no justifica las discutibles afirmaciones de la sentencia. Concretamente, el Tribunal traza una analogía entre el procedimiento de notificación del artículo 3.4.b), segundo guión, de la DCE con el que establece la Directiva 2015/1535, que prevé un procedimiento de información de proyectos de reglamentaciones técnicas relativas a los productos y de reglas sobre los SSI. De dicha analogía deduce que, con respecto al procedimiento previsto en la DCE, cabe aplicar la doctrina que, a propósito de lo que hoy es la Directiva 2015/1535, el TJUE inauguró con la sentencia *Cia Security*, de 30 de abril de 1996[64]. Como es sabido, en esta última sentencia el Tribunal de Luxemburgo afirmó que el incumplimiento por parte de un Estado miembro de la obligación, establecida por la Directiva 2015/1535 (entonces Directiva 83/189), de comunicar a la Comisión un proyecto de reglamento técnico antes de su adopción definitiva, comportaba que la reglamentación así adoptada no pudiera aplicarse a terceros. Entonces, en virtud de dicha analogía, considera que el incumplimiento por parte del Estado de destino del SSI de la obligación de notificación previa prevista en el artículo 3.4.b), segundo guión, de la DCE debe comportar la misma consecuencia, a saber, "la imposibilidad de invocar la normativa de que se trate contra los particulares"[65]. Entiendo, sin embargo, y a pesar de los argumentos expuestos en la sentencia, que semejante analogía es improcedente, puesto que los supuestos contemplados en ambas Directivas son fundamentalmente distintos: la Directiva 2015/1535 se refiere a proyectos de reglamentaciones técnicas, es decir, a proyectos de normas de carácter general, potencialmente aplicables a una pluralidad de destinatarios. En cambio, la obligación de notificación prevista en el artículo 3.4.b), segundo guión, de la DCE se refiere a una medida restrictiva específica frente a un "determinado servicio de la sociedad de la información", es decir, se trata de un acto de aplicación de carácter individual, frente a un destinatario concreto.

Pero, incluso si se admitiera la pretendida analogía entre ambos textos, no deja de ser sorprendente que se le reprochara al Estado francés no haber notificado la "Ley Hoguet" de 1970, aprobada treinta años antes de la DCE. El TJUE lo justifica con el argumento de que en dicha Directiva el legislador no previó una excepción que autorizara a los Estados miembros a mantener medidas an-

64. As. C-194/94, EU:C:1996:172.

65. Apartados 88 y 96 de la sentencia *Airbnb*.

teriores contrarias a sus disposiciones[66]. Ciertamente, estaría de acuerdo en que, con carácter general, los Estados miembros están obligados a adaptar su ordenamiento jurídico a los textos de Derecho derivado que vayan aprobándose, a no ser que el propio legislador de la Unión admita excepciones mediante las correspondientes disposiciones transitorias. Pero una cosa es esto y otra muy distinta considerar que una disposición específica que establezca obligaciones nuevas de procedimiento —como es el art. 3.4.c), segundo guión, de la DCE— deba producir efectos retroactivos. Admitir algo así podría producir resultados francamente sorprendentes. Como es obvio que el legislador francés, por muy preclaro que fuera, difícilmente habría podido imaginar en 1970 que treinta años más tarde estaría obligado a notificar la Ley Hoguet a la Comisión, ¿qué debiera hacer? ¿Tal vez debiera notificar la totalidad de su ordenamiento jurídico anterior a la Directiva a la Comisión, por si acaso pudiera tener algún efecto restrictivo de los SSI?[67] ¿Todos los Estados miembros debieran hacer lo mismo? Intuyo un trabajo digno de Hércules para los servicios de la Comisión…

Pero no terminan aquí los problemas. Incluso si se admitiera todo lo anterior, sería posible evitar una interferencia indebida en los procedimientos judiciales gracias a la ya mencionada reserva contenida en el artículo 3.4, que parece exentarlos del cumplimiento de lo previsto en el tan repetido segundo guión del artículo 3.4.b). Pues no es esta la manera de ver las cosas del TJUE, que se ocupa muy brevemente de la aplicabilidad o no de la disposición citada a los procesos judiciales en los cuatro últimos apartados de la sentencia. Para empezar, llama la atención que omita cualquier mención a la trascendencia que pudiera tener en este contexto el inciso "sin perjuicio de los procesos judiciales". En vez de ello, afirma que la inoponibilidad de la medida no notificada se puede invocar no solo con ocasión de un proceso penal, sino también en un litigio entre particulares[68]. Ello le conduce a concluir que, en el marco de un proceso penal con ejercicio accesorio de la acción civil, en el que dicha parte civil solicite la reparación del daño supuestamente causado por la infracción, el incumplimiento de la obligación de notificación establecida en el artículo 3.4.b), segundo guión, comportaría que la "medida nacional" que estableciera esa infracción no pudiera

66. Ap. 87.

67. A este respecto, no está de más recordar que la "Ley Hoguet" no era una norma relativa a los SSI, servicios que no existían en aquel momento, sino una norma de carácter general que regulaba las condiciones de ejercicio de ciertas actividades relativas a determinadas operaciones sobre inmuebles y fondos de comercio.

68. Ap. 97. Cabe preguntarse si realmente hacía falta que hiciera esta última afirmación, habida cuenta de que el caso que motivó la cuestión prejudicial era el de un procedimiento penal. Parece que la razón que lo explica es que, tal como dice el Abogado General M. Szpunar en sus conclusiones de 30-4-2019, en sus observaciones escritas el Gobierno francés alegó, con carácter subsidiario de segundo grado, que un procedimiento penal iniciado por denuncia de un supuesto perjudicado que se personara como parte civil en el marco del proceso penal debiera considerarse un procedimiento entre particulares. Con ello pretendía justificar que la Directiva 2000/31 no sería aplicable al caso, y que por tanto la cuestión prejudicial planteada por el juez nacional tendría un carácter puramente hipotético (nota núm. 41).

oponerse al particular contra el que se siguiera el procedimiento penal, ni en lo que se refiere a la responsabilidad penal, ni tampoco a la responsabilidad civil derivada del delito[69]. Al margen de la mayor o menor justificación de que en el caso concreto se eximiera a *Airbnb* de tener que cumplir la "Ley Hoguet", lo cierto es que la doctrina establecida por el TJUE es, a mi juicio, claramente insatisfactoria, y podría entorpecer la buena marcha de los procedimientos judiciales. Para empezar, y como decía anteriormente, no resulta adecuado intentar aplicar mecanismos de cooperación administrativa (o de aplicación "cooperativa" de normas europeas entre distintas Administraciones públicas nacionales[70]), al ámbito de la justicia penal o civil, que ya dispone de sus propias normas de asistencia judicial internacional, normas que se rigen por principios distintos. Es más, la doctrina que establece el TJUE en el caso *Airbnb* es de aplicación prácticamente imposible. Supongamos, por ejemplo, que se presentara una acción civil por competencia desleal contra *Airbnb* en Francia. ¿Qué es lo que debiera notificar el juez francés? ¿La "Ley Hoguet"? ¿La demanda? ¿Debiera suspender el procedimiento mientras la autoridad irlandesa y la Comisión tomaran cartas en el asunto? Suponiendo que la autoridad irlandesa (¿cuál?) decidiera tomar medidas, ¿debiera inhibirse del procedimiento el juez francés? O, yendo más allá, ¿debiera el juez francés declararse incompetente y sugerir al demandante que fuera a litigar al Estado en el que el prestador del SSI tuviera su establecimiento? Sinceramente, no creo que fuera la voluntad del TJUE crear, por la puerta de atrás, nuevas normas sobre procedimientos paralelos o sobre competencia de los tribunales en los ámbitos civil y penal, que por otra parte entrarían en contradicción manifiesta con las que hoy contiene el Derecho de la UE, y con la propia jurisprudencia del TJUE en casos coetáneos[71]. Por ello, y en mi opinión, el TJUE debiera revisar la doctrina establecida en el caso *Airbnb* en lo que se refiere a las obligaciones de información establecidas en el artículo 3.4.b), segundo guión, aclarando que debieran aplicarse únicamente en el contexto de las actuaciones administrativas (y, como máximo, por extensión, a la actuación de las jurisdicciones de tipo contencioso administrativo revisoras de la actuación de la Admi-

69. Apartados 98 y 99.

70. A propósito de las distintas variantes del reconocimiento mutuo, Agudo González, J. habla de un modelo regulativo "relacional", que generaría necesariamente "conexiones cooperativas" entre las Administraciones de los Estados miembros (2019, cit., pp. 284-289).

71. Así, por ejemplo, en la antes citada sentencia *Eva Glawisching-Piesczek c. Facebook Ireland Limited*, de 3 de octubre de 2019, el TJUE admitió que una jurisdicción civil austríaca pudiera, sobre la base del art. 15.1 de la DCE, dictar una medida cautelar que obligue a un prestador del servicio de alojamiento de datos establecido en otro Estado miembro a suprimir los datos que almacene y cuyo contenido sea idéntico o esencialmente similar al de una información declarada ilícita con anterioridad, y a obligar a dicho prestador a suprimir los datos en cuestión, o a bloquear el acceso a los mismos, a nivel mundial (ap. 48-53). Por tanto, el TJUE dejó claras dos cosas: primero, la jurisdicción civil austríaca podía dictar una medida cautelar contra un prestador de servicios de alojamiento de datos establecido en Irlanda y, segundo, que la medida no tendría por qué limitarse a la retirada o bloqueo de datos en el Estado en el que radicara la jurisdicción, sino que podría ordenar su retirada o bloqueo a nivel mundial.

nistración). Ya puestos, también podría pensarse en una reforma legislativa del citado precepto que dejara este extremo meridianamente claro.

En los párrafos anteriores hemos podido observar algunos desajustes en la interpretación y aplicación del principio del Estado de origen plasmado en el artículo 3 de la DCE, especialmente por lo que se refiere a las condiciones para adoptar medidas que restrinjan los SSI procedentes de otro Estado miembro. Estos desajustes, sin embargo, creo que en parte pueden explicarse por las dificultades de manejo del principio establecido en el tan citado artículo 3, derivadas de su carácter poliédrico o polivalente: dependiendo del contexto, en ocasiones puede funcionar como una norma de conflicto de leyes; en otras, como norma de atribución de competencia a determinadas Administraciones, o como norma de reconocimiento de determinadas actuaciones administrativas de otro Estado. Por ello, a la hora de interpretarlo y aplicarlo, es preciso atender a la relación jurídica que se plantee en cada caso (de Derecho administrativo, de Derecho penal o de Derecho privado) para determinar la función concreta que la referencia al Estado de origen del artículo 3 DCE deba desempeñar en cada caso. El vasto alcance de dicha referencia, por la gran amplitud del "ámbito coordinado", no nos deja otra opción.

6. EL PRINCIPIO DEL ESTADO DE ORIGEN EN EL RGPD: AUTORIDAD DE CONTROL "PRINCIPAL" Y OTRAS AUTORIDADES

La DCE configura el marco general de los SSI, que convive con otras normas de carácter específico. Resulta de interés, por ello, examinar hasta qué punto el principio del país de origen se ha plasmado en dichas normas, y con qué límites. De entre ellas, y por su importancia, debemos destacar el Reglamento 2016/79, de 27 de abril de 2016, de protección de datos de carácter personal (RGPD). Como se recordará, la protección de datos de carácter personal y la confidencialidad de las comunicaciones son materias excluidas del ámbito de la DCE (art. 1.5.b y considerandos 14 y 15). No les resulta aplicable, por tanto, el principio del Estado de origen plasmado en su artículo 3, aunque obviamente las obligaciones dimanantes de la legislación de la Unión en estas materias son plenamente aplicables a los SSI. En la actualidad, el RGPD proporciona una regulación unitaria y directamente aplicable, al haber sido adoptada mediante Reglamento. Constituye un Derecho común de la Unión en materia de protección de datos, complementado por alguna norma específica, como la Directiva 2002/58, de 12 de junio de 2002, sobre la privacidad y las comunicaciones electrónicas. El RGPD es, por lo demás, un texto extenso y detallado, aun cuando en determinadas cuestiones permita un cierto margen a los legisladores estatales[72].

72. Al respecto, De Miguel Asensio, P.A. (2023, cit., pp. 129-131).

El RGPD no contiene una norma similar al art. 3 DCE, ni tampoco tendría mucha trascendencia, visto el elevado grado, ya no de armonización, sino de unificación de la normativa de los Estados miembros que supone. La plasmación del principio del Estado de origen en el RGPD es distinta, y mucho más acotada, puesto que se limita al ámbito de la actividad de supervisión administrativa por autoridades especializadas, que son las agencias nacionales de protección de datos. Para el control del "tratamiento transfronterizo" (entre Estados de la UE) prevé el mecanismo llamado de "ventanilla única", que significa distinguir entre la autoridad de control "principal" y las demás. El evidente objetivo es el de evitar que, con respecto a un mismo tratamiento de datos, los responsables o encargados pudieran verse sometidos a la competencia concurrente de varias autoridades nacionales. La competencia de control corresponde, en virtud del artículo 56.1 del RGPD, a la autoridad principal, que es la del Estado miembro donde esté el "establecimiento principal" del responsable o encargado del tratamiento de datos (o el establecimiento único, si solo tuviera uno en la Unión)[73]. Las autoridades de control de los demás Estados tendrían una función subsidiaria, complementaria o auxiliar, en los términos que el propio RGPD prevé (artículos 56.2, 56.5, 66). Como es lógico, el funcionamiento de este sistema de supervisión transnacional precisa de un elevado grado de colaboración entre las agencias nacionales de protección de datos, y ello explica que el Reglamento establezca mecanismos de cooperación de autoridades administrativas considerablemente desarrollados (artículos 60 a 62 y 65). Ahora bien, a los responsables o encargados que no dispongan de establecimiento en la UE, pero a pesar de ello estén obligados a cumplir las disposiciones del RGPD, no se les aplicará el sistema de "ventanilla única", con la consecuencia de que potencialmente quedarán sujetos a la competencia concurrente de las autoridades de diferentes Estados miembros[74].

El dispositivo normativo descrito ya ha tenido ocasión de pasar por el banco de pruebas de la jurisprudencia, y a este respecto resulta de particular interés la sentencia *Facebook Ireland Ltd.*, de 15 de junio de 2021[75]. Se trataba de un litigio ente la autoridad belga de protección de datos y tres sociedades del grupo Facebook, la matriz americana, la filial irlandesa y la filial belga. De acuerdo con la ley belga, el presidente de dicha autoridad podía someter a los tribunales cualquier controversia relativa a la normativa de protección de datos. De acuerdo con ello, la autoridad belga planteó, ante la jurisdicción belga, una acción de cesación en la que se pedía el cese del tratamiento, efectuado por la red social Facebook, de datos personales de los internautas en Bélgica, puesto que los estaría recogiendo sin su consentimiento. La jurisdicción belga planteó en su cuestión prejudicial si la autoridad belga tendría o no legitimación activa para

73. Sobre la noción de establecimiento principal, art. 4.16 del RGPD.

74. En general sobre la supervisión administrativa en materia de protección de datos, particularmente en caso de "tratamientos transfronterizos", De Miguel Asensio, P.A. (2023, cit., pp. 163-166).

75. As. C-645/19, ECLI:EU:C:2021:483.

plantear semejante acción. En su prolija sentencia, el TJUE destaca que en los casos de "tratamiento transfronterizo" en el sentido del RGPD, es preciso respetar el mecanismo de "ventanilla única" y las funciones respectivas de la autoridad de control principal y de las demás. Por ello, concluye que una autoridad de control nacional que esté facultada, en virtud del artículo 58.5 del RGPD, a iniciar acciones ante una jurisdicción de su Estado en casos de supuesta infracción del RGPD, podrá ejercer dicha facultad, aun cuando no sea la autoridad de control "principal" (por no tener el responsable o encargado del tratamiento su establecimiento principal en dicho Estado miembro), siempre que se encuentre en alguna de las situaciones en las que el RGPD confiera a una autoridad de control que no sea la principal competencia para adoptar una decisión en la que se declare que el tratamiento controvertido incumple las normas del RGPD[76].

Es decir, desde un punto de vista más general, ello significa que las autoridades o agencias administrativas de control que no sean la principal únicamente podrán actuar en los supuestos y condiciones en que el RGPD delimite su actividad. Uno de los supuestos previstos sería el del llamado "procedimiento de urgencia" que recoge el artículo 66.1 del Reglamento, que permite que, en circunstancias excepcionales, cuando una autoridad de control interesada (que no sea la principal) considere urgente intervenir para proteger los derechos y libertades de los interesados, podrá adoptar inmediatamente medidas provisionales destinadas a producir efectos en su territorio, cuya duración no podrá exceder de tres meses[77].

7. EL PRINCIPIO DEL ESTADO DE ORIGEN EN EL REGLAMENTO DE SERVICIOS DIGITALES

Una novedad legislativa de singular importancia en el ámbito de los SSI ha sido el Reglamento 2022/2065, de servicios digitales, de 19 de octubre de 2022, texto aplicable desde el 17 de febrero de 2024. A diferencia del RGPD, que reguló un ámbito material que había quedado fuera del alcance de la DCE, el RSD viene a regular un ámbito que se incluye en el dominio de la DCE, aunque sea más restringido, al aplicarse no a todos los SSI, sino únicamente a los llamados

76. Sobre todo, ap. 75.

77. A este respecto, en España recientemente se ha dado un caso interesante: en marzo de 2024 se dio a conocer la orden cautelar de cesación de actividad en España adoptada por la Agencia Española de Protección de Datos (AEPD) contra la entidad *Tools for Humanity Corporation*, cuyo establecimiento principal en Europa estaría en Alemania; las razones de dicha medida estarían en que la citada entidad habría llevado a cabo en España actividades de recogida de datos biométricos (escaneo del iris) que habrían afectado a unas 400.000 personas (para más información, véase mi nota en: Gardeñes Santiago, M. (2024). Medida cautelar adoptada en el asunto Worldcoin: la AEPD ordena el cese inmediato de la actividad de recogida de datos biométricos en España. Blog *Derecho y digitalización empresarial* (post de 17-3-2024), accesible en: https://webs.uab.cat/derecho-y-digitalizacion-empresarial/2024/03/17/medida-cautelar-adoptada-en-el-asunto-worldcoin-la-aepd-ordena-el-cese-inmediato-de-la-actividad-de-recogida-de-datos-biometricos-en-espana/

"servicios intermediarios", como serían los servicios de acceso, redes sociales, plataformas en línea o alojamiento de datos[78]; en suma, los SSI más importantes. El RSD supone un esfuerzo de unificación normativa a escala europea de gran trascendencia en cuanto a las obligaciones de los prestadores de tales servicios intermediarios, pero no es mi pretensión analizar detalladamente sus disposiciones[79], sino que me centraré exclusivamente en dos aspectos: su relación con la DCE y el mecanismo de supervisión administrativa que establece.

Por lo que se refiere al primer aspecto, tal como establece su artículo 2.3, el RSD no afecta a la DCE, sino que la complementa en lo que se refiere a un tipo particular de SSI, los servicios intermediarios. Por ello, es lógico que los artículos 12 a 15 de la DCE, que regulaban hasta ahora el régimen de responsabilidad de los prestadores de servicios intermediarios, hayan sido derogados por el RSD y reemplazados por sus disposiciones. Pero, excepción hecha de esta derogación parcial, la DCE permanece incólume. Ahora bien, hay que tener en cuenta que, tal como recuerda el considerando 9 del RSD, dicho Reglamento lleva a cabo una armonización plena de las normas aplicables a los servicios intermediarios, y por tanto los Estados miembros no pueden adoptar normas en la materia objeto de armonización, a menos que el Reglamento lo prevea expresamente. Ante semejante unificación normativa, aunque el principio del Estado de origen del artículo 3 DCE seguiría siendo vigente, perdería relevancia práctica en lo que se refiere a los servicios intermediarios[80]. Sin embargo, ello no impedirá que puedan aplicarse otras disposiciones del Derecho de los Estados miembros, cuando tales disposiciones persigan objetivos de interés público distintos de los que persigue el RSD, tal como recuerda el considerando 9 *in fine*. Entonces, será

78. Sobre la noción de servicios intermediarios, art. 3 g) del RSD; como señala De Miguel Asensio, el criterio principal de distinción entre servicios intermediarios y el resto de SSI radica en que los segundos serían típicamente los proveedores de contenidos que difunden información a través de los servicios intermediarios (2023., cit, p. 59).

79. Sobre el RSD, entre otros, De Miguel Asensio, P.A. (2023, cit. pp. 59-61, 69-103), Goñi Urriza, N. (2023, cit. pp. 182-183), las distintas contribuciones publicadas en la obra colectiva dirigida por Castelló Pastor, J.J (2024). *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*. Aranzadi, y Vilà Costa, B. (2022). The new Digital Markets Act and Services Market Act and its Relevance on EU Legal Harmonization. *Evrigenis Yearbook of International and European Law*, vol. 4 (pp. 209-219), cortesía de la autora. En su interesante trabajo, la profesora Vilà pone de relieve como el RSD, junto con su gemelo, el Reglamento de mercados digitales, suponen una asimilación y adaptación del método legal comunitario de los años ochenta del siglo XX (jurisprudencia *Cassis de Dijon,* nuevo enfoque en materia de reglamentaciones técnicas…) a la realidad de la sociedad digital. Ambos textos formularían nuevos conceptos legales para la realidad digital, para que esta pueda "recibir" las nuevas normas encaminadas a la protección de los derechos fundamentales, la privacidad, la seguridad y la protección de la competencia en el mercado, entre otros objetivos.

80. En este sentido, De Miguel Asensio, P.A., (2023, 2) El criterio de origen en la Directiva sobre el comercio electrónico y su interacción con el Reglamento de servicios digitales. *Blog de Pedro de Miguel Asensio*, post de 10-11-2023, accesible en: https://pedrodemiguelasensio.blogspot.com/2023/11/el-criterio-de-origen-en-la-directiva.html; y también Feliu Álvarez de Sotomayor, S. (2024, cit., pp. 62-63).

dicho ámbito excluido de la acción armonizadora del RSD aquel en el que la referencia al Estado de origen conservará mayor trascendencia. Cabe añadir también que, como precisa el considerando 10 del RSD, dicho Reglamento se aplicará sin perjuicio de otros actos del Derecho de la UE que regulen los SSI en general, que regulen otros aspectos de la prestación de servicios intermediarios, o que complementen las normas del RSD, como sería el caso, por ejemplo, del Reglamento 2019/1150, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea[81].

Por lo que se refiere a los mecanismos de supervisión administrativa[82], son sin duda uno de los aspectos más destacables del RSD. En apretada síntesis, cabe señalar que el Reglamento establece un sistema de autoridades administrativas y de "coordinadores de servicios digitales[83]" para controlar el cumplimiento del Reglamento por los prestadores de servicios intermediarios (art. 49). A este respecto, el dato más destacable es que la autoridad del Estado miembro del establecimiento principal del prestador de servicios intermediarios tendrá una competencia que el artículo 56.1 expresamente declara "exclusiva", y ello marca una importante diferencia con respecto a lo que establece el RGPD en el ámbito de la protección de datos que, como ya se ha visto, reconoce únicamente una competencia "principal"[84]. Asimismo, el RSD establece detallados mecanismos que permiten la colaboración ente las diversas autoridades supervisoras, incluyendo la posibilidad de investigaciones conjuntas (artículos 57 a 60)[85]. Otro aspecto muy destacable de la regulación de la acción supervisora en el RSD es que, en el caso de las plataformas de servicios en línea y motores de búsqueda de muy gran tamaño, confiere una competencia ejecutiva directa a la Comisión Europea (art. 56, apartados 2, 3 y 4), que incluye también la posibilidad de imponer multas (art. 74 y ss.).

---

81. A este respecto, entre otros, Goñi Urriza, N. (2023, cit., p. 193).

82. A este respecto, De Miguel Asensio, P.A. (2023, cit., pp. 100-102).

83. En España la Comisión Nacional de los Mercados y de la Competencia (CNMC) ha sido la autoridad designada como coordinador de servicios digitales.

84. Para la determinación del establecimiento principal, véase el cdo. 123; para los prestadores sin establecimiento en la UE, la autoridad competente sería la del Estado miembro en que resida o esté establecido su representante legal en la UE (art. 56.6); si un prestador establecido en un Estado tercero no designara un representante legal de conformidad con el art. 13 del Reglamento, en tal caso quedaría sujeto a la competencia supervisora de todos los Estados miembros (art. 56.7), lo que sin duda constituiría un incentivo para designar al representante en cuestión.

85. Prevé, por ejemplo, que los interesados puedan presentar reclamaciones ante la autoridad del Estado de su residencia, que las transmitirá al coordinador de servicios digitales del Estado de establecimiento del prestador del servicio (art. 53). También prevé que los coordinadores de los Estados de destino puedan pedirle al de establecimiento del prestador que actúe (art. 58.1). Se crea una Junta Europea de Servicios Digitales, con funciones consultivas, integrada por los coordinadores de los Estados miembros (art. 61).

8. CONSIDERACIONES FINALES

A lo largo de este trabajo se ha destacado el carácter poliédrico o polivalente del principio del Estado de origen cristalizado en el artículo 3 de la DCE. Ello se debe al amplísimo alcance del ámbito coordinado en el que se aplica, que, como muy claramente ha demostrado la jurisprudencia, se proyecta tanto sobre aspectos de Derecho público como de Derecho privado. Este amplio alcance confiere fortaleza al principio del Estado de origen, que se convierte así en un poderoso instrumento de integración del mercado europeo de SSI. Pero, al mismo tiempo, supone una debilidad, por las dificultades técnicas derivadas de tener que aplicar dicho principio en contextos muy distintos. Por ello, se hace necesario distinguir unos de otros y así evitar extrapolaciones inadecuadas entre ellos.

Por lo que se refiere, en primer lugar, a las relaciones de Derecho privado, la referencia al Estado de origen implica claramente una función de coordinación de ordenamientos. Bien es cierto que el TJUE no ha obligado a los Estados miembros a incorporar el artículo 3 de la DCE en la forma de una norma de conflicto bilateral, pero está claro que el mentado artículo 3 tiene una función conflictual, cuya finalidad es asegurar que el prestador de SSI pueda valerse de la ley de su Estado de establecimiento. En este sentido, se ha destacado, a mi juicio acertadamente, que el Derecho de la Unión suministraría el material para un "pedazo" de la norma de conflicto, y que el resto lo proporcionarían, bien las normas estatales, bien el Derecho europeo armonizado. De hecho, declarar que una ley resultará aplicable con el límite derivado de otra es un mecanismo ya conocido, que se integra en el propio funcionamiento de algunas normas de conflicto de leyes[86]. Así ocurriría, por ejemplo, cuando el artículo 6.2 del Reglamento 593/2008, sobre la ley aplicable a las obligaciones contractuales, establece que en los contratos de consumo las partes podrán pactar la ley aplicable, aun cuando dicha elección no podrá impedir que se apliquen las normas no derogables por contrato de la ley que hubiera resultado aplicable a falta de elección (la del Estado de residencia del consumidor)[87]. Las normas imperativas de la ley del Estado de residencia del consumidor se convierten, entonces, en el límite infranqueable o régimen prevalente en caso de conflicto con la ley pactada. Algo parecido ocurriría entonces con la ley del Estado de origen del prestador de SSI establecido en la UE: podrá resultar aplicable otra ley, pero si fuera más restrictiva para el prestador que la del Estado de su establecimiento, prevalecería esta última[88]. A la hora de valorar esta solución, se ha criticado su carác-

86. En este sentido, Forner Delaygua, J.J. (2013, cit., p. 422).

87. Aparte del ejemplo del art. 6.2, el autor citado menciona los de los arts. 3.3, 3.4 y 8.1 del Reglamento en cuestión, y también el del art. 14.3 del Reglamento 864/2007 (*ibid.*, p. 422).

88. Como señala Forner Delaygua, la Directiva atribuye a la ley del Estado de origen —a la que dicho autor llama "ley respetable"— un "título superior" para su aplicación (2013, cit., pp. 425-426). Ahora bien, no creo que el resultado al que llegó el TJUE en el caso *eDate* resulte sorprendente, a la vista de los considerandos tanto de la DCE (núm. 23) como del Reglamento 864/2007 (núm. 35, se-

ter desequilibrado en favor del prestador del servicio, en detrimento de la otra parte[89]. En mi opinión, sin embargo, esta crítica es susceptible de alguna matización. Para empezar, es cierto que el principio del Estado de origen se tiñe de una orientación *business friendly* o *pro emprenditoris*, pero ello no es de extrañar. Desde sus propios inicios jurisprudenciales, la regla de reconocimiento mutuo en el ámbito de las libertades del mercado interior, así como el principio del Estado de origen, que es su heredero en determinados actos legislativos, han buscado favorecer la integración económica en el mercado interior mediante la eliminación (o, como mínimo, minimización) de la carga que para los operadores económicos supone la doble o múltiple regulación. Es más, en el caso particular del artículo 3 de la DCE, la regla establecida se explicaría por el contexto esencialmente transnacional y ubicuo en el que se desenvuelven los SSI, que podrían verse seriamente limitados por la aplicación cumulativa de una multiplicidad de leyes estatales. Finalmente, creo que tampoco es ocioso recordar que el legislador de la Unión adoptó medidas para evitar los efectos del principio del Estado de origen que hubieran podido ser más negativos: como ya se ha explicado, en el anexo de la DCE se excluye la materia de los contratos de consumo del principio del Estado de origen, y así se evita que el contratante típicamente débil, el consumidor, quede forzosamente sujeto a la ley del Estado de establecimiento del prestador. Por todo ello, y a fin de cuentas, creo que la solución del artículo 3 de la DCE, que además se aplica únicamente en el marco del mercado interior europeo, es aceptable. Ahora bien, también es cierto que hay algún aspecto concreto que podría reconsiderarse. Se ha puesto de relieve, no sin razón, que la referencia al Estado origen del prestador (típicamente, el editor de contenidos digitales), en lo que se refiere a su régimen de responsabilidad civil por vulneración de los derechos de la personalidad, puede resultarle injustificadamente ventajosa, en detrimento de las posibles víctimas[90]. Entiendo que este desajuste podría resolverse en una futura reforma del Reglamento 864/2007, que revise la exclusión de su ámbito material de las vulneraciones de los derechos de la personalidad, hoy contenida en su artículo 1.2.g). En el marco de esta posible reforma futura, podría erigirse una regla de conflicto específica para dicho tipo de daños, que prevaleciera, dentro su ámbito de aplicación, sobre la referencia al Estado de origen del artículo 3 de la DCE[91].

---

gundo párrafo); en el ámbito de las obligaciones contractuales, véase, en los mismos términos, el cdo. 40, segundo párrafo, del Reglamento 593/2008.

89. *Ibid*., pp. 422 y 426.

90. *Ibid*., p. 426.

91. En efecto, nada impediría que en una norma de Derecho derivado posterior a la DCE el legislador reformara o limitara el alcance del principio del país de origen de su artículo 3. Una solución relativamente sencilla sería incluir en el anexo de la DCE la materia de la responsabilidad extracontractual relacionada con los derechos de la personalidad, poniéndola así a resguardo del alcance del principio del país de origen, tal como hoy se hace con los contratos de consumo o los derechos de autor y derechos afines. En todo caso, entiendo que una futura reforma debiera incluir una indicación expresa en el sentido de que la norma de conflicto adoptada por el legislador prevalezca sobre la referencia a la ley del Estado de origen del art. 3 de la DCE, porque si no se hiciera así seguiría prevale-

Por lo que se refiere, en segundo lugar, a las relaciones del Derecho público, la función del principio del Estado de origen del artículo 3 de la DCE sería distinta: ya no se trataría de determinar la "ley aplicable" a una determinada relación jurídica, sino la de determinar el Estado miembro cuyas autoridades resulten competentes para regular y supervisar la actividad de los prestadores de SSI. Debido a la correlación entre autoridad administrativa competente y Derecho aplicable propia del Derecho público (principio de que la autoridad administrativa aplica su propia ley), en este ámbito la referencia al "régimen jurídico" del Estado de origen no lo es únicamente a sus normas, sino también a la actuación de sus autoridades. Es más, en la esfera del Derecho público las cuestiones de eficacia transnacional muchas veces se plantean como cuestiones de reconocimiento de la actuación de una autoridad extranjera (actos públicos, autorizaciones, títulos…). Por ello, la referencia del artículo 3 de la DCE puede entenderse como una norma para determinar el Estado miembro cuyas autoridades administrativas tendrán competencia, con carácter principal y salvo excepciones acotadas por la propia Directiva, para supervisar la actuación de los prestadores de SSI. Esta función de la referencia al Estado de origen como criterio de atribución de competencia de la autoridad administrativa se plasmaría muy claramente en los dos textos posteriores a la DCE que han sido objeto de análisis en este trabajo: el RGPD y el RSD. En el primero de ellos la autoridad de control del Estado del establecimiento principal dispone de la competencia "principal", y las demás autoridades desempeñan una función secundaria o complementaria. En el segundo Reglamento, en cambio, el rol de la autoridad del Estado de establecimiento principal se refuerza: su competencia pasa de ser principal a ser "exclusiva". Sin embargo, ambos textos tienen en común que establecen detallados mecanismos de cooperación entre dichas autoridades administrativas, sin los cuales el sistema no podría funcionar adecuadamente.

Resulta oportuno poner de relieve que no tener suficientemente en cuenta las especificidades de los distintos contextos en los que la referencia al Estado de origen del artículo 3 de la DCE pueda plantearse (civil, penal o administrativo) puede conducir a resultados disfuncionales. Esto es lo que, a mi juicio, habría ocurrido, como ya he explicado en este trabajo, en el caso de la sentencia *Airbnb* de 2019, que adolece, siempre en mi opinión, de dos defectos graves: por un lado, que estableciera una analogía entre el procedimiento de la Directiva 2015/1535, que se aplica a proyectos de normas de alcance general, y los requisitos procedimentales del mecanismo de excepción que prevé el artículo 3.4.b), segundo guión, de la DCE, pensado para las medidas de aplicación en caso concretos. Por otro lado, es a mi juicio aún más grave que, para poder adoptar una medida que restrinja la referencia al Estado de origen, la citada sentencia declarara aplicables, en el marco de los procedimientos judiciales penales y civiles, unas exigencias de procedimiento diseñadas para la comunica-

---

ciendo el citado art. 3, tal como se desprende del segundo párrafo del considerando 35 del Reglamento 864/2007.

ción y colaboración entre autoridades administrativas. Como se ha explicado en este trabajo, semejante intromisión de mecanismos típicos de la cooperación administrativa en el ámbito de la asistencia o cooperación judicial en materia penal o civil puede resultar muy problemático. Por ello, entiendo que la doctrina sentada en el asunto *Airbnb* de 2019 debiera ser objeto de una urgente revisión.

Por último, cabe añadir que, aunque el principio del Estado de origen proclamado en el artículo 3 de la DCE siga siendo una pieza fundamental del marco regulatorio de los SSI en el mercado interior, en los últimos años puede haber perdido algo de su trascendencia práctica, al menos por lo que se refiere a la determinación del contenido de las normas aplicables. Ello se debería al importante avance de la armonización de legislaciones en el sector digital, con la consiguiente eliminación o minimización de las disparidades normativas entre los Estados miembros[92]. En cambio, en el terreno de la determinación de la competencia supervisora de las autoridades administrativas, la armonización de legislaciones habría producido precisamente el efecto contrario, puesto que habría reforzado el rol de la autoridad del Estado de establecimiento principal del prestador. El ejemplo más destacado es el del antes analizado RSD, que otorga a la competencia de dicha autoridad un carácter exclusivo[93].

JURISPRUDENCIA DEL TJUE

Sentencia *Cassis de Dijon*, de 20 de febrero de 1979 (as. C-120/78, ECLI:EU:C:1979:42).

Sentencia *Keck*, de 24 de noviembre de 1993 (as. C-267/91 y C-268/91, ECLI:EU:C:1993:905).

Sentencia *Cia Security*, de 30 de abril de 1996 (as. C-194/94, EU:C:1996:172).

Sentencia *eDate Advertising*, de 25 de octubre de 2011 (as. C-509/09 y C-161/10. ECLI:EU:C:2011:685).

Sentencia *de Visser*, de 15 de marzo de 2012 (as. C-292/10, ECLI:EU:C:2012:142, ap. 69-72).

Sentencia *Papasavvas*, de 11 de septiembre de 2014 (as. C-291/13, ECLI:EU:C:2014:2209).

Sentencia *Vanderborght*, de 4 de mayo de 2017 (as. C-339/15, ECLI:EU:C:2017:335).

Sentencia *Asociación Profesional Élite Taxi*, de 20 de diciembre de 2017 (as. C-434/15, ECLI:EU:C:2017:981).

92. En este sentido, Feliu Álvarez de Sotomayor, S. señala que, durante casi dos décadas, la regulación del comercio electrónico se vio reducida a la DCE, que con el tiempo habría devenido insuficiente. Sin embargo, a partir de 2019 se habría producido una "eclosión" de normas armonizadoras del sector digital a escala de la Unión (2024, cit., p. 43).

93. Habría que matizar a este respecto que, en lo que se refiere a la autoridad administrativa de control, hay ocasiones en que la legislación armonizada se ha apartado del modelo de control por el Estado de origen, cuando otorga la competencia supervisora a una autoridad supranacional como la Comisión Europea.

Sentencia *College van Burgemeester en Wethouders van de gemeente Amersfoort*, de 30 de enero de 2018 (as. C-360/15 y C-31/16, ECLI:EU:C:2018:44).
Conclusiones del Abogado General M. Szpunar en el asunto *Airbnb* (as. C-390/18), presentadas el 30 de abril de 2019 (ECLI:EU:C:2019:336).
Sentencia *Austria c. Alemania*, de 18 de junio de 2019 (as. C-591/17, ECLI:EU:C:2019:504).
Sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland*, de 3 de octubre de 2019 (as. C-18/18, ECLI:EU:C:2019:821).
Sentencia *Airbnb Ireland*, de 19 de diciembre de 2019 (as. C-390/18, ECLI:EU:C:1112).
Sentencia *A contra Daniel B y otros*, de 1 de octubre de 2020 (as. C-49/18, ECLI:EU:C:2020:764).
Sentencia *La Quadrature du Net,* de 6 de octubre de 2020 (as. C-511/18 y otros, ECLI:EU:C:2020 :791).
Sentencia *Star Taxi App,* de 3 de diciembre de 2020 (as. C-62/19, ECLI:EU:C:2020:980).
Sentencia *Facebook Ireland Ltd.*, de 15 de junio de 2021 (as. C-645/19, ECLI:EU:C:2021:483).
Sentencia *Airbnb Ireland y Airbnb Payments UK*, de 22 de diciembre de 2022 (as. C-83/21, ECLI:EU:C:2022:1018, ap. 25).
Sentencia *Booky.fi Oy*, de 23 de marzo de 2023 (as. C-662/21, ECLI:EU:C:2023:239).
Sentencia *Viagogo AG*, de 27 de abril de 2023 (as. C-70/22, ECLI:EUC:2023:350).
Sentencia *Google Ireland*, de 9 de noviembre de 2023 (as. C-376/22, ECLI:EU:C:2023:835).
Sentencia *Doctipharma*, de 29 de febrero de 2024 (as. C-606/21, ECLI:EU:C:2024:179).
Sentencia *Airbnb Ireland UC* y *Amazon Services Europe Sarl*, de 30 de mayo de 2024 (as. C-662/22 y C-667/22, ECLI:EU:C:2024:432).
Sentencia *Google Ireland* y *Eg Vacation Rentals Ireland*, de 30 de mayo de 2024 (as. C-664/22 y C-666/22, ECLI:EU:C:2024:434).
Sentencia *Amazon Services Europe*, de 30 de mayo de 2024 (as. C-665/22, ECLI:EU:C:2024:435).

BIBLIOGRAFÍA

AGUDO GONZÁLEZ, J. (2019). La articulación de las relaciones jurídicas transnacionales mediante las variantes del reconocimiento mutuo. Agudo González, J. (dir.). *Relaciones jurídicas transnacionales y reconocimiento mutuo*. Aranzadi (pp. 181-310).
BALLESTA MARTÍ, L. (2023). *The Communication to the Public of Musical Works Online in the European Union's Legislation: Striving for a Fair Balance*. Tesis doctoral, Universitat Autònoma de Barcelona.
BASEDOW, J. (1995). Der kollisionrechtliche Gehalt der Produktfreiheiten im europäischen Binnenmarkt. *Rabels Z.* (pp. 1-55).

CASTELLÓ PASTOR, J.J. (dir.) (2024). *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*. Aranzadi.

DE MIGUEL ASENSIO, P. (2022). *Derecho privado de Internet*. Thomson Reuters (6ª ed.).

DE MIGUEL ASENSIO, P.A. (2023). *Manual de Derecho de las nuevas tecnologías*. Aranzadi.

DE MIGUEL ASENSIO, P.A., (2023, 2) El criterio de origen en la Directiva sobre el comercio electrónico y su interacción con el Reglamento de servicios digitales. *Blog de Pedro de Miguel Asensio*, post de 10-11-2023, accesible en: https://pedrodemiguelasensio.blogspot.com/2023/11/el-criterio-de-origen-en-la-directiva.html

DE MIGUEL ASENSIO, P.A. (2024). Criterio de origen de la Directiva sobre comercio electrónico y límites a las medidas de aplicación del Reglamento (UE) 2019/1150 sobre servicios de intermediación en línea. *Blog de Pedro De Miguel Asensio* (post de 30-5-2024), accesible en: https://pedrodemiguelasensio.blogspot.com/2024/05/criterio-de-origen-de-la-directiva.html

EL HAGE, Y. (2022). *Le droit international privé à l'épreuve de l'Internet*. L.G.D.J.

FELIU ÁLVAREZ DE SOTOMAYOR, S. (2024). Ámbito territorial y aplicación del principio de control en origen en el Reglamento (UE) de servicios digitales. Castelló Pastor, J.J. (dir.), *Análisis del Reglamento (UE) de servicios digitales y su interrelación con otras normas de la Unión Europea*. Aranzadi (pp. 41-67).

FORNER DELAYGUA, J.J. (2013), "Ley aplicable y ley respetable". Forner Delaygua et al. *Entre Bruselas y La Haya. Estudios sobre la unificación internacional y regional del Derecho internacional privado. Liber amicorum Alegría Borrás*, Marcial Pons (pp.417-427).

GARDEÑES SANTIAGO, M. (2019). El reconocimiento mutuo en la Unión Europea: su naturaleza jurídica a la luz de las técnicas o métodos del Derecho internacional privado. Agudo González, J. (dir.). *Relaciones jurídicas transnacionales y reconocimiento mutuo*. Aranzadi (pp. 123-179).

GARDEÑES SANTIAGO, M. (2024). Medida cautelar adoptada en el asunto Worldcoin: la AEPD ordena el cese inmediato de la actividad de recogida de datos biométricos en España. Blog *Derecho y digitalización empresarial* (post de 17-3-2024), accesible en: https://webs.uab.cat/derecho-y-digitalizacion-empresarial/2024/03/17/medida-cautelar-adoptada-en-el-asunto-worldcoin-la-aepd-ordena-el-cese-inmediato-de-la-actividad-de-recogida-de-datos-biometricos-en-espana/

GOÑI URRIZA, N. (2023), *La libre circulación de servicios en la Unión Europea: El régimen de la libertad de establecimiento y la libre prestación de servicios y su aplicación por los tribunales españoles*. Bosch.

HELLNER, M. (2004). The Country of Origin Principle in the E-commerce Directive: A Conflict with Conflict of Laws? Fuchs, A., Muir Watt, H. y Pataut, E. (dirs). *Les conflits de lois et le système juridique communautaire*. Dalloz (pp. 205-224).

MATTERA, A. (1991). Les principes de proportionnalité et de reconnaissance mutuelle en matière de libre circulation de personnes et des services: de l'arrêt Thieffry aux arrêts Vlassoupoulou, Mediawet et Dennemayer. *Revue du Marché Unique Européen, núm. 4* (pp. 191-203).

PICONE, P. (2004). Diritto internazionale privato comunitario e pluralità dei metodi di coordinamento tra ordenamenti. Picone, P. (ed.). *Diritto internazionale privato e diritto comunitario*. Cedam.

TEBBENS, H.D. (1994). Les conflits de lois en matière de publicité déloyale à l'épreuve du droit communautaire. *Revue critique de droit international privé* (pp. 451-481).

THOMALE C. y WELLER, M.-P. (2017). Country of origin rule. Basedow. J et al. (ed.). *Encyclopaedia of Private International Law*. Elgar (pp. 479-483).

VILÀ COSTA, B. (2022). The new Digital Markets Act and Services Market Act and its Relevance on EU Legal Harmonization. *Evrigenis Yearbook of International and European Law*, vol. 4 (pp. 209-219), cortesía de la autora.

II. Empresa y ubicación territorial

La protección de los usuarios de las plataformas de intercambio de vídeos (PIV): aspectos de interés para la determinación de la competencia judicial internacional en materia contractual

Josep Suquet Capdevila
Profesor Lector Serra Húnter de Derecho Internacional Privado
Universitat Autònoma de Barcelona (UAB)

ABSTRACT
This chapter explores a series of issues related to Video Sharing Platforms (VSPs). It starts analysing the conceptual framework of VSPs as contained in Directive 2018/1808 and Ley 13/2022, de 7 de julio, general de comunicación audiovisual. Moreover, it highlights some existing conflicts currently addressed by national courts, in particular related to influencer-generated content as well as to breaches of advertising and copyright contracts. Furthermore, from the perspective of Private International Law, and within the framework of Regulation 1215/2012 of the European Parliament and of the Council, on jurisdiction, recognition, and enforcement of judgments in civil and commercial matters, it provides for an interpre-

tation of the choice-of-forum, the contractual forum for the provision of services, and the consumer forum in light of the characteristics of VSPs.
Keywords: video-sharing platforms, General Law on Audiovisual Communication, international jurisdiction, EU Regulation 1215/2012, party autonomy, contractual forum, consumer forum
Palabras clave: plataformas de intercambio de vídeos, Ley general de comunicación audiovisual, competencia judicial internacional, Reglamento UE 1215/2012, autonomía de la voluntad, foro contractual, foro de consumo

1. INTRODUCCIÓN

Las plataformas en línea han revolucionado la manera en que consumimos información, entretenimiento y servicios en la era digital. Su impacto es innegable y sigue creciendo a medida que más personas se conectan y participan en estas plataformas. En el sector audiovisual las plataformas digitales están muy extendidas y juegan un papel muy relevante tanto a nivel económico como social y cultural. Así, algunas cifras destacan la magnitud de esta situación: Facebook, la plataforma de redes sociales más grande del mundo, contaba a febrero de 2024 con más de a tres mil millones de usuarios mensuales, y otras plataformas de redes sociales, como YouTube y WhatsApp, también contaban con más de dos mil millones de usuarios cada una.[1]

Desde hace varios años, la UE se ha dedicado a consagrar un marco regulatorio equilibrado para las plataformas online emitiendo toda una nueva batería de normas.[2] En este sentido, la diversidad de los ámbitos de actividad en los que operan las plataformas digitales y la gran variedad de modelos de negocio,

1. Statista. (2024). *Most popular social networks worldwide as of April 2024, ranked by number of monthly active users*. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. Ver E. Ortiz-Ospina. (2019). *The rise of social media*. https://ourworldindata.org/rise-of-social-media.

2. Entre otros, ver. C. Codagnone, G. Liva, T. Rodríguez de las Heras Ballell. (2022) *Identification and Assessment of Existing and Draft EU Legislation in the Digital Field*. European Parliament. Policy Department for Economic, Scientific and Quality of Life Policies; T. Rodríguez de las Heras Ballell. (2021). The background of the Digital Services Act: looking towards a platform economy. *ERA Forum*, 22(1), 75-86 p. 78.

así como el entorno rápidamente cambiante del mundo digital, ha llevado a las instituciones de la UE a evitar una definición única de "plataformas digitales".[3]

La Directiva UE 2018/1808, relativa a los servicios de comunicación audiovisual (Directiva SCA) y la Ley 13/2022, de 7 de julio, general de comunicación audiovisual, consagran algunas obligaciones que algunos proveedores que prestan servicios en este campo deben cumplir.[4] Si bien originalmente la Directiva audiovisual regulaba los servicios prestados por los proveedores tradicionales de medios de radiodifusión, hoy en día, la Directiva 2018/1808 también regula algunos de los servicios prestados por plataformas digitales.[5] En efecto, en los últimos años la convergencia tecnológica ha desdibujado los límites entre los medios establecidos y otras industrias de la comunicación, y ha difuminado los servicios de telecomunicación, radiodifusión e Internet. Además, han surgido nuevos modelos de negocio, con la proliferación de servicios de comunicación audiovisual a petición, en *streaming* y específicamente, la irrupción de las plataformas de intercambio de vídeos (PIV) en Internet. En este nuevo mercado, en el que compiten las ofertas para atraer a los usuarios como clientes, el legislador europeo ha creado un marco regulatorio gradual para las entidades que prestan sus servicios en este ámbito. Este marco normativo dota de un conjunto de reglas estrictas para los servicios tradicionales, unas reglas menos estrictas para los SCA de acceso condicional[6] y por primera vez, también crea unas reglas,

3. Parlamento Europeo. (2017). *Report on online platforms and the digital single market*. (2016/2276(INI)).

4. Ley 13/2022, de 7 de julio, *general de comunicación audiovisual* (BOE 163, 8 Julio 2022).

5. La Directiva 2010/13/UE 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) (versión codificada), DO L 95 de 15.4.2010, p. 1–24, y la Ley 13/2022, de 13 de julio, general de comunicación audiovisual, parten de la tradicional distinción entre servicios de comunicación lineal y no lineal. Así, la Ley 13/2022 contiene dentro de su ámbito de aplicación a los servicios de comunicación audiovisual televisivo lineal, entendidos como aquellos servicios de comunicación audiovisual que se prestan "para el visionado simultáneo de programas y contenidos audiovisuales sobre la base de un horario de programación" (Art. 2.5 Ley 13/2022) así como los servicios de comunicación audiovisual televisivo a petición o televisivo no lineal, entendidos como aquellos servicios de comunicación audiovisual que se prestan "para el visionado de programas y contenidos audiovisuales en el momento elegido por el espectador y a su propia petición sobre la base de un catálogo de programas seleccionado por el prestador del servicio."(Art. 2.6 Ley 13/2022). Los art. 2.7 y art. 2.8 de la Ley 13/2022 definen los servicios de comunicación audiovisual radiofónico y los servicios de comunicación audiovisual sonoro a petición, respectivamente.

6. A tenor del artículo 2.1 de la Ley 13/2022, un "servicio de comunicación audiovisual" es aquel "servicio prestado con la finalidad principal propia o de una de sus partes disociables de proporcionar, bajo la responsabilidad editorial de un prestador del servicio de comunicación audiovisual, a través de redes de comunicaciones electrónicas, programas con objeto de informar, entretener o educar al público en general, así como emitir comunicaciones comerciales audiovisuales." En efecto, la responsabilidad editorial se configura como un elemento esencial en la calificación de estos servicios, así como del prestador de los servicios de comunicación audiovisual, entendido como aquella "persona física o jurídica que tiene la responsabilidad editorial sobre la selección de los programas y

aunque más suaves, que son de aplicación para las plataformas de intercambio de vídeos (PIV).[7]

Los servicios de comunicación audiovisual de acceso condicional se han vuelto cada vez más populares en la era digital, ya que permite a los usuarios acceder a contenido específico según sus preferencias y horarios.[8] Las plataformas "Over the Top" (OTT) como Netflix, HBO y Amazon Prime Video ofrecen una amplia variedad de contenido, como películas, documentales, programas o eventos deportivos, lo que ha transformado la forma en que consumimos contenido audiovisual. Estas plataformas tienen en común que actúan como portales de pago para la distribución de contenido producido profesionalmente, a diferencia de los portales en que el contenido es generado por los usuarios como YouTube. Además, son ejemplos notables de que estas plataformas se han posicionado fuertemente en el mercado del entretenimiento, conquistando y revolucionando el panorama del entretenimiento bajo demanda.

2. PLATAFORMAS DE INTERCAMBIO DE VÍDEOS (PIV): CONCEPTO Y TIPOLOGÍA DE CONFLICTOS

Por otro lado, las plataformas de intercambio de vídeos (PIV) atraen a una amplia variedad de usuarios que interactúan con sus servicios, como creadores de contenido, personas influenciadoras, artistas, educadores, por nombrar algunos. En definitiva, estas PIV son populares entre las personas que crean y suben sus propios vídeos, y muchas han dado lugar a que los creadores de contenido tengan un gran número de seguidores y atraigan a una gran audiencia. Como usuarios de dichas plataformas, las personas principalmente las utilizan para acceder a su contenido, para buscar, navegar y acceder a una amplia variedad de vídeos subidos por otros usuarios o creadores de contenido. Además, también permiten la interacción y el compromiso entre los usuarios y los creadores de contenido, ya que los usuarios pueden dar un "me gusta", comentar y compartir vídeos, proporcionando una retroalimentación muy valiosa para los creadores de contenido. Además, dichos usuarios también pueden seguir o suscribirse a canales específicos para recibir actualizaciones de los creadores de contenido.

---

contenidos audiovisuales del servicio de comunicación audiovisual y determina la manera en que se organiza dicho contenido." (art.2.4 Ley 13/2022).

7. P. Valcke, P. & I. Lambrecht. (2021). The evolving scope of application of the AVMS Directive. En Parcu, P. L., & Brogi, E. (Eds.), *Research handbook on EU media law and policy*. Edward Elgar Publishing Limited (pp. 282-302), p 282; L. Kukliš (2019), Video-Sharing Platforms In AVMSD – A New Kind Of Content Regulation, en P. L. Parcu & E. Brogi (Eds.), *Research Handbook on EU Media Law and Policy* (pp. 303-325), Edward Elgar Publishing.

8. El art. 2.12 de la Ley 13/2022 define los servicios de comunicación audiovisual de acceso condicional, entendidos como aquellos "servicios que ofrecen, mediante un sistema de acceso condicional, programas y contenidos audiovisuales a cambio de una contraprestación por parte del usuario."

La Directiva 2018/1808 exige a los Estados Miembros que tomen medidas para que las PIV adopten medidas en relación con la organización de los contenidos para proteger a los menores de contenidos que puedan perjudicar su desarrollo físico, mental o moral, así como para proteger al público en general de contenidos que contengan incitación a la violencia o al odio, o de la difusión de contenido que constituya una infracción penal según el Derecho de la Unión.[9] La Ley 13/2022 cumple con el mandato de la Directiva y regula los servicios de intercambio de vídeos a través de plataforma (PIV).[10]

Según la Ley 13/2022, los servicios de intercambio de vídeos a través de una plataforma son proporcionados con el objeto de informar, entretener o educar, así también para emitir comunicaciones comerciales.[11] Además, una de las características esenciales de estos servicios es que, a diferencia de los servicios de comunicación audiovisual, el prestador de estos servicios no tiene responsabilidad editorial sobre los mismos. Junto a ello, la diferente tipología en la que las plataformas pueden prestar estos servicios ha hecho que el legislador haya englobado a estos servicios cuando la "finalidad principal" de la plataforma sea prestar estos servicios, así como también cuando la plataforma los provea a través de "una de sus partes disociables," e incluso cuando la plataforma preste estos servicios a través de una "funcionalidad esencial". Asimismo, estos servicios se deben prestar al público en general, "a través de redes de comunicaciones electrónicas, programas, vídeos generados por usuarios o ambas cosas". [12] Aunque la plataforma no tenga responsabilidad editorial sobre el contenido, sí que la organización de este viene determinada por el prestador de los servicios, pudiendo organizarse de manera manual o a través de algoritmos automáticos, mediante la presentación, etiquetado y la secuenciación.

Las plataformas digitales, así como las PIV, en particular, no han solido informar de forma detallada acerca de los conflictos en las que se ven involucradas. Esto puede deberse a que estos actores globales han tenido una política de secretismo, y precisamente esta falta de transparencia es la base para que la UE se haya propuesto proporcionar un entorno en línea transparente y seguro con la consagración de la Directiva 2018/2018, así como de manera más general, con toda una batería de normas muy relevantes, entre ellas el Reglamento de Servicios Digitales (DSA).[13]

---

9. Considerandos 47 y 48 de la Directiva 2018/2018.

10. Así, artículos 86 y siguientes de la Ley 13/2022, de 7 de julio.

11. Art. 2.13 de la Ley 13/2022.

12. Art. 2.13 Ley 13/2022, de 7 de julio: "Servicio de intercambio de vídeos a través de plataforma: Servicio cuya finalidad principal propia o de una de sus partes disociables o cuya funcionalidad esencial consiste en proporcionar, al público en general, a través de redes de comunicaciones electrónicas, programas, vídeos generados por usuarios o ambas cosas, sobre los que no tiene responsabilidad editorial el prestador de la plataforma, con objeto de informar, entretener o educar, así como emitir comunicaciones comerciales, y cuya organización determina el prestador, entre otros medios, con algoritmos automáticos, en particular mediante la presentación, el etiquetado y la secuenciación."

13. Art. 28 ter 3.d, y 3.i) de la Directiva 2018/1808. Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y

Así, la Ley 13/2022 establece que las plataformas de intercambio de vídeos (PIV) deben implementar procedimientos transparentes, eficaces y de fácil uso para el tratamiento y la resolución de las reclamaciones de usuarios.[14] Sin embargo, algunas investigaciones sugieren que las plataformas digitales priorizan la moderación de contenido sobre algunos ámbitos específicos por encima de otros ámbitos; enfatizan el control sobre las infracciones de derechos de autor y propiedad intelectual, así como sobre contenidos de naturaleza potencialmente criminal, mientras que parecen ignorar los conflictos que caen dentro del área del derecho del consumo.[15] De esta forma, es usual que las plataformas digitales implementen mecanismos de denuncia de conflictos de propiedad intelectual y actividades terroristas, pero no tengan ninguna categoría bajo la cual los usuarios puedan denunciar conflictos de consumo, como las ventas ilegales o el fraude. En la práctica, esto significa que estas plataformas no permiten a los usuarios informar sobre este tipo de contenidos. Por otro lado, las plataformas examinan los derechos de autor o la actividad terrorista mediante algoritmos, los cuales se eliminan en caso de infracción, mientras que el contenido que afecta a los consumidores no recibe la misma atención.[16] Por lo tanto, parece que las plataformas pueden estar implementando estos mecanismos de reparación para protegerse de su responsabilidad como intermediarios, en lugar de proteger los derechos de los consumidores.

Recientemente se ha comprobado como algunas PIV se han visto involucradas en una serie de conflictos. Así, diversas PIV han recibido diversas multas millonarias por parte de las autoridades de protección de datos: la Autoridad de Protección de Datos de Irlanda multó a TikTok con 345 millones de euros por violar las leyes de privacidad relativas al procesamiento de datos personales de niños en la Unión Europea, y Instagram fue multada con 405 millones de euros por motivos similares.[17] Desde el prisma del Derecho internacional privado, el Tribunal de Justicia de la UE tiene una rica y compleja jurisprudencia en el ámbito extracontractual en el que están involucradas plataformas digitales, aunque no específicamente las PIV.[18] Sin embargo, se ha prestado menos atención al análisis de las relaciones jurídicas contractuales involucradas con los servicios

---

por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales), DOUE Núm. 277, de 27 de octubre de 2022, DOUE-L-2022-81573.

14. Art. 89.1. g) Ley 13/2022, y art. 28 ter.3 i) de la Directiva 2018/1808. También en el ámbito del DSA (artículos 21 y 22 del DSA, que regula los mecanismos internos y de mediación, respectivamente).

15. C. Goanta, P. Ortolani. (2022). Unpacking content moderation: The rise of social media platforms as online civil courts. En X. Kramer, J. Hoevenaars, B. Kas, & E. Themeli (Eds.), *Frontiers in Civil Justice: Privatisation, Monetisation and Digitisation* (pp. 192-216). Edward Elgar Publishing. p 11.

16. Ibid., p 2.

17. BBC News. (2023). *TikTok fined 345 million euros over handling children's data in Europe*. https://www.bbc.com/news/technology-62800884. (último acceso, junio de 2024).

18. Por ejemplo, en el caso de los actos difamatorios en Internet, como la sentencia del TJUE de 21 de diciembre de 2021 en el asunto C-251/20, *Gtflix Tv v DR*, o la Sentencia del TJUE de 17 de octubre de 2017, asunto C-194/16, *Bolagsupplysningen OÜ y Ingrid Ilsjan v Svensk Handel AB*; Sen-

proporcionados por las plataformas digitales, en general, y las PIV, en particular. Estos conflictos son muy relevantes para la sociedad y los individuos debido a la fuerte posición de las plataformas digitales, y cada vez existe más jurisprudencia nacional que resuelve conflictos legales contractuales con dichas plataformas.

Uno de los ámbitos dónde existe conflictualidad con las PIV se refiere a las personas influenciadoras o *influencers*. En efecto, existen situaciones en las que personas influenciadoras se enfrentan a demandas legales debido a contenido que han subido a las PIV, que no cumple con las normas en materia de publicidad. Estas obligaciones incluyen la identificación clara de contenido publicitario y la prohibición de promocionar productos como el tabaco, el alcohol o los juegos de azar.[19] Así, un tribunal nacional ha considerado las historias de Instagram de una persona conocida como publicidad subrepticia y acto engañoso, ya que en su vídeo no mencionaba el carácter publicitario del acto.[20] En el mismo caso, aparecieron varios testimonios en vídeo de personas conocidas en el canal de YouTube de una clínica dental que, además, en cuanto productos sanitarios, debía seguir disposiciones restrictivas específicas sobre publicidad. En consecuencia, el tribunal ordenó el cese inmediato de la difusión de publicidad, así como la obligación de redactar un resumen de la sentencia en su cuenta de YouTube, Facebook e Instagram.

Además, los medios franceses también han expresado su preocupación por el hecho de que las personas influenciadoras no respeten la legislación sobre publicidad, así como la reciente normativa específica, y varios casos abordan esta cuestión.[21] Por ejemplo, la entidad francesa autorizada para controlar las prácticas publicitarias en Francia multó a una persona influenciadora que promovió en su historia de Snapchat servicios de formación de comercio de bitcoins, sin mencionar el carácter publicitario ni el hecho de que una empresa le paga-

---

tencia del TJUE (Gran Sala) de 25 Octubre de 2011, *eDate Advertising GmbH y otros v X and Société MGN Limited*, asuntos C-509/09 and C-161/10.

19. En España, el Real Decreto 444/2024 ha actualizado el artículo 94 de la Ley 13/2022, general de comunicación audiovisual. Real Decreto 444/2024, de 30 de abril, por el que se regulan los requisitos a efectos de ser considerado usuario de especial relevancia de los servicios de intercambio de vídeos a través de plataforma, en desarrollo del artículo 94 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual. Ver A. Gálvez Jiménez y G.A., García Escobar, (2023). *Derecho de la publicidad en Internet: redes sociales y plataformas digitales* (1.ª ed.). Aranzadi. Existen diversas recomendaciones y documentos de organismos internacionales sobre la actividad de las personas influenciadoras. Entre otras, ver, Dictamen del Comité Económico y Social Europeo. (2023). *La publicidad a través de influencers y su impacto en los consumidores*. (2023/C 349/15), DOUE C 349/94; ICC. (2018); *Advertising and Marketing Communications Code;* European Advertising Standards Alliance (EASA). (2023). *Best Practice Recommendation on Influencer Marketing Guidance;* ICPEN (2016). *ICPEN Guidelines for digital influencers*.

20. Artículo 5 y artículo 7 de la *Ley 3/1991, de 10 de enero, de competencia desleal*. Ver la Sentencia del Juzgado Mercantil de Madrid, de 2 de marzo de 2023, *Col.legi d'Odontòlegs v. Vitaldent*, 1321/2023, ECLI: ES: JMM:2023:1321.

21. LOI n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux, JORF nº 0133, de 10 de junio de 2023.

ra.[22] En otro caso, también en Francia, recientemente se presentó una demanda colectiva contra un famoso *influencer* con cargos por fraude y abuso de confianza. En resumen, varias personas creyeron que habían sido estafadas al invertir en productos financieros promocionados por una persona famosa en Internet y, a continuación, Meta eliminó la cuenta de Instagram de dicha persona influenciadora.[23] En otro caso, presentado ante el tribunal judicial de Paris, el tribunal dictaminó sobre la demanda de la Asociación contra la adicción en Francia contra Meta Platforms Ireland Limited.[24] En dicho supuesto, varias personas influenciadoras habían estado promocionando bebidas alcohólicas en sus cuentas de Instagram. El Tribunal de París no estimó la excepción de competencia judicial internacional de la demandada y otorgó medidas provisionales, mediante las cuales ordenó a Meta a eliminar las publicaciones alojadas en Instagram, y dictaminó una multa en caso de demora en el cumplimiento.

Otro conjunto de casos se refiere al incumplimiento de contratos publicitarios y de derechos de autor llevados a cabo a través de PIV. En efecto, en estas situaciones, los usuarios o creadores de contenido pueden enfrentarse a disputas legales debido a la falta de cumplimiento de las condiciones establecidas en los contratos publicitarios o por infringir los derechos de autor de terceros. Estas controversias pueden involucrar aspectos como el uso no autorizado de música o imágenes en los vídeos publicados en las PIV. Por ejemplo, un juzgado de Barcelona ha dictaminado sobre un asunto en el que el actor demandaba a una empresa por incumplimiento de un contrato publicitario.[25] Así, el actor y la demandada habían acordado realizar una campaña publicitaria que se debía emitir durante un periodo de tres meses; en cambio, la demandada subió el vídeo, en el que aparecía el actor, en su canal de Vimeo, el cual estuvo visible durante mucho más tiempo del permitido. En la sentencia, el juzgado de Barcelona declara la violación del contrato y dicta una indemnización para el actor. Sin embargo, el juez no se refiere al hecho de que las actividades de la demandada violaban otro contrato, en este caso, las condiciones de uso de Vimeo, que prohíben estrictamente la carga de contenido que infrinja los derechos de propiedad intelectual.[26]

---

22. Ministère de l'Économie, des Finances et de la Relance. (2021). *Communiqué de presse : Nabilla Benattia Vergara condamnée pour publicité trompeuse.* https://www.economie.gouv.fr/files/files/directions_services/dgccrf/presse/communique/2021/cp-nabilla-benattia-vergara.pdf?v=1630408421 (último acceso, Junio de 2024).

23. Le Monde. (2023). *Une plainte déposée contre des influenceurs pour escroquerie et abus de confiance.* https://www.lemonde.fr/police-justice/article/2023/01/23/une-plainte-deposee-contre-des-influenceurs-pour-escroquerie-et-abus-de-confiance_6158970_1653578.html (último acceso, Junio de 2024).

24. Sentencia del Tribunal judiciaire de Paris, de 5 enero de 2023, n° 22/57472, Portalis 352J-W-B7G-CX7J M, FMN°: 1.

25. Sentencia de la Audiencia Provincial de Barcelona, de 16 de marzo de 2022, SAP B 2600/2022 — ECLI:ES:APB:2022:2600.

26. Vimeo Help Center. (2021). *A Comprehensive Guide: What Content You Can Upload to Vimeo' (Vimeo Help Center)* https://help.vimeo.com/hc/en-us/articles/16413647508753-A-Comprehen-

En otro caso, la Audiencia Provincial de Madrid ha juzgado un asunto en el que Facebook Spain SL fue demandada por una persona cuyas cuentas de Facebook e Instagram fueron cerradas por Facebook debido a sus comentarios críticos contra la plataforma.[27] Tanto el tribunal de primera instancia como el de apelación estimaron la excepción de falta de legitimación pasiva en tanto que esta debería haber sido dirigida contra Facebook Irlanda, la empresa que gestiona las cuentas en Europa.[28] En otro caso francés, un tribunal parisino determinó la responsabilidad contractual de una empresa que no respetó un contrato de autoría, mediante el cual se podían usar algunas fotografías en Instagram por un tiempo determinado; en cambio, las fotos se difundieron en otros canales, incluidos Facebook y Twitter, y el tribunal fijó una compensación económica para el demandante.[29]

3. LA AUTONOMÍA DE LA VOLUNTAD Y LAS PLATAFORMAS DE INTERCAMBIO DE VÍDEOS (PIV)

Los términos de uso de las PIV suelen incluir cláusulas de resolución de litigios en las que se establece la competencia de los tribunales de un Estado determinado. En ocasiones el objetivo principal de este tipo de cláusulas es evitar la incertidumbre de ser demandado en un foro lejano y así saber de antemano qué foro será competente en caso de que surja un conflicto; en estos casos donde la plataforma impone sus términos de uso, la plataforma puede intentar señalar a los tribunales de su domicilio, más beneficiosos para sus intereses. Además, también pueden incluirse cláusulas de Resolución Alternativa de Disputas (ADR) y de Resolución de Disputas en Línea (ODR) en sus contratos, de modo que, si surge un conflicto, las partes deberán recurrir a mecanismos extrajudiciales como el arbitraje o la mediación, o a métodos en línea.[30]

---

sive-Guide-What-Content-You-Can-Upload-to-Vimeo (último acceso, junio de 2024).

27. En dicho caso, un usuario que estaba de viaje por África detectó que sus cuentas de Facebook, Instagram, Messenger y Whatsapp dejaron de funcionar, por lo que según él quedó incomunicado. Posteriormente, al publicar en la web que gestionaba esta persona unos comentarios relativos al abuso de poder de Facebook, se produjo el bloqueo de la web.

28. Sentencia de la Audiencia Provincial de Madrid, de 3 de julio de 2023, *315/2023*, ECLI:ES:APM:2023:12974.

29. Sentencia del Tribunal judiciaire de Paris, de 23 Junio de 2023, 20/09672.

30. Por ejemplo, en las cláusulas de Tik-Tok, se establece que: "Si no podemos resolver el litigio, tanto usted como nosotros podremos acudir a sus tribunales locales. También puede acudir a los siguientes tribunales: los tribunales de la República de Irlanda tendrán jurisdicción no exclusiva sobre los litigios con TikTok Ireland Limited; y los tribunales de Inglaterra y Gales tendrán jurisdicción no exclusiva sobre los litios con TikTok Information Technologies UK Limited. Si reside en el EEE, también puede plantear la disputa ante un organismo alternativo de resolución de disputas a través de la plataforma de resolución de litigios en línea (ODR, por sus siglas en inglés) de la Comisión Europea." Tik-Tok. (2023). *Términos de Servicio*. https://www.tiktok.com/legal/page/eea/terms-of-service/es (último acceso, junio de 2024).

Ahora bien, conviene analizar con detenimiento el contenido de dichas cláusulas, con tal de analizar su validez. Cuando el Reglamento 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 sea aplicable,[31] se debe determinar si el contrato se puede calificar de consumo, de acuerdo con el art. 17 de dicho Reglamento. En caso afirmativo, por tanto, cuando nos encontramos con un contrato entre un consumidor y un empresario, el legislador europeo protege al consumidor como parte débil. De acuerdo con el artículo 19 del Reglamento 1215/2012, se establecen unas limitaciones a la autonomía de la voluntad, por lo que solamente serán válidas las cláusulas de sumisión que sean posteriores al nacimiento del litigio, que permitan al consumidor formular demandas ante órganos jurisdiccionales distintos de los que le atribuye el Reglamento, o que cuando el consumidor y el empresario estén domiciliados o tengan residencia habitual en un mismo Estado miembro en el momento de celebración del contrato, y se atribuya la competencia a los tribunales de dicho Estado miembro, a no ser que la ley de ese Estado prohíba tales acuerdos.[32]

Además, el Reglamento 1215/2012 establece algunas formalidades para las cláusulas de elección de foro que tienen como objetivo asegurar el consentimiento entre las partes respecto de dichas cláusulas. El TJUE ha establecido que garantizar el consentimiento real de las partes está justificado por la preocupación de proteger a la parte más débil del contrato evitando que las cláusulas de competencia, incorporadas en un contrato por una de las partes, pasen desapercibidas.[33]

El artículo 25.2 del Reglamento 1215/2012 establece la equivalencia funcional de los acuerdos celebrados en línea y por escrito, siempre que se "proporcione un registro duradero del acuerdo". Por lo tanto, los contratos pueden firmarse, por ejemplo, digitalmente con una firma electrónica, que proporciona evidencia de que la persona la acepta, o realizarse mediante un intercambio de correos electrónicos. Sin embargo, normalmente los acuerdos realizados con plataformas digitales se realizan clicando en una casilla, mediante el cual un comerciante presenta los términos del contrato a la otra parte, la cual debe clicar para aceptar. En particular, el TJUE ha interpretado esta disposición en el asun-

31. Reglamento (UE) n ° 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, DO L 351 de 20.12.2012, p. 1-32.

32. Así, por ejemplo, en las cláusulas de Tik-Tok, en caso que nos encontremos ante un contrato de consumo, la siguiente afirmación no es válida: "Si no podemos resolver el litigio, tanto usted como nosotros podremos acudir a sus tribunales locales". En efecto, de acuerdo con el art. 17 del Reglamento 1215/2012, el consumidor podrá demandar a Tik-Tok, como entidad con sede en la República de Irlanda, ante los tribunales del domicilio del consumidor, mientras que Tik-Tok solamente podría demandar al consumidor ante los tribunales del domicilio de este.

33. Sentencia del TJUE de 7 de julio de 2016, asunto C-222/15, *Hőszig Kft. v Alstom Power Thermal Services*, apartado 36; Sentencia del TJUE de 8 de marzo de 2018, asunto C-64/17, *Saey Home & Garden NV/SA* v *Lusavouga-Máquinas e Acessórios Industriais SA*, apartado 25.

to *Jaouad El Majdoub*, donde el tribunal afirmó que este requisito se cumple cuando el sitio web ofrece la posibilidad de proporcionar un registro duradero de dicho acuerdo, como guardar e imprimir la información, aunque no es necesario que las partes hayan grabado dicha cláusula.[34]

Además, en la sentencia del TJUE en el asunto *Tilman y Unilever*, relativa a la aplicación del Convenio de Lugano II, el tribunal tuvo que pronunciarse sobre una cláusula de elección de foro contenida en las condiciones generales a la que el contrato dirigía a través de un enlace de hipertexto, y en la que no se requería de una cláusula para ser aceptada.[35] El Tribunal consideró que tal cláusula está válidamente concluida cuando el enlace de hipertexto permite visualizar, descargar e imprimir dichas condiciones generales, antes de la firma del contrato. Así, la interpretación del TJUE favorece la aceptación de cláusulas incluidas en condiciones que un usuario acepta mediante un clic o mediante enlaces de hipertexto, aunque es dudoso que se pueda afirmar que los consumidores hayan consentido sobre las cláusulas de sumisión, ya que algunos estudios muestran como los consumidores no leen las cláusulas y condiciones contenidas en las plataformas.[36] Además, hay que tener en cuenta que, por lo que se refiere a las formalidades requeridas en dichas cláusulas, no se pueden considerar las normas de derecho material de la UE para la protección del consumidor ya que el art. 25 es una disposición uniforme. Aun así, el art. 25.1 del Reglamento 1215/2012 aplica la ley del foro elegido (*lex fori prorogatum*), incluidas sus normas de elección de ley, a la cuestión de la validez sustantiva de un acuerdo de elección de foro, al establecer que: "a menos que el acuerdo sea nulo de pleno derecho en cuanto a su validez material según el Derecho de dicho Estado miembro", disposición que puede incrementar la litigiosidad sobre estas cláusulas.[37]

4. EL FORO CONTRACTUAL Y LAS PLATAFORMAS DE INTERCAMBIO DE VÍDEOS (PIV)

El foro especial en materia contractual del Reglamento 1215/2012 se incardina en el marco y jerarquía de foros del Reglamento. Este foro entra en funcio-

34. Sentencia del TJUE de 21 de mayo de 2015, asunto C 322/14, *Jaouad El Majdoub carsOnTheWeb.Deutschland GmbH,* apartados 32, 36.

35. Sentencia TJUE de 24 de noviembre de 2022, asunto C-358/21, *Tilman SA v Unilever Supply Chain Company AG*, apartado 57. Convenio de Lugano relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil, DO L 339 de 21.12. 2007.

36. European Commission, *Special Eurobarometer 447. Report on Online Platforms*, 2016.

37. Así, cierta doctrina ha considerado que una interpretación amplia del concepto de validez sustantiva invadiría el concepto autónomo de consentimiento desarrollado por la jurisprudencia del TJUE, pero podría evitar la necesidad de un enfoque armonizado del derecho contractual sustantivo de la UE para la aplicabilidad de los acuerdos de elección de foro frente a terceros. M. Ahmed. (2024). (2024). CoL.net: Who is bound by Choice of Court Agreements in Bills of Lading?. *ConflictsofLaws.net*. https://conflictoflaws.net/2024/who-is-bound-by-choice-of-court-agreements-in-bills-of-lading/.

namiento cuando no existe una cláusula de sumisión expresa (art. 25), [38] lo que puede ocurrir en ocasiones en las condiciones generales de las PIV. Además, cuando el contrato se caracterice como contrato de consumo, el foro especial del art. 7.1 no entrará en funcionamiento.

Desde el punto de vista del demandante, el foro contractual del art. 7.1 juega con una relación de alternatividad con el foro general del art. 4. Esto significa que el demandante puede presentar la demanda tanto ante el foro general, esto es, ante los órganos jurisdiccionales del Estado miembro donde tenga su domicilio el demandado (art. 4) como ante los tribunales que se determinen de acuerdo con el foro contractual especial (art. 7.1).

Cabe señalar que los foros especiales otorgan competencia a los tribunales de un determinado Estado miembro porque existe una proximidad razonable entre el litigio y esos tribunales, esto es, existe "un vínculo estrecho entre el contrato y el tribunal llamado a conocer y resolver el caso."[39] Esta conexión particularmente estrecha entre el litigio y el tribunal justifica la atribución de competencia a dichos tribunales por razones relativas a la buena administración de justicia y al desarrollo eficaz de los procedimientos. [40] Por tanto, esta proximidad supone que se cumple uno de los principios básicos de la atribución de competencia internacional: el principio de previsibilidad, mediante el cual un demandado habrá podido prever que podría ser demandado ante los tribunales de un determinado país.[41] En otras palabras, esta conexión particularmente estrecha garantiza la seguridad jurídica y evita la posibilidad de que una persona sea demandada ante un órgano jurisdiccional de un Estado miembro ante el cual no podía razonablemente prever que sería demandada. [42] Ello trae como consecuencia, que el lugar de emplazamiento de los servidores que esté utilizando una PIV no pueda considerarse una ubicación previsible y, por tanto, no sea adecuado como factor de conexión. [43]

El art 7.1 del Reglamento 1215/2012 contiene una norma general (art. 7.1.a y art. 7.1.c) y una particular (art. 7.1.b). Así, la regla particular del art. 7.1.b establece un foro específico respecto de un contrato de prestación de servicios, esto es, "el lugar en un Estado miembro donde, en virtud del contrato, se prestaron o deberían haberse prestado los servicios". Esta última regla unifica las

---

38. También cuando se trate de materias exclusivas (art. 24) o el demandado incurra en sumisión tácita (art. 26).

39. Sentencia del TJUE de 23 Abril 2009, asunto C-533/07, *Falco Privatstiftung and Thomas Rabitsch v Gisela Weller-Lindhorst*, apartado 24.

40. Sentencia del TJUE de 19 Abril 2012, asunto C-523/10, *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH*, apartado 18.

41. Ver el Considerando 15 del Reglamento 1215/2012.

42. Ver el Considerando 16 del Reglamento 1215/2012.

43. Sentencia del TJUE (Sala Primera) de 19 abril de 2012, asunto C-523/10, *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH*, apartado 35. También ver, T. Lutzi. (2017). Internet cases in EU Private International Law-Developing a Coherent Approach. *66 International and Comparative Law Quarterly 687*, p. 703; I. Pretelli. (2021). Protecting Digital Platform Users by Means of Private International Law. *13 Cuadernos de Derecho Transnacional 574*, p. 578.

soluciones adoptadas dentro de la UE y sigue el principio de concentración, según el cual no importa cuál es la obligación que sirve de base a la demanda (como, por ejemplo, la falta de pago), sino la ejecución característica del contrato, que es lo que debe tenerse en cuenta.[44] Para que el foro contractual del Reglamento 1215/2012 sea aplicable, el demandado debe tener su domicilio en un Estado miembro de la UE, aspecto muy relevante en el caso de las plataformas digitales, algunas de las cuales pueden operar desde fuera de la UE.

Se debe determinar si la relación entre un usuario que usa una PIV y esta se puede calificar como "materia contractual" en el sentido del art. 7.1 del Reglamento 1215/2012. Así, el TJUE ha aplicado el art. 7.1 cuando existe un "compromiso libremente asumido por una parte respecto de otra".[45] Además, se debe realizar una interpretación "autónoma" del concepto de "materia contractual", lo que implica que no se puede tener en cuenta lo que se considera como obligación contractual por las diferentes legislaciones nacionales.[46]

Además, no es estrictamente necesario que se haya celebrado un contrato entre las partes para que funcione el foro especial,[47] ya que, además de un contrato expreso, éste puede tener origen en actos tácitos. En este último caso, esto ocurre sólo cuando "se deriva de actos que manifiestan inequívocamente la voluntad de las partes".[48]

Por otro lado, el concepto de "prestación de servicios" no está definido en el Reglamento 1215/2012. Para delimitar su concepto, conviene traer a colación la jurisprudencia del TJUE, con lo que también se debe hacer una calificación autónoma, que implica que no se requiere interpretar el concepto de prestación de servicios de conformidad con el concepto establecido en los tratados de la UE.[49] El TJUE ha considerado que el concepto de prestación de servicios implica, como mínimo, que quien los presta realiza una determinada actividad a cambio de una remuneración.[50] En el caso de las PIV, el elemento remunerativo está presente cuando un usuario realiza un contrato de suscripción con la plataforma, y en estos casos, el contrato puede caracterizarse como un contrato de

---

44. P. Torremans, U. Grušić, C. Heinze, L. Merrett, A. Mills, C. Otero García-Castrillón, Z. Tang, K. Trimmings, L. Walker (2022). *Cheshire, North & Fawcett: Private International Law*. (15 ed. Oxford University Press). p. 245 y siguientes.

45. Sentencia del TJUE de 5 de febrero de 2004, asunto C-265/02, *Frahuil SA v Assitalia SpA*, apartado 24.

46. Sentencia del TJUE de 22 Marzo de 1983, asunto C-34/82, *Martin Peters Bauunternehmung GmbH v Zuid Nederlandse Aannemers Vereniging*.

47. Sentencia del TJUE de 11 de Noviembre de 2020, asunto C-433/19, *Ellmes Property Services Limited v SP,* apartado 36.

48. Sentencia del TJUE de 14 de Julio de 2016, asunto C 196/15, *Granarolo SpA v Ambrosi Emmi France SA*, apartados 24 y 28.

49. Sentencia del TJUE de 23 de abril de 2009, asunto C-533/07, *Falco Privatstiftung and Thomas Rabitsch v Gisela Weller-Lindhorst*, apartado 34.

50. Sentencia del TJUE de 23 de abril de 2009, *Falco Privatstiftung and Thomas Rabitsch v Gisela Weller-Lindhorst*, apartado 29.

prestación de servicios. Cuando no existe suscripción, ni existe pago alguno, se debe analizar si se puede calificar como contrato de prestación de servicios.

El primer criterio de la definición consagrada por el tribunal es la existencia de una "actividad", que requiere la realización de actos positivos, y no meras omisiones.[51] Este criterio se corresponde, en el caso de un contrato realizado con una PIV, con el servicio característico que brinda la plataforma, ofreciendo a los usuarios acceso a la plataforma, así como cargar contenidos, compartirlos, verlos, escucharlos, darles me gusta y comentarlos. En cuanto al segundo criterio, a saber, la "remuneración", como contraprestación por la actividad, esta no debe entenderse estrictamente como el pago de una suma de dinero.[52] Así, cuando el modelo de negocio de la plataforma se base en la publicidad, también cabe considerar que se cumple este criterio. Por lo tanto, aun cuando no exista suscripción o pago involucrado, el contrato entre un usuario y una PIV también se calificará como "prestación de servicios".[53]

Adicionalmente, el lugar de cumplimiento de la obligación característica debe estar determinado por lo que las partes hayan establecido, generalmente en las condiciones generales del contrato suscrito con la PIV. Sin embargo, puede ocurrir que en el contrato no se mencione el lugar de cumplimiento, por lo que éste deberá determinarse a través del lugar de prestación de los servicios,[54] aspecto que, según mi criterio, debe conducir al domicilio del usuario.

5. EL FORO DE CONSUMO Y LAS PLATAFORMAS DE INTERCAMBIO DE VÍDEOS (PIV)

El Reglamento UE 1215/2012 protege a un usuario de PIV cuando éste se caracteriza como consumidor. Esta protección se da en relación con la determinación de los foros competentes, mediante los cuales los consumidores pueden

---

51. Sentencia del TJUE de 19 de diciembre de 2013, asunto C-9/12, *Corman-Collins SA v La Maison du Whisky SA*, apartado 38; Sentencia del TJUE de 23 de abril de 2009, asunto C-533/07, *Falco Privatstiftung and Thomas Rabitsch v Gisela Weller-Lindhorst*, apartados 29 a 31.

52. Ello sería una restricción que no está prevista en el art. 7.1.b. Sentencia del TJUE de 19 de diciembre de 2013, asunto C-9/12, *Corman-Collins SA v La Maison du Whisky SA*, apartados 39-40.

53. El TJUE ha considerado como una prestación de servicios comprendida en la norma del art. 7.1.b), un contrato de agencia (Sentencia del TJUE de 11 de marzo de 2010, asunto C-19/09, *Wood Floor Solutions Andreas Domberger GmbH contra Silva Trade SA*, apartado 29) y un contrato de distribución (Sentencia del TJUE de 19 de diciembre de 2013, asunto C-9/12, *Corman-Collins SA v La Maison du Whisky SA*), un contrato de préstamo entre una entidad de crédito y dos deudores solidarios (Sentencia del TJUE de 15 de junio de 2017, asunto C-249/16, *Saale Kareda contra Stefan Benkö*, apartado 38), o los servicios prestados por el administrador de una empresa (Sentencia del TJUE de 10 de septiembre de 2015, asunto C-47/14, *Holterman Ferbo Exploitatie BV y otros contra Friedrich Leopold Freiherr Spies von Büllesheim*, apartado 58).

54. En el caso de la entrega material de bienes, Sentencia del TJUE de 25 de febrero de 2010, asunto C-381/08, *Car Trim GmbH contra KeySafety Systems Srl.*, apartado 62.

optar por interponer acciones judiciales contra la entidad que gestiona la PIV, ya sea ante los tribunales del Estado miembro donde está domiciliado el consumidor o del Estado en el que está domiciliado el prestador.[55] Como hemos visto, el Reglamento 1215/2012 también protege al consumidor estableciendo unas limitaciones a la autonomía de las partes en cuanto a la posibilidad de establecer pactos de sumisión.[56] Finalmente, el Reglamento 1215/2012 establece unas normas específicas en materia de reconocimiento y ejecución.[57]

Es interesante observar que el Reglamento 1215/2012 protege a los consumidores que tienen una relación contractual con una plataforma ubicada no solo en la UE sino también con plataformas ubicadas fuera de la UE.[58] Esta extensión del alcance de aplicación es relevante ya que algunas PIV pueden realizar sus servicios desde fuera de la UE.[59] Sin embargo, no se puede considerar que el lugar de la tecnología que distribuye el contenido de la plataforma digital cumpla con el concepto de "otro establecimiento", ya que no cumple con el principio de previsibilidad y seguridad jurídica que deben sustentar las reglas de competencia judicial internacional,[60] ya que la ubicación del sistema mediante el cual se prestan estos servicios es difícilmente predecible.

Para que se apliquen las normas de protección al consumidor del Reglamento 1215/2012 es necesario el cumplimiento de tres requisitos acumulativos: que exista contrato; que este contrato se realice entre una persona caracterizada como consumidor y otra persona física o jurídica caracterizada como comerciante o profesional, y que el contrato pertenezca a una de las categorías del art. 17.1a-c; en concreto, que exista una conexión territorial con el territorio del consumidor.[61]

En efecto, es necesario que exista un "contrato celebrado por una persona (…) para un uso que pueda considerarse ajeno a su actividad profesional". La jurisprudencia tradicional del TJUE se ha centrado en la transacción en cuestión, en que exista un contrato en la relación y que este contrato se haya celebrado, "con el fin de satisfacer las necesidades propias de un individuo en materia de

55. Art. 18 Reglamento 1215/2012.

56. Art 19 Reglamento 1215/2012.

57. Art. 45.1.e Reglamento 1215/2012.

58. El art. 18 afirma "con independencia del domicilio de la otra parte (…)."

59. Además, la regla del art. 17.2. Reglamento 1215/2012 añade la regla que ante un profesional no domiciliado en un Estado miembro pero con sucursal o establecimiento en un Estado miembro, se considerará para todos los litigios relativos a su explotación que está domiciliado en aquel Estado miembro.

60. Considerandos 15 y 16 Reglamento 1215/2012.

61. F. J. Garcimartín Alférez (2021). Derecho internacional privado (6a ed., Thomson Reuters), apartado 7.14; P. Torremans, U. Grušić, C. Heinze, L. Merrett, A. Mills, C. Otero García-Castrillón, Z. Tang, K. Trimmings, L. Walker (2022). *Cheshire, North & Fawcett: Private International Law*. (15 ed. Oxford University Press). p 292; G. Van Calster. (2021). *European Private International Law: Commercial Litigation in the EU* (3ed). Hart Publishing. p 105.

consumo privado".[62] Así, se requiere que este contrato haya sido" celebrado al margen e independientemente de cualquier actividad o finalidad comercial o profesional, presente o futura."[63]

La noción de consumidor debe interpretarse de manera estricta,[64] y sólo los contratos celebrados fuera e independientemente de cualquier actividad o propósito comercial o profesional, con el único fin de satisfacer las propias necesidades de un individuo en términos de consumo privado, están cubiertos por las normas del consumidor.[65] Además, el Tribunal de Justicia ha establecido que una persona sólo puede invocar las normas en materia de consumo cuando un contrato tiene por objeto un uso en parte profesional y en parte privado, cuando el vínculo entre el contrato y el comercio o la profesión es tan leve que sea marginal.[66] Por tanto, una persona influenciadora que utilice una PIV tanto para su uso personal como profesional, sólo podrá ser considerado consumidor cuando la finalidad profesional del contrato realizado sea insignificante.

Además, de la jurisprudencia del TJUE se puede concluir que en determinados casos un consumidor puede perder su consideración de consumidor, aspecto que podría suceder cuando el uso predominantemente no profesional de aquellos servicios, para los cuales la persona inicialmente celebró un contrato, se convierta posteriormente en un uso predominantemente profesional.[67] En mi opinión, una persona podría perder su condición de consumidor si hubiera ofrecido sus servicios como servicios de pago, o declarase oficialmente dicha actividad.[68]

El TJUE ha establecido que sólo pueden tenerse en cuenta elementos objetivos, en particular el contrato firmado entre las partes, para determinar si dicho contrato se destina a un uso ajeno a su actividad profesional.[69] Según el tribunal, en aras de la previsibilidad no se puede tener en cuenta una prueba subjetiva y, por lo tanto, factores como el conocimiento o la experiencia en un campo

62. Sentencia del TJUE de 3 de julio de 1997, asunto C-464/01, *Francesco Benincasa contra Dentalkit Srl*, apartado 17.

63. Ibid, para. 18.

64. Sentencia del TJUE de 20 de enero de 2005, asunto C-4614/01, *Johann Gruber contra Bay Wa AG*., apartado 16; Sentencia del TJUE de 25 de enero de 2018, asunto C-498/16, *Maximilian Schrems contra Facebook Ireland Limited*, apartado 36.

65. Sentencia del TJUE de 25 de enero de 2018, asunto 498/16, *Maximilian Schrems contra Facebook Ireland Limited*, apartado 30.

66. Sentencia del TJUE de 20 de enero de 2005, asunto C-4614/01, *Johann Gruber contra Bay Wa AG*, apartado 39; Sentencia del TJUE de 25 de enero de 2018, asunto 498/16, *Maximilian Schrems contra Facebook Ireland Limited*, apartado 32.

67. Sentencia del TJUE de 25 de enero de 2018, asunto 498/16, *Maximilian Schrems contra Facebook Ireland Limited*, apartados 33 y 38. También, Sentencia TJUE de 3 de Octubre de 2019, asunto C-208/18, *Jana Petruchová v FIBO Group Holdings Limited,* apartado 54.

68. Sentencia TJUE de 10 de diciembre de 2020, asunto C-774/19, *A. B. and B. B. v Personal Exchange International Limited*, apartados 39, 50.

69. Sentencia TJUE de 3 de Octubre de 2019, asunto C-208/18, *Jana Petruchová v FIBO Group Holdings Limited*, apartado 54.

particular,[70] el valor de las transacciones realizadas en virtud de dicho contrato, el alcance de los riesgos de las pérdidas financieras asociadas a la celebración de tales contratos, o la conducta activa de la persona en relación con tales transacciones son, como tales, en principio irrelevantes.[71]

Algunos casos recientes tramitados por el TJUE han demostrado que esta interpretación rígida comporta como consecuencia ampliar el concepto de consumidor, quizás de forma excesiva.[72] Así, podría decirse que tal interpretación va en contra de la naturaleza misma de las disposiciones especiales de los contratos de consumo, que deben interpretarse restrictivamente ya que se apartan de la regla general del domicilio del demandado.

Para analizar en qué casos los usuarios de una PIV pueden ser calificados como consumidores a los efectos del Reglamento 1215/2021, conviene detenerse casuísticamente en la concreta relación jurídica. Así, hay algunas plataformas que requieren que los usuarios paguen para poder subir vídeos. Por ejemplo, Muvi Flex o Wistia son ejemplos de PIV, que además de funcionalidades relacionadas con herramientas de edición y gestión, emplean una "funcionalidad esencial" dedicada a compartir vídeos, que se puede adquirir a cambio de una contraprestación económica.[73] Además, también hay PIV que son gratuitas, por ejemplo, YouTube o Tik-Tok.[74]

Cuando un usuario paga a una plataforma por los servicios realizados por las PIV en que no se diferencia entre cuenta profesional y personal, corresponde al contrato proporcionar información sobre la calificación de la relación. Además, algunas PIV ofrecen a los usuarios la opción de crear una cuenta como usuario profesional o usuario personal. Por ejemplo, muchas personas influenciadoras optan por una cuenta profesional, ya que ello les proporciona unas capacidades técnicas adicionales que pueden ayudar a aumentar su audiencia.

Así las cosas, si un usuario se registra para obtener una cuenta profesional, es evidente que no puede invocar las normas de protección del consumidor. Ello también se aplicaría si un usuario se hubiese registrado con una cuenta profesional, aunque su propósito real estuviera fuera de su oficio o profesión. Por ejemplo, un músico aficionado que se registrase con una cuenta profesional no debería ser calificado como consumidor, a no ser que proporcionara una evidencia objetiva. Por el contrario, si un usuario se registrase con una cuenta personal, podría reclamar la condición de consumidor y aplicársele las normas pertinentes de consumo.

---

70. Sentencia del TJUE de 25 de enero de 2018, asunto C-498/16, *Maximilian Schrems contra Facebook Ireland Limited*, apartado 39.

71. Sentencia TJUE de 3 de Octubre de 2019, asunto C-208/18, *Jana Petruchová v FIBO Group Holdings Limited*, apartado 59.

72. Sentencia TJUE de 10 de diciembre de 2020, asunto C-774/19, *A. B. and B. B. v Personal Exchange International Limited*; Sentencia TJUE de 3 de Octubre de 2019, asunto C-208/18, *Jana Petruchová v FIBO Group Holdings Limited*.

73. https://muvi.com/flex, https://wistia.com/.

74. https://www.youtube.com/ https://www.tiktok.com/en/

En algunos casos, un usuario puede registrarse con una cuenta personal con una finalidad tanto profesional como personal. Por ejemplo, un músico puede utilizar su cuenta tanto por motivos profesionales como personales. En tales casos, las normas de protección del consumidor se aplican sólo cuando el vínculo entre el contrato y la profesión u oficio es marginal. En este sentido, el hecho de que el usuario gane dinero con la actividad no es relevante. Finalmente, conviene determinar que los contratos celebrados entre consumidores no están protegidos ya que no hay actividad económica involucrada y no hay desequilibrio de poder entre las partes.[75]

Además, una persona que realice un contrato con una PIV será considerada consumidor, en el sentido del Reglamento 1215/2012, siempre que se cumpla la conexión territorial del art. 17.1.c del Reglamento. Según el TJUE, el criterio de la dirección de actividades se cumple cuando existen elementos indicativos de la misma, como el uso de nombres de dominio de primer nivel o la mención de una clientela internacional, pruebas que deberán ser tenidas en cuenta por el tribunal nacional.[76]

De hecho, la prueba de la dirección de actividades debe adaptarse a las particularidades de las PIV, y cuando se analizan las actividades de dichas plataformas en Internet, varias cuestiones deben tenerse en consideración. Ahora bien, conviene tener en cuenta que el criterio de la dirección de actividades demuestra que una página web tiene suficientes contactos con el foro, pero no necesariamente indica que ese foro sea el más apropiado o el que esté más estrechamente relacionado con una disputa.[77]

Un aspecto importante para considerar es si el hecho de que una PIV no bloque geográficamente a un usuario de un determinado territorio, ello implica que se cumple la prueba de la dirección de actividades. Así, el bloqueo geográfico impide que los usuarios accedan a plataformas disponibles en otros países.[78] Algunos proveedores de PIV no requieren la dirección de facturación o la dirección del suscriptor al crear una cuenta; en muchos casos la plataforma automáticamente geolocaliza al usuario y le asigna la cuenta a un país determinado. Claramente, esta PIV dirige sus actividades al país en el que se encuentra dicho usuario. Si dicho usuario accede a su cuenta desde otro país de la UE, la

---

75. G. Van Calster. (2021). *European Private International Law: Commercial Litigation in the EU* (3ed). Hart Publishing. p. 108.

76. Sentencia del TJUE (Gran Sala) de 7 de diciembre de 2010, asuntos acumulados C-585/08 and C-144/09, *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller*, apartados 83 y 93.

77. Université de Genève. (2015). *Geneva Internet Disputes Resolution Policies 1.0* https://www.digitallawcenter.ch/en/research/2020/geneva-internet-disputes-resolution-policies-10-gidrp-10 (último acceso, junio 2024).

78. Algunas investigaciones muestran que este es especialmente el caso de las pequeñas plataformas OTT, donde las plataformas transfronterizas de vídeo bajo demanda caen a cifras muy bajas. A. Broocks, N. Duch-Brown, E. Gómez-Herrera, and B. Martens. (2020). *JRC Technical Report, JRC Digital Economy Working Paper 2020-01. Geo-Blocking: A Literature Review and New Evidence in Online Audio-Visual Services*. European Commission. p 14 et seq.

plataforma geolocalizará automáticamente el ordenador, si bien en ocasiones, tras un periodo temporal le conducirá a un nuevo catálogo.[79] Por lo tanto, este sistema cumple con el Reglamento UE 2017/1128, según el cual las plataformas garantizarán la portabilidad de los servicios en línea, lo que implica que los suscriptores de servicios en línea basados en su Estado miembro de residencia deben poder utilizar estos servicios cuando estén temporalmente presentes en otro Estado miembro.[80]

Algunas PIV pueden optar por segmentar geográficamente el mercado por motivos comerciales. Por lo tanto, es posible que a un consumidor de un país no se le permita acceder a un catálogo particular de una PIV disponible en otro país de la UE.[81] En efecto, las PIV pueden conservar estas políticas de bloqueo geográfico, ya que los servicios audiovisuales están excluidos del ámbito de aplicación del Reglamento de la UE 2018/302, [82] que expresamente prohíbe el hecho que la geolocalización pueda comportar como consecuencia el criterio de focalización.[83]

La interpretación actual relativa a la dirección de las actividades requiere de un análisis casuístico. Está ampliamente aceptado que la mera accesibilidad no es suficiente para cumplir con la prueba de la dirección de actividades.[84] Sin embargo, sostengo que la dirección de actividades debe interpretarse ampliamente cuando se refiere a la actividad de las PIV globales. Dado que las PIV pueden geolocalizar a los usuarios por su ubicación y pueden geobloquear a los usuarios de ciertos países, se puede argumentar que cuando estas plataformas no geobloquean a los usuarios de un país de la UE en particular, se dirigen a

79. YouTube tiene muchas versiones localizadas de la plataforma, lo que facilita a los usuarios descubrir contenido relevante para su región. En consecuencia, los vídeos de tendencia en EE. UU. pueden diferir de los vídeos accesibles en España o el Reino Unido.

80. Art 1 del Reglamento (UE) 2017/1128 del Parlamento Europeo y del Consejo, de 14 de junio de 2017, relativo a la portabilidad transfronteriza de los servicios de contenidos en línea en el mercado interior. DO L 168 de 30/06/2017, p. 1-11.

81. Ibid.

82. Art. 1.3 del Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, de 28 de febrero de 2018, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) n.° 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE (Texto pertinente a efectos del EEE) DO L 60I de 2.3.2018, p. 1–15. El artículo 1.6

83. En efecto, el art. 1.6 de dicho Reglamento establece que: "El presente Reglamento se entenderá sin perjuicio del Derecho de la Unión relativo a la cooperación judicial en materia civil. Del cumplimiento del presente Reglamento no se derivará que un comerciante dirige sus actividades al Estado miembro de residencia habitual o domicilio del consumidor en el sentido del artículo 6, apartado 1, letra b), del Reglamento (CE) n.o 593/2008 y del artículo 17, apartado 1, letra c), del Reglamento (UE) n.o 1215/2012." Art. 1.6 del Reglamento (UE) 2018/302.

84. Sentencia del TJUE (Gran Sala) de 7 de diciembre de 2010, asuntos acumulados C-585/08 and C-144/09, *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller*, apartados 93-94.

los consumidores ubicados allí. Adicionalmente, se podrán considerar otros elementos indicativos respecto de la actividad prevista por la PIV.

6. CONCLUSIONES

En este capítulo se ha analizado una serie de cuestiones relativas a las plataformas de intercambio de vídeos (PIV). Así, se parte del concepto de PIV de la Directiva 2018/1808 y la Ley 13/2022, de 7 de julio, que transpone la Directiva al ordenamiento interno español, disposiciones que exigen que los proveedores de PIV cumplan una serie de obligaciones. La característica esencial de estas plataformas es la ausencia de responsabilidad editorial del contenido mostrado en las mismas.

En la actualidad, existen conflictos en los que las PIV están involucradas, y que la jurisprudencia nacional está resolviendo. Algunos de estos conflictos se refieren a las personas influenciadoras, las cuales a través de las PIV muestran productos o servicios sin tener en cuenta las normas de publicidad. También existen conflictos relacionados con las infracciones de contratos publicitarios y de derechos de autor.

Desde el prisma de las PIV, este capítulo ha analizado los acuerdos de sumisión de foro, el foro contractual de la prestación de servicios y el foro del contrato de consumo. Para ello, se analiza los artículos específicos del Reglamento 1215/2012 así como la jurisprudencia del TJUE.

Por lo que se refiere a la autonomía de la voluntad, la jurisprudencia del TJUE en los asuntos *Jaouad El Majdoub* y *Tilman y Unilever* se aplica a los acuerdos de sumisión contenidos en las PIV, ya que las cláusulas de sumisión suelen incluirse en textos de condiciones generales accesibles mediante un clic o mediante un hiperenlace. Conviene tener en cuenta la calificación de contratos de consumo y los límites a la autonomía de la voluntad del Reglamento 1215/2012.

Por lo que se refiere al foro contractual del art. 7.1 del Reglamento 1215/2012, los servicios prestados por las PIV deben ser calificados como contratos de prestación de servicios, de acuerdo con la jurisprudencia del TJUE, ya que prestan una actividad (acceso a la plataforma, cargar contenidos, compartir, comentar, entre otros aspectos) a cambio de una remuneración. Este segundo elemento se da también cuando el servicio se ofrece gratuitamente ya que el modelo de negocio basado en la publicidad también debe considerarse como remuneración. El lugar de cumplimiento de la prestación de servicios debe determinarse en el contrato y a falta de ello, debe entenderse como el domicilio del usuario.

Por lo que respecta al foro de consumo en el marco del Reglamento 1215/2012, éste protege a los consumidores que establecen una relación contractual con una PIV ubicada en un Estado miembro de la UE, si bien también con PIV ubicadas fuera de la UE, aspecto relevante cuando pueden existir plataformas que accedan al mercado europeo desde algún Estado no comunitario.

El ámbito de los contratos de consumo exige una interpretación casuística, en el que los usuarios de una PIV pueden ser considerados consumidores si el uso de esta es ajeno a su actividad profesional. Para ello, es determinante el hecho que el usuario se haya registrado con una cuenta profesional o personal. Por lo que se refiere a la vinculación territorial al territorio del consumidor, se defiende una interpretación extensiva del criterio de dirección de actividades, protectora de los consumidores, en que cuando el prestador de una PIV no geobloquee a los consumidores de un determinado Estado de la UE, ello comporte el cumplimiento del concepto de la dirección de actividades.

BIBLIOGRAFÍA

AHMED, M. (2024). CoL.net: Who is bound by Choice of Court Agreements in Bills of Lading?. *ConflictsofLaws.net*. https://conflictoflaws.net/2024/who-is-bound-by-choice-of-court-agreements-in-bills-of-lading/

BBC News. (2023). *TikTok fined 345 million euros over handling children's data in Europe*. https://www.bbc.com/news/technology-62800884.

BROOCKS, A. DUCH-BROWN, N. GÓMEZ-HERRERA, E. Y MARTENS, B. (2020). *JRC Technical Report, JRC Digital Economy Working Paper 2020-01. Geo-Blocking: A Literature Review and New Evidence in Online Audio-Visual Services.* European Commission.

CODAGNONE, C; LIVA, G; RODRÍGUEZ DE LAS HERAS BALLELL, T. (2022). *Identification and Assessment of Existing and Draft EU Legislation in the Digital Field*. European Parliament. Policy Department for Economic, Scientific and Quality of Life Policies.

European Commission. (2016). *Special Eurobarometer 447. Report on Online Platforms*.

European Advertising Standards Alliance (EASA). (2023). *Best Practice Recommendation on Influencer Marketing Guidance*.

GÁLVEZ JIMÉNEZ, A., & GARCÍA ESCOBAR, G. A. (2023). *Derecho de la publicidad en Internet: redes sociales y plataformas digitales* (1.ª ed.). Aranzadi.

GARCIMARTÍN ALFÉREZ, F,. J. (2021). Derecho Internacional Privado (6ª ed). Thomson Reuters.

GOANTA, C., & ORTOLANI, P. (2022). Unpacking content moderation: The rise of social media platforms as online civil courts. In X. Kramer, J. Hoevenaars, B. Kas, & E. Themeli (Eds.), *Frontiers in Civil Justice: Privatisation, Monetisation and Digitisation* (pp. 192-216). Edward Elgar Publishing. https://doi.org/10.4337/9781802203820.00017.

ICC. (2018). *Advertising and Marketing Communications Code*.

ICPEN (2016). *ICPEN Guidelines for digital influencers*.

Le Monde. (2023). *Une plainte déposée contre des influenceurs pour escroquerie et abus de confiance*. https://www.lemonde.fr/police-justice/article/2023/01/23/une-plainte-deposee-contre-des-influenceurs-pour-escroquerie-et-abus-de-confiance_6158970_1653578.html

LUTZI, T. (2017). Internet cases in EU Private International Law—Developing a Coherent Approach. *66 International and Comparative Law Quarterly 687*.

Ministère de l'Économie, des Finances et de la Relance. (2021). *Communiqué de presse: Nabilla Benattia Vergara condamnée pour publicité trompeuse*. https://www.economie.gouv.fr/files/files/directions_services/dgccrf/presse/communique/2021/cp-nabilla-benattia-vergara.pdf?v=1630408421

KUKLIŠ, Ľ. (2019). Video-Sharing Platforms In AVMSD – A New Kind Of Content Regulation. En P. L. Parcu & E. Brogi (Eds.), *Research Handbook on EU Media Law and Policy* (pp. 303-325). Edward Elgar Publishing.

ORTIZ-OSPINA, E (2019), *The rise of social media*, https://ourworldindata.org/rise-of-social-media.

Parlamento Europeo. (2017). *Report on online platforms and the digital single market*. (2016/2276(INI)).

PRETELLI, I. (2021). Protecting Digital Platform Users by Means of Private International Law. *13 Cuadernos de Derecho Transnacional 574*.

RODRÍGUEZ DE LAS HERAS BALLELL, T. (2021). The background of the Digital Services Act: looking towards a platform economy. *ERA Forum* 22(1). (pp. 75-86).

STATISTA. (2024). *Most popular social networks worldwide as of April 2024, ranked by number of monthly active users*. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

TORREMANS, P, GRUŠIĆ, U, HEINZE, C, MERRETT, L, MILLS, A, OTERO GARCÍA-CASTRILLÓN, C, TANG, Z, TRIMMINGS, K, WALKER, L. (2022). *Cheshire, North & Fawcett: Private International Law*. (15 ed. Oxford University Press).

VALCKE, P. & I. LAMBRECHT, I. (2021). The evolving scope of application of the AVMS Directive. En Parcu, P. L., & Brogi, E. (Eds.), *Research handbook on EU media law and policy*. Edward Elgar Publishing Limited. (pp. 282-302).

VAN CALSTER, G. (2021). *European Private International Law: Commercial Litigation in the EU* (3ed). Hart Publishing.

Vimeo Help Center. (2021). *A Comprehensive Guide: What Content You Can Upload to Vimeo' (Vimeo Help Center)* https://help.vimeo.com/hc/en-us/articles/16413647508753-A-Comprehensive-Guide-What-Content-You-Can-Upload-to-Vimeo.

Tik-Tok. (2023). *Términos de Servicio*. https://www.tiktok.com/legal/page/eea/terms-of-service/es.

Université de Genève. (2015). *Geneva Internet Disputes Resolution Policies 1.0* https://www.digitallawcenter.ch/en/research/2020/geneva-internet-disputes-resolution-policies-10-gidrp-10.

SEGUNDA PARTE

La empresa y sus relaciones con terceros

I. Empresa y responsabilidad

La transferencia internacional de datos personales a Estados Unidos: el "Transatlantic Clash" de dos culturas de privacidad

Josep Cañabate Pérez
Profesor agregado de Historia del Derecho
Universitat Autònoma de Barcelona

ABSTRACT:
The main objective of this chapter is to analyze the controversial legal regime of personal data transfers to the United States. Using the comparative law methodology, the concept of U.S. privacy is studied to determine the reasons that lead the EU to consider that it does not have an adequate level of protection. On the other hand, it focuses on the EU-US Data Privacy Framework, an instrument to guarantee the processing of Europeans' personal data by American organizations that adhere to it, which is preceded by a series of agreements annulled by the EU judiciary.

Keywords: International data transfer, privacy, Data Privacy Framework, personal data protection.

Palabras clave: Transferencia internacional de datos, privacy, Data Privacy Framework, protección de datos personales.

1. INTRODUCCIÓN

El 10 de julio de 2023 la Comisión Europea aprobó la decisión de adecuación para posibilitar la transferencia de datos personales entre entidades de la Unión Europea y de los Estados Unidos bajo el denominado *EU-US Data Privacy Framework*[1]. Este nuevo instrumento supone el último, y a buen seguro no definitivo acto, del choque jurídico entre dos modelos de poderes digitales, el *market-driven* de los EEUU y el *rights-driven* de la UE, descritos por Anu Bradford en su reciente obra *Digital Empires: The Global Battle to Regulate Technology* (Bradford, 2023).

El Tribunal de Justicia de la Unión Europea (TJUE en adelante) en su sentencia de 16 de julio de 2020 en el asunto C-311/18, *Data Protection Commissioner* contra Facebook Ireland Limited y Maximillian Schrems (Schrems II en adelante) había invalidado la Decisión de ejecución de la comisión 2016/1250 sobre el flujo de datos transatlántico, el Escudo de Privacidad UE-EEUU (*Privacy Shield*). El alto tribunal europeo consideró que las limitaciones de protección de datos personales derivadas de la legislación nacional de los Estados Unidos sobre el acceso y el uso de datos transferidos de la UE al país norteamericano por parte de las autoridades estadounidenses no satisfacía los requisitos esenciales equivalentes al derecho de la Unión en relación con la necesidad y proporcionalidad. El tribunal señaló también la inexistencia de un órgano de garantía al cual pudieran dirigirse los ciudadanos europeos para presentar sus reclamaciones sobre posibles vulneraciones de su protección de datos por parte de las agencias de inteligencia norteamericanas tal como establece el artículo 47 de la Carta sobre el derecho a recurso efectivo.

Tras la nueva anulación por parte del TJUE del marco jurídico para la transferencia de datos personales a los Estados Unidos se iniciaron conversaciones entre las autoridades de este país y la Comisión (UE) para poder elaborar una nueva decisión que cumpliese con los requisitos establecidos en el apartado 2

1. Las normas sobre transferencias de datos personales de los responsables o encargados del tratamiento en la Unión a terceros países y organizaciones se establecen en el capítulo V del RGPD.

del articulo 45 del Reglamento (UE) 2016/679[2]. Esta norma establece que la adopción de una decisión de adecuación debe basarse en un análisis exhaustivo del ordenamiento jurídico del tercer país, que abarque tanto las normas aplicables a los importadores de datos, así como las limitaciones y salvaguardias en materia de acceso a datos personales por parte de las autoridades públicas. En su evaluación, la Comisión debe determinar si el tercer país en cuestión garantiza un nivel de protección "esencialmente equivalente" al garantizado dentro de la Unión (considerando 104 del Reglamento (UE) 2016/679).

El Tribunal de Justicia de la Unión Europea ya había señalado en su conocida sentencia de 6 de octubre de 2015 en el asunto C-362/14, Maximiliam Schrems (Schrems I, en adelante) contra *Data Protection Commissioner* de Irlanda que no se requiere encontrar un nivel de protección idénticos. En este sentido, los medios a los que recurre el tercer estado para proteger los datos personales pueden diferir de los empleados en la Unión, siempre que resulten en la práctica eficaces para garantizar un nivel adecuado de protección.

El objetivo principal de este capítulo es analizar el ordenamiento jurídico de los Estados Unidos en lo referente a la privacidad a luz de los principios y estándares jurídicos de la UE para establecer si el *Data Privacy Framework* supone un instrumento adecuado de protección que colme la brecha jurídica entre los modelos que señala la mencionada autora, Anu Bradford. La hipótesis es que el *DPF* es una huida hacia adelante, pues la economía digital transatlántica no se puede detener, pero a pesar de las mejoras se está lejos de lograr un régimen de protección equivalente.

Para desarrollar el objetivo mencionado en la primera parte se realiza un análisis del concepto de *Data Privacy* en los Estados Unidos, en la segunda parte se lleva a cabo un estudio del EU-US *Data Privacy Framework*.

2. DATA PRIVACY AMERICANA VERSUS PRIVACIDAD Y PROTECCIÓN DE DATOS EUROPEA

La *privacy* es uno de los pilares de la cultura de derechos y libertades de los Estados Unidos, constituyendo un mecanismo de garantía para el sistema jurídico norteamericano de una importancia comparable, aunque menor, a la libertad de expresión recogida en la Primera Enmienda. Sus efectos jurídicos y las formas en que se manifiesta son múltiples, y en muchas ocasiones no encuentra una figura equivalente en el derecho europeo. Resulta paradójico que, a pesar de las notables diferencias actuales, el concepto original de *privacy* americano haya

2. En el artículo 45, apartado 3, del Reglamento (UE) 2016/679, establece que la Comisión podrá decidir mediante un acto de ejecución, que un tercer país, un territorio o uno o más sectores específicos dentro de un tercer país garanticen un nivel adecuado de protección. En esta condición, las transferencias de datos personales a un tercer país podrán tener lugar sin necesidad de obtener ninguna autorización adicional, según lo previsto en el artículo 45, apartado 1, y el considerando 103 del Reglamento (UE) 2016/679.

tenido una decisiva influencia en la creación y desarrollo de la privacidad y la protección de datos en los países de *civil law*. No solo el conocido artículo doctrinal de Warren y Brandeis, "The Right to Privacy" (Warren, Brandeis 1890, pp. 193-220)., sino también las primeras leyes sobre *information privacy* en los años 70, han sido importantes referentes en el desarrollo del derecho de la privacidad y protección de datos europeo.

En términos de cultura jurídica no es baladí que sea un artículo doctrinal el que sirva de arranque de un nuevo derecho en el *Common Law,* el cual acabó siendo refrendado por el Tribunal Supremo de los Estados Unidos y constituyendo el *Tort of Disclosure*. Algunos autores norteamericanos consideran que este trabajo académico ha sido el más influyente en la historia del derecho americano[3]. Ciertamente, supone un hito jurídico que unos académicos, en realidad ilustres juristas bostonianos, lograran este enorme impacto. Desde la Europa apegada a las solemnes declaraciones de derechos, o a las convenciones internacionales elaboradas por el restringido y exquisito club de Estados, puede parecer anecdótico. Sin embargo, este proceso de elaboración jurídica muestra como el *Common Law* americano es un derecho dúctil, dinámico y que reacciona ante los retos que le plantea la realidad.

La Europa postrevolucionaria de la codificación tuvo una vocación totalizante en el ámbito jurídico: sin Estado y sin regulación no debía haber derecho. Este fenómeno es denominado por Paolo Grossi como "absolutismo jurídico" (Grossi 1996, pp. 94-99). El liberalismo jurídico europeo abogó por la desaparición del acervo jurídico de Antiguo Régimen o lo arrojó a la marginalidad. El americano, por el contrario, ha recelado tradicionalmente de cualquier intervención del Estado y de sus regulaciones.

Esta concepción tan ontológica del derecho americano sigue vigente en la actualidad a pesar de los retos que supone la transformación digital. Ante la aprobación de legislación federal o estatal sobre protección datos algunos influyentes autores como Jack Balkin, profesor de derecho constitucional en Yale, anteponen el principio de la libertad de discurso recogido en la Primera Enmienda. Este autor sostiene, "[U]no de los desarrollos más importantes en el último cuarto de siglo es el surgimiento de la Primera Enmienda y del principio de libertad de discurso como una de las herramientas anti-regulatorias para los abogados de empresa" (Balkin, 2004, pp. 1-55). Balkin denomina a este fenómeno jurídico como *Second Gilded Age*[4] haciendo una analogía con el momento histórico tras la Guerra de Secesión en el que se impidió la regulación del gobierno

3. Roscoe Pound afirmó sobre que el artículo "[did] nothing less than add a chapter to our law", citado en Alpheus Manson, *Brandeis: a Free Man's Life,* 70 (1946). Harry Kalven lo ha calificado como "[the] most influential law review article of all", *vid*. Kalven (1966), pp. 326-341.

4. La denominada *Gilded Age* (1870-1891) fue un periodo de gran expansión económica, industrial y demográfica que se inició tras la Guerra de Secesión y se extendió durante dos décadas. No obstante, se produjeron grandes desigualdades sociales y económicas, y una alta conflictividad social. En el ámbito jurídico hay que destacar como los tribunales transformaron la ideología de la libertad de trabajo en un principio constitucional de la libertad de contratación que impidió a los gobiernos

de las relaciones de trabajo. La historia del derecho del trabajo en los EEUU muestra como los *Statutes* recogen en muchas ocasiones los avances jurídicos establecidos en la jurisprudencia, mientras que algunas regulaciones acaban marginadas por su no aplicación por los tribunales.

En la Unión Europea estos postulados anti-regulatorios resultan incomprensibles, cuando la norma general y abstracta, como es el RGPD, puede ser un instrumento muy eficaz para proteger a los datos personales de los ciudadanos en todos los ámbitos. Sin embargo, el derecho a la "*information privacy*" estadounidense, tal como se ha apuntado, comprende un amplio cuerpo legal compuesto por *Common Law*, derecho constitucional *Statutory Law* (federal y estatal) y derecho extranjero. Un sistema plural, sectorizado y casuístico que desde la óptica europea puede conllevar a la desprotección.

A continuación, se va a profundizar en los orígenes y tipologías de la privacidad, y su derivada la "*information privacy*" en el sistema jurídico de los Estados Unidos.

2.1. El surgimiento del derecho a la privacidad en el Common Law

En el desarrollo de los *tort remedies* para proteger la privacidad de las vulneraciones procedentes de la tecnología, tal como se ha indicado, fue muy relevante la publicación en 1890 del artículo de Warren y Brandeis[5]. El mismo no solo supone un referente en la historia del derecho de la privacidad, sino que también es alegado por la jurisprudencia actual, como ocurrió en el caso *Kyllo v. United States* en 2001. Los autores de la publicación clásica describieron a la *privacy "[as not] the principle of private property but that of inviolate personality"*. James Whitman relaciona está idea de derecho de personalidad, con el concepto de libertad de la filosofía alemana del siglo XIX. Los autores no basaron su construcción jurídica novedosa en la libertad ante el gobierno, o ante el mercado, sino en la capacidad de desarrollar libremente su potencial como individuo. Warren y Brandeis definieron este nuevo derecho a la privacidad como

regular los salarios y las condiciones de trabajo. Sobre este momento histórico-jurídico *vid.* Les Benedict (1985), pp. 293-331, Forbath (1985), pp. 767-817.

5. Los orígenes de esta sentencia han generado debate académico, *vid.* Barron (1979), pp. 875-922. En todo caso como señala Nieves Saldaña: "[p]or todo, a finales del siglo XIX el suelo constitucional norteamericano estaba ya sembrado de principios heredados de la tradición jurídica inglesa, que recepcionados en el sistema jurídico de las colonias habían alcanzado plasmación constitucional en las Enmiendas ratificadas en 1791 y en las aportaciones de conocidos constitucionalistas. Sin embargo, el gran desarrollo de la prensa y la proliferación de mecanismos de reproducción de imágenes, especialmente gracias a los avances en la fotografía, generalizó que en el último tercio del siglo XIX proliferaran las publicaciones por la prensa sensacionalista de aspectos relativos a la vida privada, frente a los que no podía ejercitarse acción legal alguna en defensa de una supuesta violación de la privacidad." Saldaña Díaz (2012), p. 207.

"*the right to be alone*". Esta idea había sido acuñada por el Juez Thomas Cooley es su tratado sobre el *Law of Torts* (Cooley, 1888, p. 29).

Los autores del ilustre artículo habían puesto de manifiesto como las acciones existentes en el *Common Law* no resultaban adecuadas para proteger la privacidad, pero podían ser modificadas para lograr este objetivo. Esta reivindicación fue atendida en 1903 tanto por los tribunales como por el legislador creando *torts* para proteger la privacidad. En 1903 en Nueva York se creó por ley (*Statute*) un *tort* de privacidad. Georgia, en el caso *Pave v. New England Life Insurance Co*. (1905) fue el primer Estado en reconocer una *common law tort action* para las vulneraciones de la privacidad.

Unas décadas más tarde, en 1960, William Prosser escribió un conocido artículo, *Privacy,* en el cual examinando más de 300 sentencias desde la publicación de Warren y Brandeis, estableciendo el siguiente concepto de privacidad:

> "The law of privacy comprises four distinct kinds of invasion of four different interest of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, "to be let alone". Without any attempt at exact definition, these four torts may be described as follows:
>
> 1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affaires.
> 2. Public disclosure of embarrassing private facts about plaintiff.
> 3. Publicity which places the plaintiff in a false light in the public eye.
> 4. Appropriation, for defendant's advantage, of the plaintiff's name or likeness." (Prosser, 1960, p. 383)

En la taxonomía que hace Prosser del concepto *privacy* se puede observar, tal como el mismo autor señala, cuatro tipologías que responden a conceptos muy diversos. Si tomamos como ejemplo el derecho español, aunque sería muy similar en el resto de los ordenamientos continentales, la revelación de hechos falsos o la suplantación identidad se corresponderían con instituciones tales como la difamación o la apropiación del estado civil. Edward Bloustein, replicando la crítica que hace Prosser cuando alega que no tienen nada en común, sostiene que aquello que une a estas figuras es la protección de la "dignidad humana" y "personalidad" (Bloustein, 1964, pp. 962-1007). Robert Post, por su parte, añade que estas categorías constituyen una forma de respeto por otras personas en el seno de la comunidad (Post,1989, pp. 957-1010).

El *Restatement of Torts*[6] reconoció, y sigue reconociendo en la actualidad, los cuatro *torts* descritos en el artículo de Prosser. Los mismos son denominados

6. En la jurisprudencia estadounidense, *Restatements of the Law* son un conjunto de tratados sobre temas legales que tratan de informar a los magistrados y abogados acerca de los principios generales del *Common Law*.

de forma conjunta como "*invasion of privacy*". Estos *torts* serían: (1) *intrusion upon seclusion,* (2) *public disclosure of private facts*[7]*,* (3) *false light*[8]*,* y (4) *appropriation*. (Solove, Rotenberg, Schwartz, 2005, p. 30)

A los mismos hay que añadir el *Breach of Confidentiality,* que pretende dar una compensación cuando un profesional divulga información confidencial de un paciente o de un cliente. El *Defamation Tort* intenta reparar el daño causado cuando alguien hace manifestaciones falsas sobre una persona que puede llegar a dañarla. El *Infliction of Emotional Distress* es un *Tort* concebido para proteger a aquellas personas víctimas de una conducta abusiva de un tercero que les causa una "angustia emocional severa". Este acoso puede producirse de manera intencionada o de forma imprudente. El *Common Law* también ofrece una protección basada en la *privacy* en el ámbito del derecho que regula las pruebas en el proceso (*evidence law*). Se trataría del privilegio de mantener el secreto de las comunicaciones entre abogado y cliente, el matrimonio, médico y paciente, psicólogo y paciente, etc. (Solove, Rotenberg, Schwartz, 2005, p. 31)

La protección que brinda el *Common Law* al derecho a la propiedad, según algunos autores (Westin, 1967; Murphy, 1996, pp. 2381-2417; Posner, 1981), también sería aplicable a la privacidad. Desde esta óptica los datos personales se consideran como una forma de propiedad. Si la información personal es entendida como una forma de propiedad mueble, el *tort of conversion*[9] sería aplicable a aquellos que recopilan y usan datos personales de manera ilícita. Por último, las políticas de privacidad, así como las condiciones de uso que contengan cláusulas sobre privacidad, pueden ser consideradas de manera análoga a un contrato, cuyo cumplimiento puede ser reivindicado ante un tribunal.

---

7. RESTATEMENT (SECOND) OF TORTS § 652D (1977). The tort of disclosure allows civil liability when the defendant "gives publicity to a matter concerning the private life of another," when the "matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."

8. El concepto de "false light" debe entenderse como una revelación de algún asunto que resulta altamente ofensivo para una persona razonable. A través de la jurisprudencia se ha definido que se entiende por este concepto.

9. Según la definición del Legal Information Institute, "[C]onversion is an intentional tort which occurs when a party takes the chattel property of another with the intent to deprive them of it. Conversion is not applicable to real property. For the purposes of conversion, "intent" merely means the objective to possess the property or exert property rights over it. As a result, a party is liable for conversion regardless of their knowledge of property's ownership status. For example, a person who picks up a necklace off the ground with the intent to resell it because they erroneously believed it was abandoned still converted that necklace. The standard remedy for conversion is return of the property in question or damages for the fair market value of the property." Legal Information Institute, https://www.law.cornell.edu/wex/conversion#:~:text=Conversion%20is%20an%20intentional%20tort,exert%20property%20rights%20over%20it.

2.2. Las restricciones de la Primera Enmienda al derecho a la privacidad

La presión de activistas de la privacidad, de académicos, y de organizaciones de consumidores para que se establezca una regulación equivalente a la europea, aunque sea muy parcialmente, está empezando a dar sus frutos con la normativa californiana o el proyecto de ley federal sobre privacidad de datos (ADPPA). La respuesta de las grandes corporaciones tecnológicas ante estos "movimientos legislativos" es alegar la Primera Enmienda. Su principal argumentación jurídica se basa en considerar como invasiva cualquier regulación invocando a la libertad más central del sistema constitucional estadounidense, la "*freedom of speech*". Eugene Volokh se ha alineado con estos razonamientos, afirmando que muchas leyes de privacidad que regulan la venta y divulgación de información personal son inconstitucionales bajo la Primera Enmienda (Volokh, 2000, pp. 1049-1124). Según este autor, *"[T]he right to information privacy — my right to control your communication of personally identifiable information about me — is a right to have the government stop you from speaking about me.*" (Volokh, 2000, pp. 1051). La afirmación parece muy radical, especialmente si tenemos en cuenta las amplias posibilidades de manipulación de la opinión de los usuarios que han mostrado tener las redes sociales en casos muy críticos para la democracia de los Estados Unidos como es el escándalo de Cambridge Analytica/Facebook.

En *Sorrell v. IMS Health Inc* el Tribunal Supremo de los Estados Unidos anuló la ley estatal de Vermont que tenía como objetivo limitar la comunicación y distribución de datos personales de los médicos. A este Estado de Nueva Inglaterra le preocupaba que las farmacias vendiesen información sobre recetas médicas a compañías de minería de datos, las cuales, a su vez, generaban informes sobre patrones de prescripción de medicamentos que ponían a disposición de las compañías farmacéuticas a cambio de elevadas sumas. La preocupación del gobierno estatal era que permitiendo a estas empresas hacer "*target advertising*" a los médicos se acabase ocasionando que estos prescribiesen los medicamentos más caros.

El Tribunal Supremo sostiene que la normativa aprobada por el Estado de Vermont es inconstitucional porque establece una restricción al acceso de la información y al discurso empleado con fines comerciales, basada en el contenido (*content-based*) y en la persona que emite el discurso (*speaker-based*). La opinión mayoritaria del Juez Kennedy señala que bajo las leyes de Vermont, los farmacéuticos pueden donar o vender esta información a terceros para finalidades científicas, periodísticas u otros propósitos.

El magistrado sostiene que la elaboración, venta y difusión de información personal en forma de datos puede requerir protección en tanto que discurso bajo la Primera Enmienda. No obstante, el juez Kennedy entiende que no es necesario entrar en el fondo del asunto, es decir, si la recopilación de datos estaba desprotegida. El derecho de Vermont, según la opinión de Kennedy, era discriminatorio en el modo en que las personas y las organizaciones pueden

usar datos personales en las comunicaciones basados en la protección de contenido y en la persona que emite el discurso (*content and speaker*). Las restricciones establecidas vulneraron la Primera Enmienda, incluso bajo el test utilizado para el discurso comercial. En este caso, estaría, según este autor, legitimado su uso, incluso la venta a terceros, y no podría establecerse ninguna restricción ya que sería inconstitucional (Balkin, 2016, pp. 1193 y 1194).

Se puede argumentar que los datos cuando son recopilados, explotados, usados y vendidos en masa no son discurso, sino más bien una *commodity*, como puede ser cualquier cereal o mineral para la industria. En *Sorrell* el juez Kennedy se muestra escéptico en entender que el formato en el cual se comunican los datos sea tan decisivo para determinar si estamos ante la protección de la Primera Enmienda. Balkin entiende que en lugar de centrarnos en la forma de la información como datos digitales, es necesario centrarse en la caracterización o la función social (Balkin, 2016, pp. 1193 y 1194). Este autor pone como ejemplo el caso Facebook, tras el caso de Cambridge Analytica bastante desafortunado; el uso de datos de los usuarios de la red social para incitarles a votar se entendería como discurso ideológico, por tanto, protegido por la Primera Enmienda.

Las regulaciones de privacidad deben ser "*content-neutral*" en relación con el tiempo, lugar y modo de expresión. Se entiende por contenido neutral aquellas leyes que se aplican a toda la expresión con independencia del fondo (*substance)* del mensaje. El Tribunal Supremo explica en *Ward v. Rock Against Racism* (1989) que "*the principal inquiry in determining content neutrality, in speech cases generally ... is whether the government has adopted a regulation of speech because of disagreement with the message it conveys*." En definitiva, según está línea jurisprudencial, las normativas federales y estatales de protección de datos deberán respetar al principio de libertad de expresión de la Primera Enmienda protegiendo el dato personal como formato, siendo "*content neutral"* sin que haya ninguna determinación de su contenido.

El profesor Balkin, tal como se había señalado más arriba, aporta una solución jurídica para evitar esta tensión anti-regulatoria a la que denomina como una segunda "*Gilded Age*". Entiende que es necesario regular para preservar los derechos y libertades de los ciudadanos ante las nuevas formas de poder económico y social, tal como se hizo en el momento histórico mencionado. No obstante, se plantea igualmente la imprescindible protección de la libertad de expresión de la Primera Enmienda. Esta otorga restricciones a la responsabilidad procedente del *Tort Law* por la revelación de información ya sea verdadera o falsa. Balkin utiliza el concepto *information fiduciary* como elemento clave para garantizar y proteger a los datos personales de los usuarios de la red (Balkin, 2016, p. 1186). El mismo se basa en que los proveedores de servicios en Internet que recopilan, analizan, usan, venden y distribuyen información personal deben ser considerados como *information fiduciaries* en relación a sus clientes y a los usuarios finales. El ostentar esta posición jurídica conlleva el deber de actuar de manera que no pueda dañar los intereses de las personas sobre las que está llevando a las acciones mencionadas.

El concepto es muy sugerente, ya que sitúa a estas empresas en una clara posición de responsabilidad, y puede conectarse con la idea de un *softlaw* preventivo a través de la autorregulación. No obstante, bajo mi punto de vista, deja muchas zonas de sombra que pueden comportar elevados riesgos. Por tanto, considero que si bien sería interesante incorporar en el derecho de la protección de datos este concepto de los *information fiduciaries*, debería hacerse con un claro marco regulatorio como ocurre en la Unión Europea. El caso Enron con la ley Sarbanes-Oexly de 2002 y su apuesta por elementos de control y auditoria financiera, así como la introducción del *Compliance*, en las empresas cotizadas sería un buen ejemplo.

2.3. El derecho a la privacidad en el derecho constitucional

La Constitución de los Estados Unidos no menciona expresamente a la privacidad, no obstante, a partir de la interpretación jurisprudencial[10] se ha entendido que diversas enmiendas de la norma suprema protegen las diferentes tipologías del derecho a la privacidad. *Griswold v. Connecticut* fue la primera sentencia en la que reconoció el "derecho a la privacidad". En *Griswold* el Tribunal Supremo sostiene que el derecho a la privacidad deriva de las penumbras de las protecciones procedentes de otros derechos constitucionales. El Tribunal usa la Primera, la Tercera, la Cuarta y la Novena enmienda para extraer esta protección. En la resolución del alto tribunal estadounidense se sostiene que cuando se juntan las zonas de penumbra, la Constitución acaba creando una "zona de privacidad"[11].

La Primera Enmienda, la cual hemos visto como límite al derecho a la privacidad, garantiza la libertad de pensamiento, de asociación y el derecho a mantener el anonimato[12]. Se establece la salvaguarda de los ciudadanos de preservar la confidencialidad con relación a su pertenencia a un grupo u organización[13], tal como estableció en *NAACP v. Alabama* (1958) y *Shelton v. Tucker* (1960), teniendo en cuenta que el derecho a la libertad de expresión tiene prevalencia frente a otros derechos como resulta en el supuesto de la privacidad.

La Tercera Enmienda, relativa a la imposibilidad de alojar soldados en las residencias particulares sin el previo consentimiento del propietario, también ha sido utilizada para proteger la privacidad (Martínez Martínez, 2004). En la salva-

10. *Vid*., entre otras: *NAACP v. Alabama*, 357 U.S. 449 (1958); *Shelton v. Tucker*, 364 U.S. 479 (1960); *Buckley v. Valeo*, 424 U.S. 1 (1976); *Fisher v. United States*, 425 U.S. 391 (1976).

11. *Vid*. *Griswold v. Connecticut*, 381 U.S. 479, 484-485 (1965).

12. *Vid*. *McIntyre v. Ohio Election Comm'n*, 514 U. S. 334 (1995).

13. La Primera Enmienda de la Constitución de los Estados Unidos establece el siguiente tenor literal: "El Congreso no hará ley alguna por la que adopte una religión como oficial del Estado o se prohíba practicarla libremente, o que coarte la libertad de palabra o de imprenta, o el derecho del pueblo para reunirse pacíficamente y para pedir al gobierno la reparación de agravios".

guarda que introduce la interpretación actual de la Cuarta Enmienda[14] ante registros arbitrarios (*unreasonable searches and seizures*)[15] efectuados por las autoridades administrativas sin disponer previamente de la debida autorización judicial el tribunal también ha reconocido un derecho a la privacidad. Se considera que la garantía no ampara únicamente a los elementos materiales, sino que también comprende a los datos electrónicos o las grabaciones obtenidas en las vigilancias[16]. En *Olmstead v. United States*[17] (1928) el Tribunal Supremo había sostenido que las escuchas telefónicas no suponían una invasión bajo la Cuarta Enmienda porque no implicaba una intrusión en el domicilio del afectado. Fue justamente Brandeis, entonces juez del Tribunal Supremo, el que manifestó su opinión en contra, argumentado que el interés central protegido por la Cuarta Enmienda no era la propiedad sino "*the right to be alone*". En 1967 en *Katz v. United States* el alto tribunal estableció la interpretación moderna de la Cuarta Enmienda señalando que esta "*protects people, not places*".

La Quinta Enmienda también ha recibido una interpretación para garantizar el derecho de la privacidad en lo relativo a la protección frente a la propia incriminación, así como sobre la protección frente a la facultad de las autoridades gubernamentales de forzar a los afectados a divulgar cierta información personal sobre ellos en contra de su propia voluntad[18]. La Novena Enmienda, posibilita la realización de una interpretación extensiva en favor de aplicar garantías jurídicas sobre la privacidad en todos aquellos supuestos no regulados específicamente en las ocho primeras enmiendas[19].

---

14. La Cuarta Enmienda de la Constitución de los Estados Unidos establece el siguiente tenor literal: "El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas".

15. *Vid*., entre otras: *United States v. Miller*, 425 U.S. 435 (1976).

16. Las garantías jurídicas efectuadas por parte de la Cuarta Enmienda fueron extendidas inicialmente a las conversaciones telefónicas, *vid*. *Katz v. United States*, 389 U.S. 347 (1967), y posteriormente limitado en aquellos supuestos en que el afectado voluntariamente cedía su información personal a terceros, *vid*. *United States v. Miller,* 425 U.S. 435 (1976). En cualquier caso, en la actualidad, la protección de la Cuarta Enmienda también se ha extendido a las comunicaciones electrónicas, en virtud de la Ley Privacidad de las Comunicaciones Electrónicas de 1986. Consultado el 24.05.2022 desde: https://it.ojp.gov/privacyliberty/authorities/statutes/1285; así como a los registros de los datos de ubicación que se generan mediante el uso de los dispositivos móviles, *vid*. *Carpenter v. United States,* 585 U.S. 84 (2018). Adicionalmente, *vid*., entre otras: *Olmstead v. United States*, 277 U.S. 438 (1928); *Goldman v. United States*, 316 U.S. 129 (1942); *Kyllo v. United States*, 533 U.S. 27 (2001).

17. En el presente caso, el Tribunal Supremo de los Estados Unidos consideró que la Cuarta Enmienda no resultaba de aplicación sobre las intervenciones telefónicas por no implicar intromisión en la propiedad privada del hogar. Posteriormente, el Congreso daría luz verde la Sección 605 de la *Federal Communications Act* de 1934, que protegía el contenido de dichas comunicaciones mediante previa autorización, así como imponiendo la obligación de no revelar a terceros el contenido de estas.

18. *Vid*. *Boyd v. United States*, 116 U.S. 616, 630 (1886); *Gouled v. United States*, 255 U.S. 298 (1921).

19. *Vid*. *Griswold v. Connecticut*, 381 U.S. 479, 484-485 (1965).

Por último, en el concepto de libertad sustantiva previsto en la cláusula del debido proceso legal (*due process of law*)[20] de la Decimocuarta Enmienda hallamos una interpretación de la *Information Privacy*. En la *concurring opinion* de *Griswold v. Connecticut* el juez Harlan estableció un derecho de la privacidad derivado de la mencionada enmienda. El juez del Supremo reprodujo su *dissenting opinion* de *Poe v. Ullman* (1961): *"I consider that this Connecticut legislation, as construed to apply to these appellants, violates the Fourteenth Amendment. I believe that a statute making it a criminal offense for married couples to use contraceptives is an intolerable and unjustifiable invasion of privacy in the conduct of the most intimate concerns of an individual's personal life*." A partir del último tercio del siglo XX, la jurisprudencia menor[21] ha tomado esta interpretación de la Catorceava Enmienda como fundamento para considerar que el derecho a la privacidad informativa (*informational privacy*)[22] ostenta rango constitucional. Sin embargo, la totalidad de los Tribunales de Circuito no se han mostrado favorables a acoger el contenido de dicha interpretación[23], así como tampoco el Tribunal Supremo de los Estados Unidos se ha pronunciado sobre el alcance constitucional de este derecho, a pesar de las numerosas críticas que ha

20. La cláusula de la Decimocuarta Enmienda que garantiza que ningún Estado "privará a ninguna persona de vida, libertad o propiedad, sin el debido proceso legal". El Tribunal Supremo de los Estados Unidos ha interpretado la cláusula del debido proceso para establecer la "incorporación selectiva" de enmiendas en los Estados, lo que significa que ni los Estados ni el propio gobierno federal pueden limitar los derechos individuales previstos por la Constitución mediante la promulgación de leyes estatales o federales. *Vid.*, entre otros: *Roe v. Wade*, 410 U.S. 113 (1973); *Whalen v. Roe*, 429 U.S. 589 (1977).

21. *Vid.*, entre otros: *Barry v. City of New York*, 712 F. 2d 1554 (2d Cir. 1983); *Slayton v. Willingham*, 726 F. 2d 631 (10th Cir. 1984).

22. Podemos referirnos al derecho a la privacidad informativa (*information privacy*) como aquella nueva vertiente del tradicional derecho a la privacidad desarrollado en Estados Unidos, que surge a tenor de un cambio en la jurisprudencia del Tribunal Supremo durante la década de 1960, como consecuencia de los tratamientos masivos que se realizan de información personal mediante el uso de las nuevas tecnologías desarrolladas bajo el acervo de internet. Su principal cometido radica en dotar a los afectados de las herramientas y los mecanismos necesarios que les permita disponer del control efectivo sobre sus datos personales, como parte integrante de una manifestación más del libre desarrollo de la personalidad contenido en el concepto de libertad sustantiva que se propugna en la cláusula del debido proceso establecida en la Decimocuarta Enmienda. *Vid*. Westin (1967), p. 7; Fried (1968), pp. 475-493; Cate (1997).

p. 22; pp. 1609-1701; Kang (1998), pp. 1193-1294; Schwartz (2000), pp. 815-859.

23. A este respecto, en palabras de Nieves Saldaña: "[t]odos los Tribunales de Circuito sostienen que el derecho a la *informational privacy* no es absoluto, ponderándose el interés individual en la protección de la información personal frente al interés estatal en la adquisición o divulgación de esa información, aunque difieren en cuanto a la relevancia que otorgan al interés estatal. Así, el Cuarto, Sexto y Décimo Circuitos aplican un examen judicial riguroso (*strict scrutiny*) a las invasiones estatales de la *informational privacy*, aunque el Sexto Circuito solo reconoce una violación de la información personal cuando afecta a derechos fundamentales, exigiendo demostrar un interés estatal esencial (*compelling state interest*) para invadir derechos fundamentales a través de la revelación de información personal, mientras que el Cuarto Circuito también aplica un escrutinio riguroso para evaluar la divulgación estatal de la información personal que no afecta a derechos fundamentales." Saldaña Díaz (2011), p. 306.

recibido por parte del sector doctrinal· (Flaherty 1991, pp. 831-855; Chlapowski, 1991, pp. 133-136; Turkington, 1990, pp. 496-503).

En *Whale v. Roe* (1977) el Tribunal amplió su protección a la privacidad sustantiva durante el proceso a la *information privacy*, sosteniendo que la zona de privacidad protegida por la constitución abarca el interés individual en evitar la divulgación de asuntos personales. Esta rama del derecho a la privacidad se conoce como el derecho constitucional a la privacidad de la información. En el amplio concepto de *privacy* hay que delimitar la *information privacy* que es la que se correspondería de manera más directa con el derecho fundamental a la protección de datos personales.

La "*information privacy"* está relacionada con la recopilación, uso, y revelación de información personal. Este concepto se diferencia de la "*decisional privacy*", el cual se corresponde con la libertad que tienen las personas de tomar decisiones sobre su propio cuerpo o familia (Solove, Rotenberg, Schwartz, 2005, p. 1). La "*decisional privacy"* tiene relación con como la anticoncepción, la procreación, el aborto y la crianza de los hijos. La misma es el centro de una serie de casos del Tribunal Supremo de los Estados Unidos relacionados con el proceso debido o el derecho constitucional a la privacidad. La reciente sentencia de 24 de junio de 2022 en el caso *Dobbs v. Jackson Women's Health Organization*, estableciendo que la Constitución no confiere un derecho al aborto y, por tanto, anulando la histórica sentencia del caso *Roe v. Wade* que protegía la libertad de una mujer para abortar sin excesivas restricciones gubernamentales, ilustraría el uso de la "*decisional privacy"*. La "*information privacy"* cada vez incorpora más elementos de la "*decisional privacy"*, ya que el uso de datos afecta decisivamente a la autonomía individual.

2.4. Statutory Law y derecho a la privacidad

El rápido avance de las tecnologías de computación produjo un profundo debate sobre la privacidad desde mediados de los 60. La privacidad, en efecto, pasó a ser una preocupación central de la sociedad estadounidense. El Tribunal Supremo, tal como se ha señalado más arriba, emitió una serie de pronunciamientos que han sido referente en la construcción del derecho a la privacidad.

En 1973 se publicó un informe que tuvo un gran impacto e influencia por el *United States Department of Health, Education, and Welfare*. Este documento realizó una profunda revisión de cómo se estaban procesando los datos en Estados Unidos, y propuso un *Code of Fair Information Practices*[24]. El código estableció unos principios básicos para el tratamiento de los datos personales, así como responsabilidades en la recopilación y uso de la información personal. En estos cabe destacar: a) la prohibición de mantener información personal de

24. U.S. *Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and Rights of Citizens* (1973).

forma secreta, b) el establecimiento de un derecho de acceso a las bases de datos para que los individuos conozcan si contienen información personal suya, c) la existencia de procedimientos que prevengan que los datos personales son utilizados con una finalidad distinta a la que se había consentido, d) el desarrollo de una forma para rectificar la información que los identifica, d) la obligación en cualquier organización que cree, mantenga, use o difunda registros de datos personales identificables de garantizar la confiabilidad de los datos para el uso previsto, y de tomar precauciones razonables para evitar el uso indebido de los datos.

Como ha señalado Marc Rottenberg, (Rotenberg, 2001, pp. 26-39). las recomendaciones establecidas en este código de buenas prácticas constituyeron un decisivo marco para la legislación sobre información personal que se aprobó desde mediados de los 70 en los Estados Unidos. La legislación sobre privacidad de la información en los Estados Unidos de América no cuenta con una reglamentación general al estilo del RGPD europeo que se aplique a cualquier tratamiento de datos personales. Por el contrario, se efectúa a través de diversas normativas federales y estatales de carácter sectorial[25].

Entre las regulaciones que se promulgaron en la década de los 70, se puede destacar a la *Privacy Act*[26]. Esta norma fue la primera ley federal que regulaba la recopilación, el mantenimiento, el uso y la difusión de la información personal almacenada por las distintas agencias federales norteamericanas sobre sus ciudadanos y terceros que pudieran resultar relevantes para los fines perseguidos. La *Freedom of Information Act*[27] (1966), por su parte, obligaba a facilitar a los ciudadanos la información y documentación que obre en sus respectivos archivos o expedientes, siempre medie el consentimiento previo del afectado o la divulgación se pueda efectuar por existir una habilitación normativa en virtud de las excepciones que contiene la norma.

El sistema liberal y antirregulatorio de las corporaciones, que se ha señalado, prefiere el uso de autorregulación (Schwartz, Solove, 2009; Solove, Rotenberg,

---

25. Se puede citar sin ánimos de exhaustividad: la *Right to Financial Privacy Act (RFPA)* de 1978; la *Financial Services Modernization Act* de 1999, habitualmente conocida como la *Gramm-Leach-Bliley Act (GLBA)* de 1999; la *Fair and Accurate Credit Transactions Act (FACTA)* de 2003; por lo que hace referencia a datos médicos, la *Health Insurance Portability and Accountability Act (HIPAA)* de 1996; y con una relativa mayor actualidad, en lo relativo a la privacidad genética, podríamos citar la *Genetic Information Nondiscrimination Act (GINA)* de 2008, así como la *California Consumer Privacy Act (CCPA)* de 2018 relativa a la protección de la información personal de los consumidores residentes en California. Haciendo énfasis igualmente en la protección de la información personal en las comunicaciones electrónicas, cabe citar, en especial, la *Cable Communication Policy Act* (CCPA) de 1984; la *Electronic Communications Privacy Act* (ECPA) de 1986; la *Telecomunications Act* de 1996; la *Children's On-line Privacy Protection Act* (COPPA) de 1998 y la *E-Government Act* de 2002.

26. Estados Unidos. *Privacy Act,* 5 U.S.C. § 552 a), *Section* 2. Promulgada del 31 de diciembre de 1974 por parte del Congreso de los Estados Unidos de América.

27. Estados Unidos. *Freedom of Information Act (FOIA)*, 5 U.S.C. § 552. Promulgada el 4 de julio de 1966 por parte del Congreso de los Estados Unidos de América.

Schwartz, 2005) a una intervención legislativa similar a la que se opera en el sector público. Al respecto, Arribas Luque señala que: "La irrupción de las nuevas tecnologías y la escasa protección legislativa de la *privacy* motivó la pérdida de la confianza del consumidor norteamericano y forzó la autoimposición empresarial, voluntaria y como táctica comercial, de normas de conducta limitativas del libre uso de los datos personales, en la creencia de que una política, debidamente difundida, de protección de la privacidad de las personas frente a la intromisión generalizada en aquella que caracterizaba a la competencia redundaría en una mayor captación de clientela y en mayores beneficios." (Arribas Luque, 2002, pp. 1587-1599)

Más recientemente, en 2018 se aprobó *la California Consumer Privacy Act* ("CCPA"), esto hizo que California fuera uno de los primeros Estados en elaborar una regulación para la privacidad y protección de datos de los consumidores. El principal impulso de la norma fue el apoyo popular a la iniciativa con más de 600.000 firmas. En esta norma, junto a los derechos de acceso y supresión, destaca la apelación directa a las empresas a no vender información personal: *"[A] consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out*."[28]

El ámbito subjetivo de protección de la CCPA se restringe a los "consumidores", en este sentido se puede señalar una de las principales diferencias con el régimen de la protección de datos de la Unión Europea, el cual como es sabido, afecta a todos los tratamientos de datos personales, sean públicos o privados, haya o no relación de consumo. En este sentido, vemos dos modelos de cultura jurídica, una que ha constituido un nuevo derecho fundamental, y la otra que prefiere adoptar la perspectiva del consumidor, del "ciudadano administrado", o en algunos casos del paciente, o del menor.

Recientemente diversos Estados han seguido la senda de California y han aprobado leyes sobre protección datos. Las mismas, en efecto, siguen el modelo de la *California Consumer Privacy Act* CCPA, así como adoptan una definición del concepto de datos personal muy similar a la del Reglamento General de Protección de Datos (RGPD). No obstante, se debe insistir en que el ámbito de aplicación es únicamente consumo, que las causas de legitimación no se corresponden con el RGPD, y que hay muchas excepciones y salvades procedentes de otras normas de privacidad. En todo caso, las conocidas como "States Privacy Laws" son: la *Colorado Protect Personal Data Privacy Act* (ColoPA) de 7 de julio de 2021, que entrará en vigor en la misma fecha del 2023, la *Conneticut Privacy Act* (CTPA), de 10 de mayo de 2022, que entrará plenamente en vigor el 1 de julio de 2023; la *Virgina Consumer Data Protection Act* (VCDPA) de 2 de marzo de 2021 que entrará en vigor el 1 de enero de 2023; y la *Utah Consumer Priva-*

28. Art. 1798.120, letra a) de la California Consumer Privacy Act of 2018 [1798.100 — 1798.199.100] *(Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3).*

cy Act (UCPA) de 24 de marzo de 2022 que entrará en vigor el 31 de diciembre de 2023.

Para acabar este análisis se debe hacer referencia la mencionada iniciativa legislativa federal que está suscitando gran interés a ambos lados del Atlántico: la *American Data Privacy and Protection Act* (a partir de ahora ADPPA). Tras décadas de inactividad en el ámbito de la protección de datos se quiere establecer un "*federal privacy statute*". Entre los aspectos más relevantes de este nuevo régimen jurídica estaría la "*data minimization*". En este concepto hallamos una trasposición del principio recogido en el artículo 5 del RGPD, según el cual, los datos de personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". Igualmente, introduce el principio de "limitación de la finalidad" de la norma europea. La compañía solo podrá recopilar datos si es necesario para alguno de los diecisiete propósitos permitidos en el proyecto de ley. Se puede destacar una sustancial diferencia entre este *numerus clausus* de finalidades permitidas, y el complejo sistema de causas de legitimación del RGPD[29], en el cual figuras como el "interés legítimo" han ganado relevancia ante el tradicional "consentimiento del afectado".

La elaboración de la ADPPA está suscitando cuestiones competenciales entre el derecho federal y el estatal. Se está planteando si la futura legislación federal debería prevalecer sobre la legislación estatal, hecho que ha planteado la firme oposición de los Estados que han elaborado normativa y han constituido agencias de protección de datos. La creación de un "derecho de acción privado" que permita a las personas, no solo al gobierno, demandar a las empresas por violaciones es otros de los aspectos que está desatando mayor polémica en sede parlamentaria. Los demócratas generalmente están en contra de la preferencia del derecho federal y a favor de un derecho de acción privado, los republicanos lo contrario.

A buen seguro este nuevo régimen de la protección de datos no supondrá un cambio en la consideración de Estados Unidos como un país con un nivel no adecuado de protección, pues sigue manteniéndose la sectorización, y su ámbito de aplicación no afecta a la seguridad nacional, principal preocupación del Tribunal de Justicia de la Unión Europea como se analizará a continuación.

3. EL NUEVO DATA PRIVACY FRAMEWORK TRANSATLÁNTICO

Las transferencias de datos personales desde la Unión Europea hacia los Estado Unidos tienen un impacto muy significativo en las relaciones comerciales y en las inversiones entre las dos potencias económicas. Por otra parte, refuer-

29. Según el artículo 6 del RGPD son: a) consentimiento, b) relación contractual, c) Intereses vitales del interesado o de otras personas, d) cumplimiento de una obligación legal para el responsable, e) interés público o ejercicio de poderes públicos.

zan la comunicación on-line, sirven para monitorizar las cadenas mundiales de abastecimiento, establecen servicios transfronterizos y fomentan la innovación tecnológica, entre muchos otros aspectos. En el año 2020, el tráfico mercantil de los servicios de tecnologías de la información y la comunicación ascendió a 264 miles de millones, cifra que revela la enorme importancia de las relaciones transatlánticas. En este sentido, la obtención de una decisión de adecuación se convierte en un elemento crítico para el desarrollo de la economía digital entre ambas áreas. En los siguientes apartados se va a analizar sintéticamente la evolución de este régimen especial hasta llegar al marco actual, el *Data Privacy Framework*.

3.1. Antecedentes: Safe Harbor y Privacy Shield

Las diferentes concepciones sobre la privacidad y la protección de datos entre los Estados Unidos de América y la Unión Europea condujeron a la Comisión Europea a no considerar que el primero cuenta con un nivel adecuado de protección. Sin duda la diversidad y pluralidad del derecho a la privacidad que hemos visto en los apartados anteriores ha condicionado a que su régimen jurídico no sea homologado. Aunque las acciones de vigilancia masiva llevadas a cabo por parte de las agencias de inteligencia de los Estados Unidos, reguladas por la *Foreign Intelligence Surveillance Act* (FISA) de 1978 son las que marcaron el verdadero escollo para obtener la homologación.

Estas problemáticas se manifestaron durante la negociación del primer acuerdo de intercambio de datos entre ambos territorios, articulado a través de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, loa *EU-US Safe Harbor Principles*. El órgano consultor en materia de protección de datos de la UE denominado "Grupo de trabajo del Artículo 29" (GT 29) denunció reiteradamente las carencias de las que adolecía. Las mismas se sustentaban esencialmente en las particularidades propias de la legislación interna de los Estados Unidos, basada en la prevalencia de la seguridad nacional frente a la protección de otros bienes jurídicos[30].

A la situación descrita se suma que las autoridades norteamericanas competentes no velaban por la aplicación de la propia Decisión. Se establecieron, además, una serie de excepciones que socavaban peligrosamente las garantías de los ciudadanos europeos. Las mismas se relacionaban con el cumplimiento de las exigencias de seguridad nacional, interés público y cumplimiento de la ley. En 2013 la Comisión Europea propone una serie de recomendaciones y propuestas para apaciguar las crecientes críticas al acuerdo con los Estados Unidos.

Las revelaciones de exagente de la NSA, Edward Snowden, no hicieron más que acrecentar las denuncias de vulneración masiva de los datos personales europeos. Una figura crucial en estas reivindicaciones fue el abogado y activista

30. *Vid*. Castellanos Rodríguez (2022).

austriaco Maximiliam Schrems. En 2013, tal como se ha apuntado más arriba, presentó una denuncia contra Facebook Ireland Ltd en el *Irish Protection Commissioner,* ya que en este país están situados las oficinas centrales de la red social en Europa. En la misma se solicitaba que se prohibiese la transferencia de datos desde Irlanda a Estados Unidos alegando que Facebook USA estaba implicado en el programa de vigilancia masiva conocido como PRISM. La base jurídica de la petición se sustentaba en que la normativa de protección de datos de la Unión Europea no autorizaba la transferencia internacional de datos a países que no garantizasen "un adecuado nivel de protección". Tras ser rechazada por la autoridad de protección de datos irlandesa, interpuso una demanda al *Irish High Court*. El tribunal planteó una cuestión prejudicial al Tribunal de Justicia de la Unión Europea (TJUE) en el cual se solicitaba la interpretación del artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea que recoge el derecho a la protección de datos personales.

El 6 de octubre de 2015 el TJUE dictó una resolución que supuso un verdadero movimiento sísmico en las relaciones económicas digitales entre las dos potencias. Se determinó la invalidez de la Decisión (*Safe Harbor*) y se declaró la imposibilidad de efectuar transferencias internacionales a los Estados Unidos de América. En esta sentencia, conocida como *Schrems I*, el Alto Tribunal comunitario aprovechó para responsabilizar a la Comisión Europea de no haber efectuado las comprobaciones necesarias que hubieran permitido determinar con exactitud que los Estados Unidos no gozaban de un nivel de protección adecuado para ser el destinatario de los datos personales de ciudadanos de la Unión.

Como reacción a las revelaciones efectuadas por Snowden, el país norteamericano aprobó una serie de instrumentos normativos en los cuales supuestamente se trataba de garantizar que no se produjesen prácticas abusivas en materia de vigilancia y obtención de información por parte de las agencias de inteligencia norteamericanas. Tras más de dos años de negociaciones, el 16 de julio de 2016, se aprobó el segundo acuerdo de intercambio de datos entre la Unión Europea y los EE. UU., a través de la Decisión de Ejecución (UE) nº 2016/1250, de la Comisión Europea bautizado con un nombre muy significativo *"Privacy Shield"*. A pesar de que introdujo una serie de novedades en virtud de los mandamientos contenidos en el pronunciamiento del TJUE, las mismas no resultaron suficientes. En idénticos términos que le había sucedido a su antecesor, desde un primer momento fue objeto de críticas por parte de distintos organismos comunitarios —como el GT29, el Supervisor Europeo de Protección de Datos y el propio Parlamento Europeo— motivadas precisamente por las deficientes garantías que se establecían en su contenido respecto la protección de los derechos y libertades de los afectados situados en la Unión.

Dichas deficiencias serían sucesivamente puestas de manifiesto en las distintas revisiones que se efectuaban sobre la eficacia del acuerdo por parte del GT29 o la propia Comisión, entre otros organismos comunitarios. La situación se sustanciará nuevamente con la invalidación del acuerdo *Privacy Shield* por el TJUE en la sentencia *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (C-311/18) conocida como *Schrems II*. Entre las diversas cues-

tiones que fundamentaran el pronunciamiento por parte del TJUE, se puede encontrar la ausencia de límites tangibles que impusieran restricciones a las actuaciones realizadas por las agencias de inteligencia norteamericanas bajo el mandato de la Sección 702 de la FISA[31], así como la inexistencia de garantías específicas que pusieran de manifiesto la efectividad e independencia de la figura del Defensor del Pueblo respecto al poder ejecutivo[32].

El caso *Schrems II* pone de manifiesto nuevamente las vulneraciones a la privacidad y protección de datos de los usuarios europeos de Facebook causadas por la revelación masiva de los mismos a la *National Security Agency* (NSA) y al *Federal Bureau of Investigation* (FBI) para la lucha contra el terrorismo. La compañía de Mark Zückerberg, además de este asunto, amparado dudosamente en la seguridad nacional, ha protagonizado en la última década numerosos escándalos relacionados con la cesión ilegal de datos personales. En julio de 2019 marcó un hito, le fue impuesta por la *Federal Trade Commission* (FTC en adelante) la multa más elevada de la historia, no sólo en Estados Unidos sino también en el resto del planeta[33]. La FTC sancionó a la red social con 5.000 millones de dólares, así como muy elevados requerimientos para impulsar la "*accountability*" y la transparencia[34], por la venta indiscriminada y sin ninguna legitimación de millones de datos personales de sus usuarios[35]. El caso *Facebook-Cambridge Analytica* constituye otra muestra del enorme riesgo del tratamiento ilícito de datos no solo para los derechos y libertades fundamentales de los ciudadanos europeos o americanos sino para el núcleo mismo de la demo-

31. *Vid*. Apartados 291, 292 y 297 de las conclusiones del Abogado General Sr. Henrik Saugmandsgaard Øe sobre el asunto C-311/18.

32. *Ibidem*, apdo. 337.

33. La multa monetaria fue casi diez veces superior a la punición de 575 millones de dólares impuesta a Equifax por la FTC y por el *Consumer Financial Protection Bureau* (CFPB) por una violación de seguridad en sus datos. "Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach", nota de prensa de la FTC, https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related. (Recuperado el 11 de agosto de 2019).

34. Véase "FTC Approves Final Settlement With Facebook. Facebook Must Obtain Consumers' Consent Before Sharing Their Information Beyond Established Privacy Settings", nota de prensa de la FTC, 10 de agosto de 2012, https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook (Recuperado el 11 de agosto de 2019).

35. La resolución se basa en la Sección 5 (a) y (l) y 16 (a) (l) de la *Federal Trade Commission* Act ("FTC Act"), 15 U.S.C., 45 (a) y (l) y 56 (a) (l), por las violaciones de la orden de 2012 de la FTC por las violaciones de la Section 5 (a) de la FTC. Véase "COMMISSION ORDER" In Re Facebook Inc., C-4365, 2012 FTC LEXIS 135 (F.T.C. 2012) (Decision and Order). La sanción se basó en la vulneración de los requerimientos que habían sido impuestos a Facebook en la Orden de la FTC de 2012. Esta sanción estaba motivada en el engaño a los usuarios sobre su capacidad de controlar la privacidad de su información personal. El acuerdo, igualmente, imponía nuevas restricciones a las operaciones de negocio de Facebook y crea múltiples canales de "*Compliance*". La orden requiere a la compañía reestructurar su aproximación a la privacidad desde el nivel de dirección de la compañía (Corporate Board) hacía abajo. Se impone, por tanto, una nueva estructura de privacidad a Facebook y nuevas herramientas a la FTC para monitorear su actividad.

cracia[36]. Supuso la recopilación de millones de datos de usuarios de la red social sin su consentimiento con fines de propaganda política en la campaña presidencial de Trump en el 2016 o en el referéndum del Brexit del mismo año.

Estos oscuros affaires, que tienen el común denominador del mayor conglomerado de redes sociales del mundo, revelan la enorme tensión que están sufriendo los mecanismos de garantías de derechos y libertades en los principales sistemas jurídicos del ámbito occidental. Grandes cantidades de información usadas por los gobiernos y por las empresas. Los afectados en el primer caso son los ciudadanos, y en el segundo los consumidores.

Por último, el pasado 25 de marzo 2022 la Unión Europea y los Estados Unidos realizaron un anuncio conjunto de una importancia trascendental: la tramitación de un nuevo acuerdo sobre el régimen legal de las transferencias de datos personales entre ambos territorios, al cual se denominó *Trans-Atlantic Data Privacy Framework*[37]. Este marco jurídico pretende dar respuesta a las graves problemáticas señaladas por el Tribunal de Justicia de la Unión Europea a *Schrems II*. Sin embargo, todo apunta a que el nuevo acuerdo no será más que un ejercicio de maquillaje, pues Estados Unidos no va a modificar ni un ápice su política de seguridad nacional, y las nuevas iniciativas legislativas, muy orientadas al ámbito de consumo, no alteraran la consabida fragmentación del régimen jurídico de la protección de datos.

3.2. EU-US Data Privacy Framework

El 10 de julio de 2023, tal como se ha señalado, la Comisión Europea aprobó la decisión de adecuación para posibilitar la transferencia de datos personales entre entidades de la Unión Europea y de los Estados Unidos bajo el denominado *EU-US Data Privacy Framework*[38]. El sistema se compone de tres partes: la decisión de adecuación del "Marco de Privacidad de Datos UE-EEUU" de la Comisión Europea, los "Principios del Marco de Privacidad de Datos UE-EE.UU." del Departamento de Comercio de EE.UU., y otros documentos complementarios del lado estadounidense para el marco, incluida la Orden Ejecutiva 14086 que se examinará más adelante.

El DPF se basa en un sistema de certificación, que debe renovarse anualmente, mediante el cual las organizaciones estadounidenses[39] se comprometen a respetar un conjunto de principios de privacidad. En este sentido, el DPF toma

36. Véase sobre la manipulación digital de elecciones a Zittrain (2014).

37. European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2087 (Consultado

38. Las normas sobre transferencias de datos personales de los responsables o encargados del tratamiento en la Unión a terceros países y organizaciones se establecen en el capítulo V del RGPD.

39. Para que una organización puede acogerse al DPF debe estar sujeta a los poderes de investigación de la *Federal Trade Commission* (FTC) o del Departamento de Transporte.

como base el Artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE), así como los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. La decisión, por otra parte, recoge los principios establecidos en el artículo 5 del RGPD[40]. Estos exigen un tratamiento lícito, leal, transparente, limitado a la finalidad y al tiempo por los cuales se recogieron. Asimismo, establece obligaciones con relación a la exactitud, minimización y seguridad de la información (confidencialidad, integridad y disponibilidad).

Cuando una organización haya decidido certificarse voluntariamente según el DPF el cumplimiento efectivo de los principios es obligatorio y exigible. Estas deberán tomar las medidas para verificar que sus políticas de privacidad se ajustan a los principios y a que se cumplan, así como deberán implementar estos principios en su política de privacidad. En este sentido, la decisión aboga por los mecanismos de autoevaluación, las auditorías tanto internas como externas, así como por la capacitación de los empleados.

El DPF acoge la definición de dato personal del RGPD, como "datos sobre un individuo identificado o identificable recibidos por una organización en los Estados Unidos desde la UE registrados por cualquier medio". La aplicación de concepto de protección de datos del reglamento europeo implica que también se extienda a los datos pseudonimizados, incluso cuando la organización norteamericana receptora no tenga acceso a la clave de decodificación. Del mismo modo, se trasladan las salvaguardas para las categorías especiales de datos establecidas en el RGPD, es decir, datos personales que especifican condiciones médicas o de salud, origen racial o étnico, opiniones políticas, creencias religio-

---

40. Artículo 5 del RGPD,

Principios relativos al tratamiento

1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

sas o filosóficas, afiliación sindical, información sobre la vida sexual del individuo o cualquier información recibida de un tercero que sea identificada por esta como sensible. De manera similar, la noción de procesamiento se define como "cualquier operación o conjunto de operaciones que se realiza sobre datos personales, ya sea por medios automatizados o no, tales como recolección, registro, organización, almacenamiento, adaptación o alteración, recuperación, consulta, uso, divulgación o difusión y supresión o destrucción."[41]

Los interesados deben tener determinados derechos que puedan oponerse al responsable o al encargado del tratamiento, en particular el derecho de acceso a los datos, el derecho a oponerse al tratamiento y el derecho a que los datos sean rectificados y suprimidos. Estos son los conocidos como derechos ARCO plus por la normativa europea y suponen el núcleo del *habeas data*, es decir, el derecho de los interesados a contar con mecanismos e instrumentos para ejercer un control efectivo de sus datos personales.

El considerando 35 de la decisión de adecuación hace referencia a diversas normas que pueden ofrecer un nivel de protección similar en la "improbable situación" (en palabras del considerando), de que las decisiones automatizadas fueran adoptadas por la propia organización. En cualquier caso, en aquellos ámbitos donde las empresas probablemente recurran al procesamiento automatizado de datos personales para tomar decisiones que afectan a los individuos (por ejemplo, préstamos de crédito, ofertas hipotecarias, empleo, vivienda y seguros), la legislación estadounidense proporciona protecciones específicas contra decisiones adversas. Estas leyes generalmente establecen que las personas tienen derecho a ser informadas de los motivos específicos que fundamentan la decisión (como el rechazo de un crédito), a cuestionar la información incompleta o inexacta (así como la dependencia de factores ilícitos) y a buscar reparación.

En el ámbito del crédito al consumo, la Ley de Informes Crediticios Justos (FCRA) y la Ley de Igualdad de Oportunidades Crediticias (ECOA) contienen salvaguardias que otorgan a los consumidores el derecho a una explicación y la posibilidad de impugnar la decisión. Estas leyes son relevantes en una amplia gama de contextos, incluyendo el crédito, el empleo, la vivienda y los seguros. Además, ciertas leyes contra la discriminación, como el Título VII de la Ley de Derechos Civiles y la Ley de Vivienda Justa, proporcionan protección a las personas frente a los modelos utilizados en la toma de decisiones automatizadas que podrían conducir a la discriminación basada en determinadas características, y les otorgan derechos para impugnar tales decisiones, incluidas las automatizadas.

En relación con la información de salud, la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) establece que cualquier decisión basada en el procesamiento automatizado normalmente será tomada por el responsable de tratamiento en la Unión Europea, que es quien tiene una relación directa con el

41. (Anexo I, apartado I.8.b).

interesado y, por ende, está directamente sujeto al Reglamento (UE) 2016/679. Esto incluye escenarios de transferencia en los que el procesamiento es llevado a cabo por un operador comercial extranjero (por ejemplo, en Estados Unidos) que actúa como agente (encargado de tratamiento) en nombre del responsable del tratamiento en la Unión Europea (o como subencargado que actúa en nombre del encargado del tratamiento en la Unión Europea que recibió los datos de un responsable del tratamiento en la Unión Europea que los recopiló) y, sobre esta base, toma la decisión. La regla de privacidad de la HIPAA crea ciertos derechos que son análogos a los establecidos en el Reglamento (UE) 2016/679 en cuanto al acceso a la información de salud personal. Asimismo, la orientación de las autoridades estadounidenses exige que los proveedores médicos reciban información precisa y completa.

Por último, se debe señalar que el Departamento de Comercio es el encargado de supervisar de forma continua el cumplimiento efectivo de los principios por parte de las organizaciones adheridas al DPF. En este sentido, llevará a cabo diversas acciones tales como verificaciones aleatorias de las organizaciones selecciones, supervisión de aquellas en las que se identifiquen problemas de cumplimiento para verificar posibles quejas o solicitudes de los interesados, o revisar la política de privacidad. Si hay elementos probatorios suficientes el Departamento de Comercio envía un cuestionario al cual si no se responde se podrán tomar posibles acciones coercitivas. Para garantizar en la práctica un nivel adecuado de protección existirán autoridades de control independientes con competencias para controlar y hacer cumplir las normas de protección de datos. En este sentido, es necesario que las organizaciones estadounidenses que se quieran acoger al DPF se hallen bajo la jurisdicción de la *Federal Trade Commission* o del Departamento de Comercio.

3.3. La Orden Ejecutiva 14086 "Enhancing Safeguards in United States Signals Intelligence Activities"

La Orden Ejecutiva 14086 *"Enhancing Safeguards in United States Signals Intelligence Activities"* de 7 de octubre de 2022 estableció un nuevo proceso para que las personas puedan buscar reparación con respecto a presuntas violaciones de la ley en relación con actividades de inteligencia de señales[42] que afecten a sus datos transferidos desde un "Estado calificado" (todos los miembros de la UE lo son) a los Estados Unidos. La normal presidencial creó una figura de garantía jurisdiccional, el denominado, Tribunal de Revisión de Protec-

42. Inteligencia de señales (en inglés: signals intelligence; SIGINT) es la forma de recopilación de información, inteligencia militar, mediante la interceptación de señales, bien a partir de comunicaciones directas entre personas (inteligencia de comunicaciones; en inglés: communications Intelligence, COMINT), bien de distintos medios electrónicos que no sirven para las comunicaciones directas (inteligencia electrónica; en inglés: electronic Intelligence, ELINT), o bien una combinación de ambos.

ción de Datos (DPRC, por sus siglas en inglés). Esta novedosa institución forma parte de un nuevo proceso de revisión independiente e imparcial en dos niveles de las denuncias presentadas por ciudadanos de países considerados como "Estados calificados", entre los que se encuentran todos los Estados miembros de la UE. La denuncia debe estar basada en una vulneración de los datos personales por Inteligencia de señales (SIGINT).

La función principal del DPRC es revisar las decisiones del Oficial de Protección de Libertades Civiles de la Oficina del director de Inteligencia Nacional (CLPO) con respecto a las denuncias presentadas por individuos en países u organizaciones regionales de integración económica que el Fiscal General de EEUU ha designado como "estados calificados" bajo la Orden Ejecutiva 14086. Para utilizar el proceso de reparación del DPRC, los individuos deben pasar por el primer nivel del mecanismo de reparación, el mecanismo de reparación del CLPO.

Los ciudadanos de la UE, en tanto que nacionales de Estados calificados, pueden presentar sus quejas ante sus autoridades de control, alegando que Estados Unidos violó su propia ley de inteligencia al recolectar o manejar sus datos a través de actividades de inteligencia de señales. Tras las verificaciones pertinentes la autoridad de control remitirá la denuncia al CLPO. Esta figura revisa que la denuncia cumpla con los requisitos, investigará el caso y dictará una resolución. Si el denunciante no está conforme con la decisión podrá solicitar la revisión por parte del DPRC, el cual revisará la decisión del CLPO y podrá solicitar información adicional con el fin de averiguar si se produjo una vulneración, y en caso afirmativo, establecería la indemnización o las medidas oportunas para compensar el daño.

Los cambios introducidos por la EO 14086 han incrementado las garantías y salvaguardas por las actividades de inteligencia de señales en relación con PPD-28, el cual fue parcialmente revocado por National Security Memorandum de 7 de octubre de 2022. En particular se establece la obligatoriedad de emplear criterios de "necesidad" y "proporcionalidad" para el uso de SIGINT. Por otra parte, se limita la recopilación masiva de inteligencia de señales en tres modos: 1) la información necesaria no puede ser "razonablemente" adquirida por una recopilación dirigida, 2) los datos recopilados se deben circunscribir a los necesarios, 3) debe cumplirse con al menos uno de los seis objetivos establecidos en la norma. A pesar de estos avances, la norma puede vulnerar los principios del RGPD y con la jurisprudencia del TJUE.

Los conceptos de necesidad y proporcionalidad no son interpretados a la luz de la tradición europea, con lo cual las prioridades de inteligencia de los Estados Unidos no pueden ser aceptadas desde el punto de vista de la protección de datos y el derecho a la intimidad de la UE. En cuanto al concepto de "proporcionado" reproduciendo las palabras de Schrems:

> "The EU and the US now agree on the use of the word 'proportionate' but seem to disagree on the meaning of it. In the end, the CJEU's definition will prevail — likely killing any EU decision again. The European Commission is

> turning a blind eye on US law again and allowing the continued surveillance of Europeans."

En conclusión, se puede afirmar que las salvaguardas introducidas por el DPF son insuficientes para cumplir con el estándar europeo de protección de datos e intimidad, lo cual nos sitúa ante más que una probable Sentencia Schrems III.

3. CONCLUSIONES

La comparación es el ejercicio de encontrar las diferencias entre dos culturas jurídicas o dos sistemas jurídicos para hallar el mejor modelo, o al menos extraer lecciones aplicables al derecho propio. En el ámbito de la privacidad y la protección de datos está premisa de la ciencia comparatística se convierte en una necesidad acuciante ante los retos y las amenazas que plantea el "capitalismo vigilante" de Zuboff o la cosificación que sufre el individuo "dataficado" descrito por Han. Si atendemos a la posición hegemónica y monopolística de los grandes proveedores de servicios estadounidenses la protección que ofrece el derecho de la Unión Europea a sus ciudadanos sufre una preocupante merma. El afán regulatorio del gigante europeo trata de equilibrar el inmenso poder del club de grandes corporaciones conocido como GAFAM.

La aprobación del Reglamento General de Protección de Datos en 2016 fue un notable avance, más bien una "actualización", dicho en términos informáticos. A pesar del enorme impacto mundial de la legislación europea de protección de datos, que se está convirtiendo en estándar internacional, desde la fecha de su aprobación no han dejado de sucederse los escándalos, las vulneraciones masivas de la protección de datos de los europeos por parte de las grandes corporaciones tecnológicas, y lo que es más grave del propio gobierno de los Estados Unidos. Esta situación está tensionando las relaciones económicas entre las dos potencias, ya que la UE está poniendo grandes trabas jurídicas a las transferencias internacionales de datos a EEUU.

Este desencuentro no es nuevo, la UE nunca ha considerado que los EEUU tienen un nivel adecuado de protección de los datos personales. Resulta curioso que el país que "inventó" un derecho personalísimo para proteger la dignidad de sus ciudadanos ante el avance las tecnologías a finales del siglo XIX, y que en la década de los 70 fue pionero en regular el uso de los datos de los ciudadanos por las agencias gubernamentales, no reciba tal consideración. Todavía más, si observamos que estos logros son indiscutiblemente el origen también de la privacidad y protección de datos en Europa. Estamos ante un interesante caso de trasplante jurídico de instituciones que en la tierra nueva echa raíces más profundas y da muchos más frutos.

Se puede concluir que hay una diferencia muy sustancial entre ambas culturas jurídicas que imposibilitan esta homologación. Es cierto que en Estados Unidos hay una protección jurisdiccional enorme a través del derecho de *torts* del *Common Law*, que empequeñece al sistema de responsabilidad civil por

vulneración de protección de datos europeo. La fuerza disuasoria que tiene para las empresas en los EEUU la posibilidad de ser demandados por cantidades millonarias ha abierto tradicionalmente la puerta a una autorregulación. Por otra parte, el dinamismo y ductilidad del derecho creado por los jueces es una característica sumamente útil y eficiente cuando estamos ante fenómenos como la vertiginosa transformación digital.

No obstante, son los propios jueces los que han anulado en muchas ocasiones legislaciones de protección de datos por entender que vulneraban la libertad de expresión de la Primera Enmienda. Los recelos antirregulatorios no son solo de los jueces, sino también de un importante sector doctrinal, y estudiando la privacidad y el impacto del artículo de Warren y Brandeis, se antoja innecesario subrayar la importancia que tiene en Estados Unidos el sector académico. En cuanto a las empresas, sería una obviedad señalar que no desean ser reguladas. Desde la concepción de la libertad de expresión de la Unión Europea resulta totalmente incomprensible este "balance" entre los derechos, en el cual sale perdiendo la protección de datos.

En el derecho constitucional americano la privacidad está muy desarrollada, aunque no hay una mención expresa, el Tribunal Supremo ha interpretado su existencia en un total de cinco enmiendas de su Constitución. Esto ha convertido a la privacidad en un elemento central de su sistema constitucional de garantías, creando figuras como la "*decisional privacy*", clave en el derecho al aborto, que no encuentran un equivalente en el derecho europeo. Sin embargo, ha originado una gran fragmentación del derecho a la privacidad, y consecuentemente a la "*information privacy*", que puede redundar en un debilitamiento del mismo.

El régimen general y abstracto europeo rechazado desde el *Common Law* y desde los sectores más libertarios de la academia americana, seduce muy notablemente al gobierno federal, y a muchos gobiernos estatales. Además, cuenta con firmes defensores entre los activistas de la privacidad. El Estado de California está a la cabeza de este movimiento, seguido de Colorado, Connecticut, Virginia y Utah. A estas leyes estatales se suma el proyecto federal de una ley de protección de datos. No obstante, estas normas están orientadas al ámbito de consumo, y a pesar de algunas similitudes con el RGPD, cuentan con sustanciales diferencias en las causas de legitimación, las obligaciones a las empresas, etc. Tampoco es descabellado que puedan sufrir algún importante recorte por parte del Tribunal Supremo por colisionar con otros derechos constitucionales. Sin olvidar que no se aplican a ámbitos como la seguridad nacional que el tema más conflictivo en las relaciones entre EEUU y la UE.

Por otra parte, los cambios introducidos por la Orden Ejecutiva 14086 (EO 14086) han incrementado las garantías y salvaguardas en las actividades de inteligencia de señales, especialmente en relación con la Directiva Presidencial de Política-28 (PPD-28), que fue parcialmente revocada por el Memorándum de Seguridad Nacional del 7 de octubre de 2022. La EO 14086 establece la obligatoriedad de emplear criterios de "necesidad" y "proporcionalidad" para el uso de inteligencia de señales (SIGINT). Además, limita la recopilación masiva de inte-

ligencia de señales a través de tres modos específicos: primero, cuando la información necesaria no puede ser "razonablemente" adquirida por una recopilación dirigida; segundo, los datos recopilados deben restringirse a lo necesario; y tercero, debe cumplirse al menos uno de los seis objetivos establecidos en la norma.

A pesar de estos avances, se observan importantes discrepancias con los principios del Reglamento General de Protección de Datos (RGPD) y la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE). Los conceptos de necesidad y proporcionalidad no son interpretados según la tradición europea, lo que significa que las prioridades de inteligencia de los Estados Unidos no pueden ser aceptadas desde el punto de vista de la protección de datos y el derecho a la intimidad de la UE. Mientras que la UE y los EE.UU. están de acuerdo en el uso de la palabra "proporcional", parece que no concuerdan en su significado real. Al final, es probable que prevalezca la definición del TJUE, lo que podría llevar nuevamente a la anulación de cualquier decisión de la UE en este ámbito.

La Comisión Europea, en su intento de encontrar un equilibrio, parece ignorar las diferencias fundamentales en la interpretación de la legislación estadounidense, permitiendo así la continua vigilancia de los ciudadanos europeos. Esto representa una situación delicada y crítica, pues las salvaguardas introducidas por el Data Privacy Framework (DPF) resultan insuficientes para cumplir con el estándar europeo de protección de datos e intimidad.

En resumen, las modificaciones establecidas por el DPF y la EO 14086, aunque representan un avance, no logran alinearse completamente con los requisitos europeos de protección de datos. La falta de una interpretación compartida de conceptos clave como "necesidad" y "proporcionalidad" crea una discordancia significativa entre ambos sistemas legales. La aparente condescendencia de la Comisión Europea frente a las prácticas estadounidenses pone en riesgo la privacidad de los ciudadanos europeos y abre la puerta a futuras disputas judiciales, siendo muy probable que se emita una Sentencia Schrems III. Esta sentencia, como sus predecesoras, podría invalidar nuevamente los acuerdos de transferencia de datos entre la UE y los EE.UU., subrayando la necesidad de un marco más robusto y armonizado que garantice efectivamente la protección de los datos personales en el contexto transatlántico.

BIBLIOGRAFÍA

ARENAS RAMIRO, M. (2006), *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Ed. Tirant lo Blanch.

ARRIBAS LUQUE, J. M. (2002), "Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE. UU.: El sistema de principios de Puerto Seguro", en *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, pp. 1587-1599.

ARZOZ SANTIESTEBAN, X. (2009), "Artículo 8: derecho al respeto de la vida privada y familiar", en *Convenio Europeo de Derechos Humanos. Comentario sistemático*, Navarra: Ed. Thomson-Reuters (Civitas).

BALKIN, J. M. (2004), "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society"*, New York University Law Review*, 79, pp. 1-55.

— (2016), "Information Fiduciaries and the First Amendment", en *UC Davies Law Review,* 49, pp. 1183-1234.

BARRON, J. H. (1979), "Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark Citation", 13 *Suffolk Law Review,* pp. 875-922.

BLOUSTEIN, E. J. (1964), "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser"*, New York University Law Review*, pp. 962-1007.

BRADFORD, A. (2019), *The Brussels Effect: How the European Union Rules the World*, Oxford University Press.

BRAGE CAMEZANO, J. (2005), "Aproximación a una teoría general de los derechos fundamentales en el Convenio Europeo de Derechos Humanos", en *Revista Española de Derecho Constitucional,* n.º 74, pp. 111-137.

CASTELLANOS RODRÍGUEZ, A. (2022), *Deconstruyendo las transferencias internacionales de datos personales,* Cizur Menor, Thomson Reuters-Aranzadi.

CATE, F. H. (1997), *Privacy in the Information Age*, Washington, Ed. Brookings Institution Press.

CHLAPOWSKI, F. S. (1991), "The Constitutional Right to Informational Privacy", en *Boston University Law Review*, n.º 71, pp. 133-136.

CHUECA SANCHO, A. G. (2004), "Por una Europa de los derechos humanos: la adhesión de la Unión Europea al Convenio Europeo de Derechos Humanos", en *Unión Europea y Derechos fundamentales en perspectiva constitucional*, Madrid: Ed. Dykinson, pp. 37-58.

COOLEY, T. C. (1888), *Law of Torts*, Chicago, Callaghan & Co.

DAVARA RODRÍGUEZ, A. (1988), *La protección de datos en Europa*, Madrid, Ed. Grupo ASNEF-Equifax / Universidad Pontificia de Comillas.

FLAHERTY, D. H. (1991), "On the Utility of Constitutional Rights to Privacy and Data Protection", en *Case Western Reserve Law Review*, nº 41, pp. 831-855.

FORBATH, W. E. (1985), "The Ambiguities of Free Labor: Labor and the Law in the Gilded Age", *Wisconsin Law Review,* pp. 767-817.

FRIED, C. (1968), "Privacy", en *The Yale Law Journal*, n.º 77, pp. 475-493.

GARZÓN, G. (1981), "La protección de datos y la función formativa del Consejo de Europa", *Revista de Instituciones Europeas,* vol. 8, núm. 1, pp. 9-25.

GROSSI, P. (1996). "Absolutismo jurídico y derecho privado en el siglo XIX", en *Derecho & Sociedad*, n.º 11, pp. 94-99.

HAN, B.-C., (2014), *Psicopolítica, Neoliberalismo y nuevas técnicas de poder* Barcelona., Herder.

HORNUNG, G., SCHNABEL, C. (2009), "*Data protection in Germany I: The population census decision and the right to informational self-determination",* en *Computer Law & Security Review,* 25, pp. 84-88.

KALVEN, H. Jr. (1966), "Privacy in Tort Law – Were Warren and Brandeis Wrong?, n.º 31, *Law & Contemporary Problems*, pp. 326-341.

KANG, J. (1998) "Information Privacy in Cyberspace Transactions", en *Stanford Law Review*, 50, pp. 1193-1294.

KAISER, B. (2019) *La dictadura de los datos. La verdadera historia desde dentro de Cambridge Analytica y de cómo el Big Data, Trump y Facebook rompieron la democracia, y cómo puede volver a pasar,* Madrid, HarperCollins.

LES BENEDICT, M. (1985), "Laissez-Faire and Liberty: A Re-Evaluation of the Meaning and Origins of Laissez-Faire Constitutionalism", 3 *Law & History Review,* pp. 293-331.

LESSIG, LAWRENCE (1999), *Code and Other Laws of Cyberspace,* New York, Basic Books.

LUCAS MURILLO DE LA CUEVA, P. (1993), "La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", en *El derecho a la autodeterminación informativa*, Madrid, Ed. Fundación Coloquio Jurídico Europeo, pp. 81-179.

MARTÍNEZ MARTÍNEZ, R. (2004), *Una aproximación crítica a la autodeterminación informativa*, Madrid, Ed. Civitas.

MANSON, A. (1946), *Brandeis: a Free Man's Life*, New York, Viking.

MURPHY, R. S. (1996), *Property Rights in Personal Information: An Economic Defense of Privacy, 84, Georgia Law Journal,* 84, 2381-2417.

POSNER, R. A. (1981), *The Economics of Justice*, Harvard University Press.

POST, R. C. (1989), "The Social Foundations of Privacy: Community and Self in Common Law Tort", en *California Law Review,* 77, pp. 957-1010.

PROSSER, W. (1960), "Privacy", en *Californian Law Review*, 48, pp. 383-423.

ROIG BATALLA, A. (2020), *Las garantías frente a las decisiones automatizas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica,* Barcelona, Bosch Editor.

ROTENBERG, M. (2001), "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get), *Stanford Technology Law Review,* pp. 26-39.

RUÍZ MIGUEL, C. (1944), *El Derecho a la Protección de la Vida Privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos*, Pamplona, Thomson — Reuters (Civitas).

SALDAÑA DÍAZ, M. N. (2011), "El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego", en *Teoría y Realidad Constitucional,* Universidad Nacional de Educación a Distancia (UNED), nº 28 (2011), Madrid, pp. 279-312.

— (2012), "«The right to privacy». La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario de Warren y Brandeis, *Revista de Derecho Político,* n.º 85, pp. 195-240.

SCHWARTZ P. M. (1999), "Privacy and Democracy in Cyberspace", en *Vanderbilt Law Review*, pp. 1609-1701.

— (2000), "Internet Privacy and the State", en *Conneticut Law Review*, pp. 815-859.

SCHWARTZ, P. M. y Solove, D. J., (2009), *Information Privacy: Statutes and Regulations 2010-2011*, New York, Ed. Wolters Kluwer (Aspen Publishing Co.).

SOLOVE, D. J., ROTENBERG, M., SCHWARTZ, P. M. (2005), *Information Privacy Law (Second Edition),* New York, Aspen.

TURKINGTON, R. C. (1990), "Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy", en *Northern Illinois University Law Review*, n.º 10, pp. 496-503.

VOLOKH, E. (2000), "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You", en *Stanford Law Review*, 52, pp. 1049-1124.

WARREN, S., Brandeis, L. (1890), "The Right to Privacy", *Harvard Law Review,* 4, n.º 5, pp. 193-220.

WESTIN, A. F. (1967), *Privacy and Freedom,* New York, Athenum.

ZIMMERMAN, D. (1983), "L. Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort", 68, *Cornell Law Review,* pp. 291-367.

ZITTRAIN, J. (2014), "Engineering an Election: Digital Gerrymandering Poses a Threat to Democracy", 127 *Harvard Law Review Forum*, 335 Disponible en www.harvardlawreview.org/2014/06/engineering-an-election/ (Consultado el 5-09-2022).

ZUBOFF, S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs.

I. Empresa y responsabilidad

La empresa de salud digital y la implementación de sistemas de IA: Cuestiones de responsabilidad civil en el nuevo marco europeo

Sandra Camacho Clavijo
Profesora agregada de Derecho Civil
Universitat Autònoma de Barcelona (España)

ABSTRACT:
The implementation of telemedicine and artificial intelligence (hereinafter AI) systems constitutes a solution to relieve a healthcare system pressured by the care consequences of an aging population. In this study, we will analyze the current degree of AI implementation in the clinical process and the civil liability issues that arise from the use of these systems as support tools for both diagnostic and therapeutic medical decisions. We will mainly focus on studying the medical-hospital liability for damages caused to the patient by AI system errors and the fit of this liability within our legal framework, but also within the new European liability framework composed of the AI Regulation and the proposed AI Liability Directive.

Keywords: Artificial intelligence, high-risk AI system, medical device, medical civil liability, professional diligence standard, deployment responsible.

Palabras Clave: Inteligencia artificial, sistema de IA de alto riesgo, producto sanitario, responsabilidad civil médica, estándar de diligencia profesional, responsable del despliegue.

SUMARIO:

1. LA EMPRESA DE SALUD DIGITAL Y LA IMPLEMENTACIÓN DE LA IA: HACIA UN CAMBIO EN EL MODELO ASISTENCIAL

Se estima que para el 2050 el número de personas de 65 años o más alcanzará el 16% de la población mundial. Este incremento de la esperanza de vida se asocia a un futuro aumento de las enfermedades crónicas. Así, la ONU y la OMS estiman que para el año 2025, el 70% de todas las enfermedades serán crónicas o comórbidas. Estos datos son la clave del importante incremento de costes de la asistencia sanitaria, pues se prevé que los costes sanitarios totales a escala mundial aumenten de 8'4 millones de dólares en 2015 a 18'3 billones en

2030[1]. La implementación de la telemedicina y de los sistemas de Inteligencia artificial (en adelante IA) constituyen una vía o solución para liberar un sistema sanitario presionado por las consecuencias asistenciales del envejecimiento de la población[2].

Esta solución es contemplada por la Comisión Europea que reconoce que las tecnologías tienen un protagonismo especial en el ámbito de la salud tanto en el impulso regulador de la IA, como en la Estrategia Europea de Datos[3]. Por su parte, en España también el artículo XXIII de la Carta de Derechos Digitales adoptada en 2021, regula sin carácter normativo el derecho a la protección de la salud en el entorno digital y en relación con la implementación de los sistemas de IA en la asistencia sanitaria y ordena que "*Los poderes públicos promoverán que la investigación y la tecnología contribuyan al logro de una medicina preventiva, predictiva, personalizada, participativa y poblacional*" y que, con relación al empleo de los sistema de IA de "*asistencia al diagnóstico, y en particular de procesos basados en inteligencia artificial no limitará el derecho al libre criterio clínico del personal sanitario*"[4].

Los nuevos modelos asistenciales que resultan de la implementación de las nuevas tecnologías tienen el propósito de reducir los costes y mejorar la calidad asistencial e imponen nuevos tipos de negocio en el sector sanitario: la transformación de las empresas de dispositivos médicos en entidades de servicios en las que el laboratorio y la gestión a distancia constituyen formas importantes de relacionarse, la ampliación de la cadena de valor de los proveedores de servicios médicos ya que monitorizan a los pacientes después del alta hospitalaria…etc.

---

1. Ver datos en Bohr, A/Memarzadeh,K; La asistencia sanitaria actual, los datos masivos y el aprendizaje automático; Dir. Bohr, A/Memarzadeh,K (2021), *Inteligencia artificial en el ámbito de la salud,* pp. 1-24, Elsevier. Academic Press.

2. Reiter, B/Tureck,J/Weindenfeld, W, (2011) Telemedizin-ZUkunftsgut im Gesundheitswesen*, C.A.P. Analyse*, 1/2011, pp 1-25.

3. Vid como ejemplo documentos publicados por la Comisión Europea en febrero de 2020. Vid. Comisión Europea, Comunicación de la Comisión «Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza». Bruselas, 19.02.2020. COM (2020) 65 final. Disponible en: https://ec.europa.eu/info/sites/info/files/commission-white- paper-artificial-intelligence-feb2020_es.pdf; Comisión Europea Comunicación de la Comisión «Una Estrategia Europea de Datos». Bruselas, 19.02.2020. COM (2020) 66 final. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0066.

Por su parte, el Grupo de Trabajo en Inteligencia Artificial (GTIA) cuya misión principal ha sido realizar un borrador que sirva como base para diseñar y aprobar una Estrategia de I+D+I en Inteligencia Artificial, admite que la salud es uno de los sectores estratégicos a promover por el Plan Coordinado de la IA, Ver informe "ESTRATEGIA ESPAÑOLA DE I+D+I EN INTELIGENCIA ARTIFICIAL" emitido por el Ministerio de Ciencia, Innovación y Universidades, en fecha 2019 (Vid www.ciencia.gob.es), consultada en fecha 8 de mayo de 2024. De conformidad con el informe: "*la IA permitirá ahorrar miles de millones de euros al mejorar la prevención, el diagnóstico y el tratamiento de la obesidad infantil, las enfermedades cardiovasculares y sus secuelas, las enfermedades neurodegenerativas y el cáncer de mama, entre otros ámbitos. Además, permitirá desarrollar nuevos medicamentos y fomentar la medicina personalizada y domiciliaria o mejorar la calidad de vida de los ancianos."*

4. Ver carta de derechos digitales presentada en fecha 24 de julio de 2021 https://lamoncloa.gob.es

En suma, en el futuro será muy común la asociación entre sector sanitario (farmacéuticas, fabricantes de dispositivos) y las empresas de tecnologías (Google, IBM, Apple o Microsoft).

En este marco transformador del sistema sanitario, la implementación de los sistemas de IA adquiere relevancia. Éstos aportarán mejoras en los procesos que constituyen la prestación sanitaria pero también comportarán un ahorro de costes debido al cambio del modelo asistencial a un modelo proactivo centrado en la gestión de la salud más que en el tratamiento de la enfermedad[5].

2. EL SISTEMA DE IA CON FINALIDAD MÉDICA: CALIFICACIÓN JURÍDICA

2.1. Concepto de sistema de IA en el Reglamento de IA

Se habla de Inteligencia Artificial cuando una máquina imita las funciones cognitivas del ser humano. Una de esas cualidades es la capacidad de aprender. La rama de la Inteligencia Artificial que proporciona a las computadoras la capacidad de aprender desde los datos, sin ser programadas explícitamente es la que se conoce como *machine learning* o aprendizaje automático. El aprendizaje profundo es posible gracias al funcionamiento de un algoritmo o modelo matemático que resume las propiedades de los datos utilizados en su entrenamiento, generalmente con un objeto predictivo, aunque también puede ser diagnóstico (exploratorio) o prescriptivo (predicción tras intervención). Como veremos en este trabajo este tipo de IA es la que mayor impacto tiene en el proceso clínico[6].

La diversidad de definiciones de IA propuestas por la comunidad científica ha dificultado el camino hacia una única definición de la Inteligencia Artificial y en consecuencia la tipificación legal de un concepto de IA ha sido compleja. Así la inicial propuesta de Reglamento de IA definía la IA por remisión a propuestas normativas posteriores como la reciente Propuesta de Directiva sobre responsabilidad en materia de IA[7]. En ésta, la inteligencia artificial es definida como "*el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en*

5. Bohr, A/Memarzadeh,K; El auge de la inteligencia artificial en las aplicaciones sanitarias; Dir. Bohr, A/Memarzadeh,K (2021), *Inteligencia artificial en el ámbito de la salud,* , Elsevier. Academic Press. pp. 1-24

6. Beunza, J.J/Condés, E; "Conceptos" en Beunza, JJ et Al. (2023), *Manual práctico de Inteligencia Artificial en entornos sanitarios,* Elsevier, Barcelona, pp. 7-17.

7. Ver propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA), Bruselas, 28.9.2022 COM (2022) 496 final, 2022/0303 (COD9).

los entornos con los que interactúa". Esta definición había sido criticada porque, las estrategias enumeradas en el Anexo I[8] eran tan amplias que incluso simples programas informáticos quedarían incluidos en esta categoría[9]. Sin duda, el legislador europeo al proponer una definición tan amplia, buscaba incluir tanto los sistemas de IA simples, con poco o ningún impacto en el entorno, como los sistemas más complejos que pueden tener graves efectos en intereses generales como son la vida o la integridad física de las personas.

Finalmente, el art. 3 del Reglamento europeo por el que se establecen normas armonizadas en materia de inteligencia artificial (en adelante Reglamento IA), en su última versión corregida de abril de 2024[10], define el sistema de IA como: "*un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales*". Con esta definición el Reglamento IA propone un concepto más restrictivo que subsana los defectos de la amplia definición anterior. Por otra parte, en esta definición se identifican aquellas características especiales del sistema de IA que permiten su diferenciación del simple software o de la programación más sencilla.

Conforme el Considerando 12 del Reglamento IA las características especiales del sistema de IA son:

a) El sistema de IA no es un software sino un "*sistema basado en una maquina*" y conforme relata el Considerando, se refiere al hecho de que los sistemas de IA se ejecutan en máquinas. El concepto recoge así la advertencia de parte de la comunidad científica que, con relación a la definición de la IA defendían que, el conjunto de instrucciones que se facilitan a la computadora para que, a partir de los datos de entrada construya unos datos de salida, son siempre implementadas por una máquina[11].

---

8. Las estrategias citadas en el Anexo I de la Propuesta de Ley de IA son: "Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo. Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico). Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización"

9. Thiermann, A/ Böck, R.N; (2022), "Künstliche Intelligenz in Medizinprodukten Regulatorisches Regelwerk und Haftungsvorgaben", *Recht digital* (Rdi), 333, Pisani, C/Stief, M, (2022), „Regulatorische und haftungsrechtliche Herausforderungen für KI-Medizinprodukte" en *Medizinprodukterecht im Wandel. Festschrift für Ulrich M. Gassner zum 65. Geburtstag*, Nomos, Baden-Baden, p. 472, IQBAL.

10. Art 3. 1) del Reglamento de IA (versión corregida de 16.04.2024), COM (2021)0206 – C9-0146/2021 – 2021/0106(COD) (RR\P9_TA(2024)0138_ES.docx.

11. Ver en este sentido estudio del concepto en Beunza, J.J/Condés, E; "Conceptos", ob.cit.p.7

b) El sistema de IA tiene *la capacidad de inferencia* que se refiere al proceso de obtención de resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que puede influir en entornos físicos y virtuales. En la construcción de un sistema de IA se aplican técnicas que permiten la inferencia y que incluyen estrategias de aprendizaje automático que aprenden de los datos. Gracias a estos datos los sistemas conciben cómo alcanzar determinados objetivos y estrategias basadas en la lógica y también obtienen el conocimiento que infieren a partir de conocimientos codificados o de una representación simbólica de la tarea que debe resolverse. La capacidad de inferencia de un sistema de IA trasciende el tratamiento básico de datos que podemos encontrar en la programación tradicional, pues permiten el aprendizaje, el razonamiento o la modelización.
c) El sistema de IA tiene la *capacidad para deducir modelos o algoritmos,* o ambos, a partir de información de entrada o datos.
d) El sistema de IA tiene la *capacidad de adaptación*: Los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía, lo que significa que pueden actuar con cierto grado de independencia con respecto a la actuación humana y tienen ciertas capacidades para funcionar sin intervención humana. La capacidad de adaptación que un sistema de IA podría mostrar tras su despliegue se refiere a las capacidades de autoaprendizaje que permiten al sistema cambiar mientras está en uso.

2.2. El sistema de IA con finalidad médica como sistema de IA de alto riesgo y como producto sanitario

Los sistemas de IA con finalidad médica son calificados como sistemas de IA de alto riesgo conforme al Reglamento IA, pero también son calificados como productos sanitarios desde el punto de vista del Derecho Comunitario. Veamos a continuación los elementos atributivos en ambas categorías y sus consecuencias jurídicas:

a) El sistema de IA con finalidad médica constituye un producto sanitario conforme la definición de producto sanitario del actual Reglamento UE 2017/745 sobre productos sanitarios (en adelante *Medical Devices Regulation* o MDR): "*todo instrumento, dispositivo, equipo, programa informático, implante, reactivo, material u otro artículo destinado por el fabricante a ser utilizado en personas, por separado o en combinación, con alguno de los siguientes fines médicos específicos: diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad*"[12].

12. Reglamento (UE) 2017/745 Del Parlamento Europeo y del Consejo de 5 de abril de 2017 sobre los productos sanitarios (DOUE-L-2017-80916).

Así, conforme el art. 2.1. del MDR el software que utiliza IA con fines médicos, de diagnóstico, prevención y tratamiento de enfermedades está considerado como producto sanitario y para ser comercializado e introducido en el mercado de la Unión europea, al igual que cualquier otro dispositivo médico, deberá llevar el marcado CE[13].

Para obtener el marcado CE, el art. 51 y 52 del MDR establecen que el software deberá ser sometido a un procedimiento de evaluación de conformidad que viene determinado en función de la clasificación del producto sanitario. En este caso, el software con finalidad médica puede ser clasificado de clase II a, II b o III según su función y uso: *"Los programas informáticos destinados a proporcionar información que se utiliza para tomar decisiones con fines terapéuticos o de diagnóstico se clasifican en la clase IIa, salvo si estas decisiones tienen un impacto que pueda causar:— la muerte o un deterioro irreversible del estado de salud de una persona, en cuyo caso se clasifican en la clase III, o — un deterioro grave del estado de salud de una persona o una intervención quirúrgica, en cuyo caso se clasifican en la clase IIb."* (regla número 11 del Anexo VIII del MDR)[14].

b) *El sistema de IA con finalidad médica constituye un sistema de IA de alto riesgo*: La herramienta de inteligencia artificial con finalidad médica es también un sistema de IA de alto riesgo conforme el art 6 del Reglamento IA[15]. Esta calificación es acertada atendiendo que el funcionamiento del sistema de IA con finalidad médica puede comprometer derechos fundamentales como la salud, pero también el derecho a la protección de datos personales, en su especial categoría de datos de salud (art 9 RGPD)[16].

---

13. En la labor de delimitar el concepto de 'producto sanitario' es relevante la Sentencia TJUE (Sala Cuarta), de 7 de diciembre de 2017 (Caso Snitem), cuyo considerando 25 prevé que "*Un programa informático que realiza un cotejo de los datos propios del paciente con los medicamentos que el facultativo pretende prescribir, siendo con ello capaz de proporcionarle automáticamente un análisis para detectar, en particular, las posibles contraindicaciones, interacciones de medicamentos y posologías excesivas, se utiliza con fines de prevención, control, tratamiento o alivio de una enfermedad y persigue, en consecuencia, una finalidad específicamente médica, lo que lo convierte en un producto sanitario en el sentido del artículo 1, apartado 2, letra a), de la Directiva 93/42*" y conforme el Considerando 32 de la misma sentencia:" *para que los programas informáticos sean calificados como productos sanitarios poco importa que actúen o no directamente en el cuerpo humano, siendo lo esencial que su finalidad sea específicamente una de las contempladas en el apartado 24 de la presente sentencia"*. Ver Sentencia TJUE (Sala Cuarta), de 7 de diciembre de 2017 (C-329/16), *Caso Snitem y Philips France*.

14. Ver Dettling, H.U; (2019) „Künstliche Intelligenz und digitale Unterstützung ärztlicher Entscheidungen in Diagnostik und Therapie", *PharmaRecht*, 633.

15. Así resulta de la remisión del artículo 6 al Anexo I, sección A, regla núm. 11 y 12 del Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de IA (Ley de Inteligencia Artificial) de 21.04.2021 (COM 2021, 206 final), 2021/0106 (COD).

16. También en Díaz Hernández, M; (2023), "El Reglamento de Inteligencia Artificial: Un análisis desde el punto de vista sanitario" en *Derecho y Salud,* vol 33 , pp.25-44.

La calificación del sistema de IA como sistema de alto riesgo implica que, para su comercialización, requiere el cumplimiento de los requisitos de la sección II, del Capítulo III del Reglamento de IA. El sistema será sometido a un proceso de evaluación en el que se comprobará el cumplimiento de los siguientes requerimientos legales que podemos clasificar en tres tipos: de gestión y control de riesgos, de uso de datos y documentación; y de información y transparencia.

1º) Obligaciones de gestión y control de riesgos:

En el proceso de evaluación se comprobará que el sistema cumple con la obligación de disponer de un sistema de gestión de riesgos (art.9), que es un proceso iterativo continuo, planificado y ejecutado a lo largo de todo el ciclo de vida de un sistema de IA de alto riesgo y que requiere una revisión y actualización periódicas y sistemáticas. La gestión de riesgos comprende tres etapas: 1ª etapa) la de identificación y el análisis de los riesgos conocidos y de los riesgos razonablemente previsibles que el sistema de IA de alto riesgo puede plantear para la salud, la seguridad o los derechos fundamentales cuando el sistema de IA de alto riesgo se utilice de acuerdo con su finalidad prevista; 2ª etapa) la estimación y evaluación de los riesgos que pueden surgir cuando el sistema de IA de alto riesgo se utiliza de acuerdo con su finalidad prevista, y en condiciones de uso indebido razonablemente previsibles y; 3ª etapa) la evaluación de otros riesgos que puedan surgir, basada en el análisis de los datos recogidos en el sistema de seguimiento en la poscomercialización[17]. Estas etapas vienen acompañadas de la consecuente adopción de medidas adecuadas y específicas de gestión de riesgos. El objetivo es eliminar o reducir los riesgos y, de ser imposible mitigarlos y controlarlos.

2º) Obligaciones relativas al uso de datos:

En congruencia con la legislación sobre protección de datos, en el caso de que el sistema de IA utilice técnicas que implican *el entrenamiento de modelos de IA con datos* (art. 10), este entrenamiento se desarrollará sobre la base de conjuntos de datos de entrenamiento, validación y prueba que cumplan los criterios de calidad, es decir datos sujetos a prácticas de gobernanza y gestión de datos adecuadas a la finalidad prevista del sistema de IA de alto riesgo. Algún autor señala en este caso, la extrañeza que causa, la derogación fáctica, aunque suavizada por la obligación de *pseudonimización* o cifrado, de la prohibición de procesar datos de categorías especiales del art. 9 RGPD[18]. Entendemos que la justificación puede deberse a que una prohibición en tal sentido frenaría el desarrollo de la implementación de los sistemas de IA.

17. Este plan de vigilancia de poscomercialización viene a ser regulado en artículo 72 del Reglamento de IA

18. Ver Díaz Hernández, M; (2023), "El Reglamento de Inteligencia Artificial: Un análisis desde el punto de vista sanitario…", ob.cit.p. 30.

3º) Obligaciones de información y transparencia:

El Reglamento fija la obligada existencia de una documentación técnica del sistema de IA de alto riesgo que se elaborará antes de su comercialización o puesta en servicio y se mantendrá actualizada (art. 11). Además, se comprobará que los sistemas de IA de alto riesgo: a) deberán permitir técnicamente el registro automático de eventos (logs) durante la vida útil del sistema (art. 12); y b) deberá ser diseñado y desarrollado de forma que garantice que su funcionamiento lo suficientemente transparente como para permitir a los implantadores interpretar los resultados del sistema y utilizarlos adecuadamente (art 13). Con esta finalidad también deberán ir acompañados de instrucciones de uso en un formato digital adecuado o de otro tipo que incluya información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para quienes los desplieguen.

2.3. El Sistema de IA con finalidad médica: la simultaneidad y complementariedad de evaluaciones para su comercialización

Según lo estudiado *ut supra*, el sistema de IA con finalidad médica quedará entonces sometido a una aplicación simultánea y complementaria del procedimiento de evaluación del MDR y también del proceso de evaluación del cumplimiento de los requisitos del título II del Reglamento IA. Así lo reconoce el propio considerando 64 del Reglamento IA que establece que es norma general que "*más de un acto jurídico de la legislación de armonización de la Unión puede ser aplicable a un producto, ya que la comercialización o la puesta en servicio solamente puede producirse cuando el producto cumple toda la legislación de armonización de la Unión aplicable*".

¿Cuál sería el fundamento de este doble proceso evaluador simultáneo? El mismo Reglamento califica la actuación evaluadora como complementaria y la justifica en la distinta finalidad que ambos procedimientos cumplen: "*Los peligros de los sistemas de IA cubiertos por los requisitos del presente Reglamento se refieren a aspectos diferentes de los contemplados en la legislación de armonización de la Unión existente y, por consiguiente, los requisitos del presente Reglamento completarían el conjunto existente de legislación de armonización de la Unión. Por ejemplo, las máquinas o los productos sanitarios que incorporan un sistema de IA pueden presentar riesgos de los que no se ocupan los requisitos esenciales de salud y seguridad establecidos en la legislación armonizada de la Unión pertinente, ya que esa legislación sectorial no aborda los riesgos específicos de los sistemas de IA"* (Considerando 64).

Ahora bien, con el fin de evitar una carga administrativa excesiva para los proveedores de aquellos productos que, como el sistema de IA con finalidad médica, deban someterse a diferentes evaluaciones, el Reglamento IA propone una flexibilidad en la manera de garantizar su conformidad. Una flexibilidad que, según señala el propio Reglamento en ningún caso significará la relajación

en la obligación del proveedor de cumplir todos los requisitos aplicables. El considerando 64 nos pone un ejemplo de cómo llevar a cabo dicha flexibilidad: "*la decisión del proveedor de integrar una parte de los procesos de prueba y notificación necesarios, así como la información y la documentación exigidas en virtud del presente Reglamento, en la documentación y los procedimientos ya existentes exigidos en virtud de los actos legislativos de armonización de la Unión vigentes basados en el nuevo marco legislativo*", en nuestro caso, la integración se daría en los procedimientos exigidos en el MDR.

En suma, una vez realizados todos los procesos de evaluación y cumplidos todos los requisitos, la robustez técnica y consistencia del funcionamiento de los sistemas de IA de alto riesgo reduce considerablemente el riesgo de errores del sistema. Ahora bien, si el sistema de IA con finalidad médica emite una predicción errónea o existe un erróneo funcionamiento y las consecuencias derivadas son graves, causando daños en el paciente e incluso la muerte ¿Quien asume la responsabilidad de indemnizar los daños causados en el paciente por un fallo predictivo del sistema de IA?

3. LA APLICACIÓN DEL SISTEMA DE IA EN EL SERVICIO MÉDICO: HACIA UNA TRANSFORMACIÓN DE LA ACTIVIDAD HUMANA

Actualmente, las herramientas basadas en IA y en algoritmos de *machine learning* (en adelante ML) o de aprendizaje automático en particular, inciden en todo el proceso clínico en el que es posible su implementación: desde la actividad de cribaje hospitalario, pasando por la actividad asistencial y finalizando con el seguimiento y predicción de resultados. La técnica del ML es uno de los componentes más esenciales de la IA y se define como el proceso mediante el cual el ordenador, a través de algoritmos, tiene la capacidad de identificar patrones en datos masivos y elaborar predicciones (análisis predictivo) sin programación explícita[19].

La mayor parte de los algoritmos de IA disponibles en salud (diagnóstico de neumonía en radiografía de tórax, predicción de riesgo coronario basado en parámetros analíticos, diagnóstico oncológico por análisis de muestra patológica, ...etc.) dan respuesta a una necesidad puntual y concreta con resultados muy superiores a los modelos y herramientas clásicas. Por tanto, representan una

19. Una de las técnicas de ML más utilizada es el Deep Learning que utiliza una red neuronal para procesar los datos. La red neuronal procesa la señal en capas que incluyen unidades computacionales. Estas redes están formadas por una capa de entrada, una capa oculta y una capa de salida, que están interconectadas. Los datos introducidos a través de la capa de entrada se procesan matemáticamente en la capa oculta, y las predicciones se transmiten a la capa de salida. El aprendizaje profundo moderno implica más de una capa oculta para proponer patrones más complejos. Ver Sánchez-Salmerón, R et al. (2022) "Machine learning methods applied to triage in emergency services: a systematic review", *International Emergency Nursing,* Vol. 60, Elsevier,, article 101109.

herramienta de apoyo en la decisión médica que potencia la capacidad diagnóstica y terapéutica de los profesionales. La finalidad de estas herramientas puede ser variada, de diagnóstico, de prognosis o de elección terapéutica, pero también de ayuda en las decisiones tomadas en el cribaje del servicio de urgencias hospitalario[20].

> Los sistemas construidos mediante el aprendizaje automático, y especialmente el aprendizaje profundo, para el diagnóstico basado en imagen médica es un ejemplo de esta implementación. Especialidades como radiología, dermatología, oftalmología, cardiología u oncología se sirven de esta herramienta. A modo de ejemplo los sistemas de IA se están implementando para definir la susceptibilidad de las personas al cáncer, para mejorar el diagnóstico y estadificación del cáncer y para predecir la respuesta al tratamiento[21]. El sistema de IA también se implementa para la prognosis, es decir para la predicción en la salud, así por ejemplo para la predicción de muertes prematuras por patologías crónicas o la predicción de obesidad a partir de datos tanto sociodemográficos y ambientales como genéticos, y en general, sistemas basados en la identificación de individuos con determinadas enfermedades o afecciones y su clasificación según el estadio, la gravedad y otras características. El aprovechamiento de esta capacidad "predictiva" podría ser especialmente útil a la hora de optimizar la actuación y asignación de recursos en servicios de emergencia o a la hora de detectar posibles imprevistos en el transcurso de operaciones quirúrgicas[22].

Si bien la implementación del sistema de IA plantea un debate centrado en preguntarnos si el funcionamiento automatizado del sistema conllevará la sustitución humana, en este caso la sustitución del facultativo, compartimos la opinión de otros autores que consideran que, en la actualidad, la principal cuestión que se plantea es otra. En efecto, la importancia de la actual implementación de los sistemas de IA en la asistencia sanitaria como herramientas de apoyo en las decisiones médicas, nos indica que una de las principales consecuencias de su aplicación será la transformación de la actividad humana, no su sustitución[23]. En consecuencia, las cuestiones jurídicas más relevantes están estrechamente rela-

---

20. Así el propio Considerando 58 pone como ejemplo de sistema de IA de alto riesgo los sistemas de IA empleados para evaluar y clasificar llamadas de emergencia de personas físicas en los sistemas de triaje de pacientes para la asistencia sanitaria de emergencia, ya que adoptan decisiones en situaciones sumamente críticas para la vida y la salud de las personas y de sus bienes. Para ampliar sobre las consecuencias jurídicas de estas herramientas de triaje ver Camacho Clavijo, S. "AI assessment tools for decision-making on telemedicine: liability in case of mistakes". *Discov Artif Intell* 4, 24 (2024). https://doi.org/10.1007/s44163-024-00117-4.

21. Ver estudio en Minerzami, R; "Decisiones de diagnóstico y tratamiento del cáncer mediante Inteligencia Artificial", en Dir. Bohr, A/Memarzadeh,K (2021), *Inteligencia artificial en el ámbito de la salud,* Elsevier. Academic Press, pp. 1-24.

22. Ver análisis de los algoritmos utilizados en salud en Beunza, J.J. "Algoritmos disponibles en la práctica sanitaria", Beunza, JJ et Al. (2023), *Manual práctico de Inteligencia Artificial en entornos sanitarios,* Elsevier, Barcelona, pp. 19-39.

23. Ver en este sentido Lazcoz Moratinos, G (2022) "*Sistemas de Inteligencia Artificial en la Asistencia Sanitaria: Cómo Garantizar la supervisión humana desde la normativa de protección de*

cionadas con esta transformación de la actividad humana. Podemos poner como ejemplo, en particular, la cuestión relativa a la identificación del tipo de conducta requerida cuando el profesional utiliza la IA. Esta conducta actuará como modelo de determinación del cuidado y precisión exigible de acuerdo con las circunstancias y los riesgos inherentes a la utilización del sistema de IA, constituyendo el estándar de diligencia exigible que se espera en la actuación diligente del profesional médico.

En el ámbito sanitario, existe una gran incertidumbre en la determinación de quién es el responsable en el caso de errores en la predicción o consejo emitido por el sistema de IA utilizado en la asistencia médica y qué modelo de diligencia será exigido al profesional médico que utilice el sistema de IA. Este tema es relevante pues el éxito de la implementación de la IA en las decisiones médicas dependerá en gran medida de la confianza y seguridad que para los profesionales médicos genere los sistemas de predicciones basados en algoritmos[24].

A continuación, analizaremos la responsabilidad civil tanto médica como hospitalaria por la utilización del sistema de IA con finalidad médica y si esta cuestión puede quedar resuelta al amparo de la nueva propuesta de Directiva sobre responsabilidad en materia de IA de 28 de septiembre de 2022[25].

4. LA RESPONSABILIDAD CIVIL MÉDICA Y HOSPITALARIA POR LA UTILIZACIÓN DEL SISTEMA DE IA EN LA PROPUESTA DE DIRECTIVA SOBRE RESPONSABILIDAD EN MATERIA DE IA.

Como hemos avanzado *ut supra* el sistema de IA con finalidad médica es considerado un sistema de alto riesgo conforme el art. 6 del Reglamento de IA. La cuestión que nos preguntamos es quién será responsable de los daños causados en el paciente por la errónea predicción del sistema de IA. En materia de responsabilidad civil extracontractual por la utilización de un sistema de IA, el artículo 4 de la propuesta de Directiva sobre responsabilidad de IA prevé una presunción refutable de relación de causalidad entre la culpa del demandado y

datos" Premio de Investigación en Protección de Datos. Personales *Emilio Aced* correspondiente al año *2022*.

24. A modo de ejemplo una revisión de las aplicaciones basadas en algoritmos de aprendizaje automático para evaluar el riesgo de cáncer de piel reveló metodologías deficientes y concluyó que el actual proceso de regulación del "marcado CE" no proporciona una protección adecuada, en este sentido estudio en Freeman et al., (2020) "Algorithm based smartphone apps to assess risk of skin cancer in adults: systematic review of diagnostic accuracy studies", *BMJ,* Feb, doi: 10.1136/bmj.m127

25. Nos referimos a la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA) de 28.9.2022, COM/2022/496 final, 2022/0303(COD).

el resultado producido por el sistema de IA (o la no producción de resultados)[26]. El mismo precepto distingue entre la demanda por daños y perjuicios dirigidos contra un proveedor del sistema de IA y la demanda de daños y perjuicios dirigida contra un usuario del sistema de IA.

Nos preguntaremos a continuación si al amparo de la propuesta de Directiva sobre responsabilidad en materia de IA, puede prosperar una demanda de responsabilidad extracontractual subjetiva médico-hospitalaria por los daños causados por una decisión basada en una predicción de un sistema de IA. Esta cuestión plantea toda una serie de cuestiones que analizaremos a continuación.

4.1. ¿Quién es responsable del despliegue del sistema de IA con finalidad médica: el facultativo o el Hospital o sociedad empresarial sanitaria?

La primera cuestión relevante que nos formulamos es si el facultativo puede tener legitimación pasiva en la demanda de responsabilidad extracontractual interpuesta por los daños producidos por un sistema de IA. La Propuesta de Directiva sobre responsabilidad en materia de IA, identifica como sujeto pasivo al sujeto que actúa como proveedor y al usuario del sistema de IA con finalidad médica. Generalmente el facultativo que preste un servicio sanitario utilizando una herramienta de IA no será considerado proveedor ya que su actuación se circunscribirá al uso de la herramienta y de conformidad con el Reglamento se considera proveedor a la "*persona física o jurídica, autoridad pública, agencia u otro organismo que desarrolle un sistema de IA o un modelo de IA de propósito general o que haga desarrollar un sistema de IA o un modelo de IA de propósito general y lo comercialice o ponga en servicio el sistema de IA bajo su propio nombre o marca, ya sea a cambio de una remuneración o de forma gratuita*".

Ahora bien, ¿Puede ser considerado usuario? La propuesta de Directiva sobre responsabilidad en materia de IA define el término de usuario por remisión al art 3. 4 del Reglamento de IA, pero en el aprobado Reglamento de IA el concepto de usuario ha sido suprimido y en su lugar se utiliza el término de "responsable del despliegue" que se define como ""*una persona física o jurídica, autoridad pública, agencia u otro organismo que utilice un sistema de IA bajo su autoridad, excepto cuando el sistema de IA se utilice en el curso de una actividad personal no profesional*".

De la literalidad del precepto resultaría que, a efectos de responsabilidad civil sanitaria por la utilización del sistema de IA, es el Hospital el encargado del despliegue del servicio sanitario que utiliza el sistema de IA y por tanto, actúa como responsable del despliegue del sistema de IA, o dicho en los términos que

26. Conforme el art. 4.7 de la Propuesta de Directiva sobre responsabilidad en materia de IA, la presunción es refutable y el demandado tiene la posibilidad de refutarla demostrando que la culpa no puede haber sido la causante del daño.

la norma emplea, sería la autoridad bajo la que se utiliza dicho sistema. En suma, aquellas demandas de responsabilidad extracontractual dirigidas por el paciente contra el Hospital por los daños producidos por la utilización del sistema de IA podrían ser tramitadas conforme la propuesta de Directiva sobre responsabilidad en materia de IA. Lo que nos lleva a cuestionarnos en qué caso el régimen de responsabilidad hospitalario es extracontractual.

En el Ordenamiento jurídico español, la vinculación entre el centro hospitalario y el paciente en el ámbito sanitario privado puede revestir diversas modalidades, aunque en la mayoría de estos supuestos la relación que se establece entre el paciente y la clínica suele ser extracontractual. Veamos las modalidades: a) existencia de un contrato entre la clínica y el paciente; b) existencia de un seguro de asistencia médica suscrito entre una compañía aseguradora que a su vez contrata los servicios médicos con una serie de establecimientos y profesionales sanitarios y; c) existencia de un contrato con el médico que, a su vez mantiene un contrato de colaboración con la clínica[27].

Excluyendo el primer supuesto en el que la relación con el servicio hospitalario es contractual, en las otras dos modalidades se establece un vínculo extracontractual entre el paciente y la clínica. Sin embargo, la relación médico-paciente sería extracontractual en el primer y segundo caso, mientras que en el tercer supuesto el vínculo entre paciente y médico es contractual. De todas las modalidades expuestas, en sanidad privada, la situación más común es que el servicio sanitario se realice en el marco de un seguro médico. En éste, la relación jurídica es contractual con la Compañía de Seguros, pero extracontractual entre el paciente y el médico y entre el paciente y el Hospital.

En suma, la demanda por daños y perjuicios causados por la utilización del sistema de IA dirigida contra el Hospital podría prosperar conforme la Propuesta de Directiva sobre responsabilidad en materia de IA. La cuestión que se plantea entonces es si puede ser demandado el facultativo junto con el Hospital que actúa como responsable del despliegue "*strictu sensu*". A esta cuestión dedicaremos el siguiente epígrafe.

4.2. La conducta del "responsable del despliegue" jurídicamente reprochable de conformidad con la Propuesta de Directiva sobre responsabilidad en materia de IA: ¿Hacia una interpretación amplia del concepto de "responsable del despliegue"?

Una segunda reflexión en la que debemos detenernos es, en qué casos la actuación del responsable del despliegue del sistema de IA es jurídicamente

27. Ver en este sentido análisis en Rodríguez López, P (2004); *Responsabilidad médica y hospitalaria,* Bosch, Barcelona, p. 143, Plaza Penadés; J (2002); *El Nuevo Marco de la Responsabilidad Médica y Hospitalaria,* Aranzadi, Navarra, p. 49.

reprochable y activará la presunción de relación de causalidad entre la culpa del demandado y el resultado producido por el sistema de IA prevista en la Propuesta de Directiva. Si atendemos al texto de la propuesta de Directiva, en ésta se indica que no toda culpa da lugar a la presunción de relación de causalidad y para el supuesto de responsable del despliegue, se prevé que deberá probarse:

a) Que concurra la culpa por incumplimiento de un deber de diligencia: En el caso de sistema de IA de alto riesgo, la Propuesta de Directiva determina la concurrencia de la culpa del responsable del despliegue si se prueba:

— Que el responsable del despliegue, en este caso el Hospital, no cumplió con sus obligaciones de *utilizar o supervisar el sistema de IA de conformidad con las instrucciones de uso adjuntas* o en su caso de *suspender o interrumpir su uso con arreglo al art 29 de la Ley de IA*. En este caso, es evidente que se refiere a las obligaciones del art. 26 del Reglamento de IA aprobado y que se refieren a las obligaciones del responsable del despliegue, ya que en este Reglamento ha desparecido el concepto de usuario.

— Que el responsable del despliegue, en este caso, el Hospital expuso el sistema de IA a datos de entrada bajo su control que no eran pertinentes habida cuenta de la finalidad prevista. Los datos de entrada se refieren de conformidad con el Reglamento de IA a "*los datos proporcionados a un sistema de IA o adquiridos directamente por éste, a partir de los cuales el sistema produce un resultado"* (art 3).

No parece arriesgado aventurar que los supuestos de conducta reprochable para el responsable del despliegue aquí analizados y regulados por la Propuesta de Directiva sobre responsabilidad en materia de IA pueden sufrir modificaciones en orden a su adecuación al texto del Reglamento de IA. En primer lugar, porque en el Reglamento de IA desparece el término de usuario y pasa a ser sustituido por el de responsable del despliegue cuyo alcance, como hemos analizado, es más restringido y parece excluir al usuario. En segundo lugar, la regulación de los supuestos de conducta reprochable del "responsable del despliegue" deberán ajustarse a las obligaciones impuestas y tipificadas en el art. 26 del Reglamento de IA.

Con relación a este comportamiento o modelo de conducta al que la Propuesta de Directiva sobre responsabilidad en materia de IA, en caso de infracción, asocia la culpa del responsable del despliegue, nos preguntamos si la actuación del facultativo queda contemplada, al ser considerado usuario material necesario en el despliegue del sistema IA. Por ejemplo, si queda acreditado en el procedimiento que el facultativo incumplió la obligación de seguir las instrucciones de uso en la utilización del sistema de IA o que expuso el sistema de IA a datos no pertinentes. En este caso, si atendemos a una interpretación amplia del concepto de responsable del despliegue, podría concurrir también la responsabilidad del facultativo de conformidad con la Propuesta de Directiva. Se daría

en este supuesto una culpa in operando de ambos, porque pueda probarse que, tanto el Hospital como el médico hayan infringido los deberes de conducta establecidos en la utilización del sistema de IA. En todo caso, se tendrá que esperar a la aprobación del texto definitivo de la Propuesta de Directiva sobre responsabilidad en materia de IA para conocer si esta interpretación es posible.

Finalmente, junto a este requisito de prueba de la infracción del deber de diligencia, la Propuesta de Directiva exige la concurrencia de otros dos requisitos para activar la presunción del nexo causal del art 4:

b) Deberá probarse como razonablemente probable que la culpa ha influido en los resultados producidos por el sistema de IA[28] y;
c) Deberá probarse que la información da salida del sistema de IA causó los daños.

4.3. La equiparación entre culpa y requisitos de conducta del agente en la Propuesta de Directiva sobre responsabilidad en materia de IA

En suma, en la Propuesta de Directiva sobre responsabilidad en materia de IA, la prueba del comportamiento dañoso del implantador implicaría dar por probado el criterio de imputación. De esta forma, el comportamiento del agente causante del daño es el fundamento jurídico de su responsabilidad y, por lo tanto, la culpa queda asimilada con la infracción material de los requisitos de conducta tipificados en la Propuesta de Directiva.

Este es un ejemplo de cómo la utilización de los sistemas de IA en la actividad profesional imprime una transformación en la actividad humana y en particular, en cómo ésta se integra en el concepto jurídico de diligencia profesional. En efecto, en este caso, la verificación de una mera infracción de la actividad humana legalmente establecida determina el automático reconocimiento del incumplimiento de la diligencia profesional. El estándar de diligencia exigible se corresponde aquí con el cumplimiento de unos deberes establecidos legalmente, de forma que su incumplimiento comportará la culpa del agente. En suma, la necesaria valoración jurídica sobre la existencia de la culpa del agente que causa el daño (sea proveedor, sea responsable del despliegue), desaparece y queda reducida a una mera comprobación de la infracción material de los deberes legalmente establecidos[29].

---

28. Por ejemplo, no se considera razonablemente probable que, el incumplimiento de la obligación de presentar ciertos documentos o del registro ante la Autoridad (aunque esté previsto para la actividad concreta o esté previsto para el funcionamiento del sistema de IA) haya influido en la información de salida producida por el sistema de IA o en la no producción de la información de salida. Ver Considerando 25 de la Propuesta de Directiva sobre responsabilidad en materia de IA.

29. En este sentido ver Navas Navarro, S (2022); "Régimen Europeo en ciernes en materia de responsabilidad derivada de los sistemas de Inteligencia Artificial", *Revista CESCO de Derecho de Con-*

5. LA UTILIZACIÓN DEL SISTEMA DE IA POR EL FACULTATIVO: HACIA UNA REVISIÓN DEL CONCEPTO DE DILIGENCIA PROFESIONAL DEL 1104 CC

5.1. La decisión médica basada en una predicción errónea del sistema de IA como supuesto excluido de la aplicación de la propuesta de Directiva sobre responsabilidad em materia de IA.

En el caso de que se pruebe que el facultativo ha utilizado el sistema de IA conforme a las instrucciones y ha expuesto el sistema de IA a los datos de entrada pertinentes, la demanda por la actuación del facultativo que utiliza un sistema de IA como soporte de una decisión médica de la que resultan daños no podría formularse conforme a la Propuesta de Directiva sobre responsabilidad en materia de IA.

Según establece el Considerando 15 de la propuesta de Directiva, ésta solo abarca las demandas por daños y perjuicios que hayan sido causados por una información de salida —o por la no producción de una información de salida— imputable a un sistema de IA cuando medie culpa de una persona, por ejemplo, el proveedor o el usuario con arreglo a la Directiva. La Directiva no abarca la demanda de responsabilidad extracontractual cuando los daños hayan sido causados por una decisión humana, aunque esta decisión se fundamente en una predicción emitida por el sistema de IA de alto riesgo. Por lo tanto, queda excluida del ámbito de la Directiva, la responsabilidad civil derivada de los daños causados por la evaluación humana seguida de una acción u omisión humana, en la que el sistema de IA haya proporcionado información o asesoramiento que el agente humano haya tenido en cuenta.

En suma, en el caso de que se hayan seguido las instrucciones del sistema de IA y se haya expuesto el sistema a datos de entrada pertinentes, los daños causados por la decisión médica basada en la predicción de un sistema de IA quedan excluidos de la aplicación de la propuesta de Directiva. Como consecuencia no podrán ser aplicadas las medidas previstas por la propuesta de Directiva: a) las medidas relativas a la exhibición de pruebas consistentes en facilitar el requerimiento por parte del órgano jurisdiccional al proveedor (o personas sujetas a sus obligaciones[30]) o el requerimiento al usuario para la exhibición de pruebas pertinentes relativas al sistema de IA de alto riesgo (art. 3 de la Propuesta de Directiva sobre responsabilidad civil en materia de IA), y b)

---

sumo, nº 44/2022.

30. Conforme las obligaciones de los fabricantes de proveedores, obligaciones de los distribuidores e importadores y los responsables del despliegue previstas en la sección 3 del Capítulo III del Reglamento de IA.

la presunción refutable de la relación de causalidad en el caso de culpa (art. 4 Propuesta de Directiva sobre responsabilidad civil en materia de IA).

Conforme manifiesta el texto de la Directiva, la decisión clínica basada en los sistemas predictivos de IA es una decisión humana. El sistema de IA funciona como mero apoyo en la decisión médica, pero no reemplaza la función del médico que es quien decide y, por lo tanto, puede desviarse de la recomendación del sistema de IA[31]. En este sentido, también se expresa el nuevo Código español de deontología médica (2022), al regular la utilización de la IA en la práctica médica y reconocer que la IA puede ser utilizada como base de la decisión médica pero no sustituye al facultativo: "*Los datos de salud extraídos de grandes bases de datos sanitarias o los sistemas robóticos pueden servir de ayuda en la toma de decisiones clínicas y sanitarias, pero no sustituyen a la obligación que el médico tiene de utilizar los métodos necesarios para la buena práctica profesional*."(art.86.1)

La cuestión que se plantea y analizaremos a continuación es si, conforme a nuestro sistema de responsabilidad civil, el médico que toma la decisión final con apoyo del sistema de IA es responsable de los daños causados en el paciente por el error en la predicción del sistema.

5.2. La explicabilidad del sistema de IA como condición del alcance de la negligencia profesional médica de conformidad con el 1104 CC

Como se ha explicado *ut supra*, la decisión médica, diagnostica o terapéutica basada en los sistemas predictivos de IA es una decisión humana sólo imputable al médico. En el caso de que, como consecuencia de dicha decisión, se causen daños al paciente, concurre una responsabilidad civil por hecho propio, por un acto médico, que deberá ser resuelta conforme a las normas vigentes en materia de responsabilidad civil de los Estados miembros. En suma, tanto si la responsabilidad médica se resuelve con arreglo a la responsabilidad contractual o a la responsabilidad extracontractual, cada Estado miembro deberá identificar el estándar de diligencia exigible al médico en este caso.

En el ordenamiento jurídico español, la doctrina ha admitido como concepto de culpa, la noción de culpa o negligencia del artículo 1.104 CC que dice: "*La culpa o negligencia del deudor consiste en la omisión de aquella diligencia que exija la naturaleza de la obligación y corresponda a las circunstancias de las personas, del tiempo y del lugar. Cuando la obligación no exprese la diligencia*

31. Heinrichs,B/Heinrichs, J-H/Rüther, M; *Künstliche Intelligenz,* (2022) De Gruyter, Berlin-Boston, pp.114-115, Staudenmayer, D, (2023) "Haftung für Künstliche Intelligenz.Die deliktsrechtliche Anpassung des europäischen Privatrechts an die Digitalisierung", NJW, , 894, Navas Navarro, S; "Derecho e Inteligencia artificial desde el diseño. Aproximaciones" en Navas Navarro, S (Coord), (2017) *Inteligencia artificial Tecnología Derecho*, Tirant lo Blanch, Valencia, pp.23-72.

que ha de prestarse en su cumplimiento, se exigirá la que correspondería a un buen padre de familia." Aunque esta previsión del CC está circunscrita al cumplimiento de obligaciones contractuales, el criterio que establece, así como el concepto de culpa o negligencia es extensible a todos los ámbitos incluidos los supuestos de responsabilidad extracontractual[32].

La culpa en la responsabilidad médica es la falta de diligencia o previsión, es decir la infracción por parte del médico del deber de actuar con la diligencia objetivamente exigida por la naturaleza del acto médico que se ejecuta según las circunstancias de las personas, del tiempo y lugar. La observancia de las reglas que rigen la actuación médica y que conforman su *lex artis ad hoc,* integrada en esencia por los protocolos médicos de actuación, permite en línea de principio valorar la corrección del concreto acto médico[33]. Se toma en consideración las especiales características del facultativo, de su posible especialización, de la complejidad y trascendencia vital para el paciente y todas las demás circunstancias objetivas y subjetivas concurrentes.

¿El cumplimiento de la *lex artis ad hoc* requiere de una supervisión clínica de la decisión del sistema de IA para garantizar que las recomendaciones son seguras y pertinentes para el paciente?

Entendemos que exigir un deber de cuidado tan elevado sería un obstáculo para la implementación de los sistemas de IA como apoyo en la toma de decisiones clínicas. Ahora bien, el médico debe formarse en el manejo de los dispositivos médicos que utiliza y observar todas las instrucciones que sean necesarias para el buen funcionamiento del sistema[34]. En Alemania, por ejemplo, conforme a la interpretación jurisprudencial se considera que el médico que utiliza un dispositivo tecnológico en la prestación del acto médico deberá observar y atender los fallos obvios reconocibles y también deberá familiarizarse con el funcionamiento en la medida que se pueda esperar razonablemente de una persona científica[35].

> Conforme la sentencia del BGH alemán de 11 de octubre de 1977: "*Como regla general, el médico solo puede prometer esfuerzos ingeniosos, pero no el éxito*

---

32. En este sentido ver Rodríguez López, P; *Responsabilidad médica…,* ob.cit.p. 42, Plaza Penadés; J ; *El Nuevo Marco de…,* ob.cit. p. 36, Bustos Lago, J.M; "La responsabilidad civil médica y hospitalaria" en Bustos Lago, J.M/Reglero Campos, L (2013) , *Lecciones de Responsabilidad civil* , Aranzadi, Navarra, pp. 297-328.

33. Ver Ataz López, J (2002), *Los médicos y la responsabilidad civil,* Montecorvo, Madrid, p. 290,

34. Ver Katzenmeier, «§ 630h Beweislast bei Haftung für Behandlungs- und Aufklärungsfehler», en Hau/Poseck, (2023) Beck's on line BGB, 65. Edition, CH Beck, Rn.21, sin embargo, en Austria algún autor considera que la obligación de formación continua del médico no debe exagerarse y bastará con obtener una información general en este sentido Wilrbel-Rusch, A; *Telemedizin-Haftungsfragen,* Juristische Schriftenreihe ; 178, Wien , Verlag Österreich, p.67-69.

35. En este sentido ver Röhle, M; " Berufs und zivilrechtliche Fragestellungen im Zusammenhang mit dem Einsatz moderner Kommunikationsmittel in der ärztlichen Kooperation in Rahmen der Behandlung" en Krückl, K; (2011) *Vielschichtiges Medizinrecht*, Trauner, Linz, pp.399-457.

Berufs-und zivilrechtliche….", ob.cit. p. 440.

> *de la curación (...) Sin embargo, este principio no puede aplicarse al cumplimiento de obligaciones accesorias plenamente controlables, en particular la garantía de requisitos técnicos para una manipulación adecuada y segura (...) Es cierto que la creciente mecanización de la medicina moderna significa que el médico ya no puede captar todos los detalles técnicos de los dispositivos disponibles para él y tenerlos en la actualidad. Sin embargo, esto no lo exime de la obligación de familiarizarse con el funcionamiento de los dispositivos en particular, cuyo uso es de gran importancia para el paciente, al menos en la medida en que sea posible y razonable para una persona científica y técnicamente de mente abierta*"[36].

En suma y siguiendo este razonamiento, siempre que el sistema de IA se haya mantenido correctamente y haya sido utilizado de forma adecuada por el médico, el error del sistema de IA es un riesgo que está fuera del control del médico, salvo el caso de un error de predicción evidente y por lo tanto apreciable[37]. La apreciabilidad del error por parte del médico vendrá determinada por el grado de transparencia del funcionamiento del sistema de IA. Y en este caso, el hecho de que el sistema explique al médico o no, los presupuestos en los que fundamenta la predicción realizada, será determinante para valorar si el facultativo puede apreciar el error.

En relación con la capacidad de explicabilidad de los sistemas de IA hay que tener presente que la naturaleza de tipo "*caja negra*" hace difícilmente interpretable muchas de las técnicas más modernas de la IA. Se habla de *interpretabilidad* del modelo de IA para referirse al grado en que un ser humano puede entender la causa de una decisión tomada por un determinado modelo de IA. Por otra parte, nos referimos a la *explicabilidad* del modelo de IA para hacer referencia a la capacidad del modelo de ofrecer una explicación de una decisión tomada por un algoritmo que sea comprensible para el ser humano. Mientras la interpretabilidad se centra en la comprensión del proceso de toma de decisiones de un modelo de IA, la *explicabilidad* lo hace en comunicar claramente esa comprensión a los demás. Ambos conceptos están muy interrelacionados[38].

Un modelo con baja interpretabilidad puede ser más difícil de entender para un humano y, en consecuencia, el usuario del sistema puede verse expuesto a una mayor exigencia en su actuación, ya que la utilización del sistema de IA requerirá más experiencia o la realización de un análisis más detallado para interpretar la toma de decisiones del sistema. En este caso, la advertencia por el

---

36. Ver BGH Urt von 11. 10. 1977 — VI ZR 110/75 (Hamm) NJW 1978,584, también sobre la obligación del médico de verificar por si mismo el dispositivo médico ver, BGH, Urteil von 24. 6. 1975 — VI ZR 72/74 (Hamm), NJW 1975, 2245 sobre los daños causados en un menor de edad por la no comprobación de los defectos en un tubo anestésico.

37. En este sentido, para Alemania y la aplicación del 630 h BGB ver Schmidt, J.R. (2023) "Die Auswirkungen der Nutzung von KI-Software auf die ärztliche Haftung", *GesundheitsRecht* (GesR), núm. 6, p. 341 y ss.

38. Ver Cobo Cano, M/Lloret Iglesias, L (2023), *Inteligencia artificial y medicina;* CSIC, Madrid, p.59 y ss.

humano del error de la predicción será más compleja. Mientras que la utilización un modelo de IA de alta interpretabilidad permitirá la advertencia de predicciones erróneas del sistema y su utilización será más adecuada cuando del uso de la IA resulten consecuencias importantes para la persona, como puede ocurrir en el caso de un diagnóstico médico o de una predicción sobre el pronóstico de un paciente.

Sin embargo, el problema actual es que la exigencia de la interpretabilidad en el sistema de IA implica que el rendimiento predictivo del sistema sea inferior. Ya que, en la actualidad, una de las formas de llegar a la interpretabilidad del sistema es la interpretabilidad intrínseca y ésta implica utilizar algoritmos que sean interpretables por sí mismos, a costa de reducir su complejidad. Si bien, la ventaja es que las explicaciones vienen dadas por el modelo de forma automática, el modelo de IA al utilizar técnicas más sencillas manifiesta un menor rendimiento. En la actualidad no existe un consenso en cómo evaluar la interpretabilidad de un método, pero se está trabajando para conseguir mejores métodos de interpretabilidad que hagan los sistemas de IA suficientemente interpretables para los humanos. Sin duda, la mejora en la interpretabilidad de los sistemas de IA generará una mayor confianza en su utilización médica pues permitirá conocer por el facultativo la causa de la decisión predictiva tomada por la máquina y hará más reconocibles sus fallos.

6. A MODO DE CONCLUSIÓN

La implementación de los sistemas de IA transformará el sistema sanitario por las mejoras aportadas en los procesos clínicos y por el ahorro de costes que supondrá el cambio a un modelo asistencial proactivo centrado en la gestión de la salud más que en el tratamiento de la enfermedad. El Reglamento IA con el objeto de ordenar la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA formula un concepto de IA más restrictivo que hace posible una identificación de aquellas características especiales del sistema de IA que lo diferencian del simple software o de la programación más sencilla.

De conformidad con su doble calificación jurídica como producto sanitario y como sistema de IA de alto riesgo, el sistema de IA con finalidad médica queda sometido a una aplicación simultánea y complementaria de distintos procedimientos de evaluación para su comercialización, salvo que conforme con el Reglamento de IA el proveedor decida una integración de ambos procesos. En todo caso, una vez realizados todos los procesos de evaluación y cumplidos todos los requisitos, la robustez técnica y consistencia del funcionamiento de los sistemas de IA de alto riesgo reduce considerablemente el riesgo de errores del sistema.

La implementación de los sistemas de IA en la prestación sanitaria se encuentra en un estadio inicial en el que la IA es utilizada como herramienta de apoyo en las decisiones médicas. En esta fase inicial, las principales consecuencias jurídicas de su implementación se relacionan con la transformación de la

actividad humana y no con su sustitución. Una de las principales cuestiones relacionada con la responsabilidad civil, es la determinación del tipo de conducta exigible al profesional que utiliza la IA.

En el caso que resulten daños para el paciente por la errónea predicción emitida por un sistema de IA la responsabilidad civil médico-hospitalaria podría dirimirse en el marco de la propuesta de Directiva sobre responsabilidad en materia de IA, pero también en el marco del ordenamiento jurídico español.

En el marco de la Propuesta de Directiva sobre responsabilidad en materia de IA, el Hospital o empresa sanitaria es el responsable del despliegue del servicio sanitario que utiliza el sistema de IA y se presume la relación de causalidad entre su culpa y el resultado producido por el sistema siempre que se pruebe: a) que no utilizó o supervisó el sistema de IA de conformidad con las instrucciones de uso adjuntas o en su caso no suspendió o no interrumpió su uso y; b) que expuso el sistema de IA a datos de entrada bajo su control que no eran pertinentes habida cuenta de la finalidad prevista.

La Propuesta de Directiva sobre responsabilidad en materia de IA sólo se aplica a las demandas de responsabilidad extracontractual por daños causados por la IA, y por tanto en el ámbito de la sanidad privada comprendería las demandas interpuestas por el paciente contra el Hospital o empresa sanitaria por los daños causados por el servicio sanitario realizado en el marco de un seguro médico.

La sustitución en el Reglamento de IA del término "usuario" por el término más restrictivo de "responsable del despliegue" conlleva, dejar fuera de la Propuesta de Directiva sobre responsabilidad en materia de IA, dada su remisión, la responsabilidad del facultativo al no ser considerado "responsable del despliegue". En nuestra opinión, si atendemos a que el usuario es un agente material necesario en el despliegue de la IA, sería adecuada una interpretación amplia del concepto de "responsable del despliegue" para que la presunción de la relación de causalidad sea también extensible a la culpa *"in operando*" del facultativo. Siempre que se pruebe, conforme a la Propuesta de Directiva, que éste actuó sin seguir las instrucciones del sistema o que expuso el sistema a datos no adecuados.

Finalmente, con relación a nuestro sistema de responsabilidad civil, tanto si la responsabilidad médica se resuelve con arreglo a la responsabilidad contractual o a la responsabilidad extracontractual, deberá identificarse conforme el art. 1104 CC el estándar de diligencia exigible al médico que utiliza la IA. En este caso entendemos que, siempre que el sistema de IA se haya mantenido correctamente y haya sido utilizado de forma adecuada por el médico, el error del sistema de IA es un riesgo que está fuera del control del médico, salvo el caso de un error de predicción evidente y por lo tanto apreciable. En este supuesto, el grado de transparencia o explicabilidad del funcionamiento del sistema de IA, es decir, si el sistema comunica al médico o no los datos que han motivado su predicción, será determinante para valorar si éste debió apreciar el error.

BIBLIOGRAFÍA

ATAZ LÓPEZ, J. (2002), *Los médicos y la responsabilidad civil,* Montecorvo, Madrid.

BEUNZA, J.J. /CONDÉS, E. "Conceptos" en Beunza, JJ et Al. (2023), *Manual práctico de Inteligencia Artificial en entornos sanitarios,* Elsevier, Barcelona, pp. 7-17.

BEUNZA, J.J. "Algoritmos disponibles en la práctica sanitaria", Beunza, JJ et Al. (2023), *Manual práctico de Inteligencia Artificial en entornos sanitarios,* Elsevier, Barcelona, pp. 19-39.

BOHR, A/MEMARZADEH, K. "La asistencia sanitaria actual, los datos masivos y el aprendizaje automático"; Dir. Bohr, A/Memarzadeh,K (2021), *Inteligencia artificial en el ámbito de la salud,* pp. 1-24, Elsevier. Academic Press.

BOHR, A/MEMARZADEH, K. "El auge de la inteligencia artificial en las aplicaciones sanitarias"; Dir. Bohr, A/Memarzadeh,K (2021), *Inteligencia artificial en el ámbito de la salud,* , Elsevier. Academic Press. pp. 1-24.

BUSTOS LAGO, J.M. "La responsabilidad civil médica y hospitalaria" en Bustos Lago, J.M/Reglero Campos, L (2013), *Lecciones de Responsabilidad civil*, Aranzadi, Navarra, pp. 297-328.

CAMACHO CLAVIJO, S. "AI assessment tools for decision-making on telemedicine: liability in case of mistakes". *Discov Artif Intell* 4, 24 (2024). https://doi.org/10.1007/s44163-024-00117-4

COBO CANO, M. / LLORET IGLESIAS, L. (2023), *Inteligencia artificial y medicina;* CSIC, Madrid,

DETTLING, H.U. (2019) „Künstliche Intelligenz und digitale Unterstützung ärztlicher Entscheidungen in Diagnostik und Therapie", *PharmaRecht*, 633.

DÍAZ HERNÁNDEZ, M. (2023), "El Reglamento de Inteligencia Artificial: Un análisis desde el punto de vista sanitario" en *Derecho y Salud,* vol 33 , pp.25-44.

FREEMAN et al., (2020) "Algorithm based smartphone apps to assess risk of skin cancer in adults: systematic review of diagnostic accuracy studies", *BMJ,* Feb, doi: 10.1136/bmj.m127.

HEINRICHS,B./ HEINRICHS, J-H./ RÜTHER, M. *Künstliche Intelligenz,* (2022) De Gruyter, Berlin-Boston, pp.114-115.

KATZENMEIER, «§ 630h Beweislast bei Haftung für Behandlungs- und Aufklärungsfehler», en Hau/Poseck, (2023) Beck's on line BGB, 65. Edition, CH Beck, Rn.21.

LAZCOZ MORATINOS, G. (2022) "*Sistemas de Inteligencia Artificial en la Asistencia Sanitaria: Cómo Garantizar la supervisión humana desde la normativa de protección de datos" Premio* de Investigación en Protección de Datos. Personales *Emilio Aced* correspondiente al año *2022*.

MINERZAMI, R. "Decisiones de diagnóstico y tratamiento del cáncer mediante Inteligencia Artificial", en Dir. Bohr, A/Memarzadeh,K (2021), *Inteligencia artificial en el ámbito de la salud,* Elsevier. Academic Press, pp. 1-24.

NAVAS NAVARRO, S. (2022); "Régimen Europeo en ciernes en materia de responsabilidad derivada de los sistemas de Inteligencia Artificial"*, Revista CESCO de Derecho de Consumo, nº 44/2022.*

NAVAS NAVARRO, S. "Derecho e Inteligencia artificial desde el diseño. Aproximaciones" en Navas Navarro, S (Coord), (2017) *Inteligencia artificial Tecnología Derecho*, Tirant lo Blanch, Valencia, pp.23-72.

PISANI, C/STIEF, M. (2022), „Regulatorische und haftungsrechtliche Herausforderungen für KI-Medizinprodukte" en *Medizinprodukterecht im Wandel. Festschrift für Ulrich M. Gassner zum 65. Geburtstag*, Nomos, Baden-Baden, p. 472, IQBAL.

PLAZA PENADÉS; J. (2002); *El Nuevo Marco de la Responsabilidad Médica y Hospitalaria,* Aranzadi, Navarra.

REITER, B./TURECK, J./ WEINDENFELD, W. (2011) Telemedizin-ZUkunftsgut im Gesundheitswesen*, C.A.P. Analyse*, 1/2011, pp 1-25.

RODRÍGUEZ LÓPEZ, P. (2004); *Responsabilidad médica y hospitalaria,* Bosch, Barcelona.

RÖHLE, M. " Berufs und zivilrechtliche Fragestellungen im Zusammenhang mit dem Einsatz moderner Kommunikationsmittel in der ärztlichen Kooperation in Rahmen der Behandlung" en Krückl, K; (2011) *Vielschichtiges Medizinrecht*, Trauner, Linz, pp.399-457.

SÁNCHEZ-SALMERÓN, R. et al. (2022) "Machine learning methods applied to triage in emergency services: a systematic review", *International Emergency Nursing,* Vol. 60, Elsevier, article 101109.

SCHMIDT, J.R. (2023) "Die Auswirkungen der Nutzung von KI-Software auf die ärztliche Haftung", *GesundheitsRecht* (GesR), núm. 6, p. 341 y ss.

STAUDENMAYER, D. (2023) "Haftung für Künstliche Intelligenz.Die deliktsrechtliche Anpassung des europäischen Privatrechts an die Digitalisierung", NJW, 894.

THIERMANN, A/ BÖCK, R.N. (2022), "Künstliche Intelligenz in Medizinprodukten Regulatorisches Regelwerk und Haftungsvorgaben", *Recht digital* (Rdi), 333.

WILRBEL-RUSCH, A. *Telemedizin-Haftungsfragen,* Juristische Schriftenreihe; 178, Wien, Verlag Österreich.

I. Empresa y responsabilidad

Los modelos de inteligencia artificial de propósito general y responsabilidad civil. Aproximación crítica

Susana Navas Navarro
Catedrática de Derecho civil
Universidad Autónoma de Barcelona

ABSTRACT:
This contribution, first of all, addresses the distinction between artificial intelligence (AI) systems and general-purpose AI models, one example of which is generative AI. Besides, the regulation of these models according to whether they present a systemic risk is discussed. Finally, aspects relating to civil liability for damages that may be caused by these general-purpose AI models are presented in relation to the Proposals for Directives on the subject that were published on September 28, 2022. In this regard, doubts are expressed about the application of these Proposals to AI models.

Keywords: AI systems, AI models, general purpose, generative AI, civil liability.

Palabras claves: sistemas de IA, modelos de IA, propósito general, IA generativa, responsabilidad civil.

SUMARIO:

1. INTRODUCCIÓN

El Reglamento de inteligencia artificial (RIA) diferencia entre sistema de IA y modelo de IA de propósito general. En este último término se englobaría a la inteligencia artificial generativa (IAG). En la última versión del RIA que se conoce después de las negociaciones del "trilogue", es decir, una versión corregida, desaparece la referencia, que estaba presente en la versión del Parlamento europeo de 14 de junio de 2023[1], a los modelos fundacionales[2] y a la IAG (art. 28 ter apartado 4) como tipo de modelo fundacional. Sin entrar a discutir si, desde el punto de vista técnico, es más coherente un planteamiento u otro, o si los conceptos que maneja la última versión generan más confusión que claridad, paso a exponer qué entiende el RIA por un modelo de IA de propósito general, dentro del cual se encontraría los conocidos ChatGPT, Stable Diffusion, E-Dalle, Bard, Gemini, etc.. en comparación con el sistema de IA (2.) para después detenerme específicamente en los modelos de IA de propósito general (3.).

1. P9_TA(2023)0236. *Artificial Intelligence Act. Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). Versión corregida 2020/2024: 16.04.2024. Fecha de la consulta: mayo 2024.

2. Estos modelos aparecían definidos en el art. 3.1c de la última versión de la Propuesta de reglamento de IA de 14 de junio de 2023 hecha pública con las enmiendas del Parlamento europeo como "*modelos de IA que son entrenados con una amplia cantidad de datos a escala, designados para obtener una generalidad de resultados y que pueden adaptarse a un amplio abanico de tareas diversas"*. Estando en fase de edición esta obra apareció la publicación del Reglamento de inteligencia artificial (RIA) en el DOUE (12.07.2024) por lo que solo he podido tener en cuenta la última versión corregida hecha pública por el Parlamento europeo y solo a ella me refiero en mi contribución.

2. SISTEMAS DE INTELIGENCIA ARTIFICIAL Y MODELOS DE INTELIGENCIA ARTIFICIAL DE PROPÓSITO GENERAL

En primer lugar, abordaré las diferencias entre el sistema de IA y el modelo de IA de propósito general (2.1.) para, posteriormente centrarme en la excepción en caso de investigación en cuanto a la aplicación del RIA (2.2.).

2.1. Diferencias entre uno y otro

Según el art. 3 apartado 63 RIA un "modelo de IA de propósito general" consiste en un modelo de IA que se ha entrenado con una gran cantidad de datos, que emplea la autosupervisión a escala, que muestra una generalidad significativa y es capaz de realizar de forma competente, una amplia gama de tareas distintas, independientemente de la forma en que se comercialice el modelo, y que puede integrarse en una variedad de sistemas o aplicaciones posteriores (v. gr. los grandes generadores de contenido como los citados al inicio). Esto no incluye los modelos de IA que se utilizan antes de su comercialización para actividades de investigación, desarrollo y creación de productos o actividades como prototipos. A la excepción de investigación me refiero específicamente en el apartado siguiente.

El modelo de IA con propósito general puede ser un componente del sistema de IA cuando éste emplea aprendizaje automático y toma de decisiones. Por "sistema de IA" se entiende, en el art. 3.1 RIA, un sistema basado en máquinas diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada de inputs que recibe, genera salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. La definición de "sistema de IA" comprende un enfoque basado en aprendizaje automático, en lógica y el conocimiento que infieren a partir del conocimiento codificado y la representación simbólica de tareas a resolver. Se aleja del software tradicional, de enfoques de programación y sistemas que se basan en reglas predefinidas para ejecutar tareas de manera automática (considerando núm. 6 RIA). Se trata de un concepto que ha ido variando a lo largo de su andadura legislativa pero finalmente se ha acogido una definición próxima a la dada por organizaciones internacionales como la OCDE[3] que tiene en cuenta que funciona de forma independiente a la intervención humana (niveles de autonomía) y con autoaprendizaje (capacidad de adaptación). En definitiva, aprendizaje, razonamiento y modelado.

3. OECD (2019), "Scoping the OECD AI principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO)", *OECD Digital Economy Papers*, No. 291, OECD Publishing, Paris, https://doi.org/10.1787/d62f618a-en. Fecha de la consulta: mayo 2024.

Deben diferenciarse ambos. La definición de modelo de IA de propósito general se basa en las características funcionales claves, en concreto, la generalidad y la capacidad de realizar de forma competente una amplia gama de tareas diferentes (considerando núm. 85 RIA). Aunque los modelos suelen ser componentes esenciales de un sistema de IA, no constituyen por sí mismos sistemas de IA. Deberían añadirse otros componentes para convertirse en este último como, por ejemplo, una interfaz de usuario.

Cuando un modelo de IA de propósito general se integra en un sistema de IA[4] o forma parte de él, este sistema debe considerarse un sistema de IA de propósito general, y podría ser considerado de alto riesgo, en su caso. Cuando debido a esta integración, este sistema tenga la capacidad de servir a diversos fines. Un sistema de IA de propósito general puede emplearse directamente o para fines diversos (considerando núm. 85 RIA).

Los sistemas de IA de riesgo limitado (art. 50 RIA) y los modelos de IA de propósito general deben ser transparentes, en el sentido de que, los proveedores[5] y desarrolladores[6] deben de informar a las personas que interactúan con ellos que están tratando con un sistema y no con una persona humana (art. 50.1 RIA), salvo que sea obvio por las circunstancias y el contexto del uso que no es necesaria esa información. En el caso de que manipulen contenido deben indicar si este contenido se ha generado artificialmente o no, es decir, si se trata de una *deep fake* o no (art. 50.4 RIA). El propio RIA define lo que debe de entenderse por "deep fake" (art. 3 apartado 60). Se trata de "*contenidos de imagen, audio o vídeo generados o manipulados por IA que se asemejan a personas, objetos, lugares u otras entidades o acontecimientos existentes y que a una persona le parecerían falsamente auténticos o veraces*".

Cuando este contenido se combina con trabajos artísticos, la información no debe menoscabar ni afectar a la parte de contenido sobre el que existen derechos de autor ni conducir a error o confusión acerca de qué parte se ha generado artificialmente y qué parte la ha creado el humano, si bien se establece alguna que otra excepción cuando se trata de investigaciones criminales previa orden judicial. Por ello se establece la obligación a los proveedores de que apliquen tecnologías que permitan detectar la parte del contenido que ha sido ge-

4. Esta tarea la lleva a cabo el *'downstream provider' means a provider of an AI system, including a general-purpose AI system, which integrates an AI model, regardless of whether the AI model is provided by themselves and vertically integrated or provided by another entity based on contractual relations* (art. 3.68 RIA).

5. Art. 3.2 define a quién se considera proveedor: *"una persona física o jurídica, autoridad pública, agencia u otro organismo que desarrolle un sistema de IA o un modelo de IA de propósito general o que haga desarrollar un sistema de IA o un modelo de IA de propósito general y los comercialice o ponga en servicio bajo su propio nombre o marca comercial, ya sea a título oneroso o gratuito*".

6. Es el conocido en la versión inglesa como "deployer", aunque también se le puede denominar "desplegador": "*cualquier persona física o jurídica, autoridad pública, agencia u otro organismo que utilice un sistema de IA bajo su autoridad, excepto cuando el sistema de IA se utilice en el curso de una actividad personal no profesional*".

nerado artificialmente teniendo en cuenta el estado del arte, el coste económico de la innovación tecnológica y de los beneficios que se puedan obtener.

2.2. La inaplicación del Reglamento en caso de investigación

Hay varias excepciones a la aplicación del Reglamento: cuando el sistema de IA se produce y se emplea para fines militares, cuando se produce con fines científicos y de investigación (art. 2.6) y cuando quien emplea el sistema de IA es una persona física en el curso de una actividad no profesional. En el caso de los fines científicos o de investigación, la excepción trata de potenciar la innovación en IA y no ponerle trabas. Esto quiere decir que este sistema de IA no se ha introducido en el mercado ni puesto en servicio en él. Ahora bien, si para producir este sistema se emplean otros sistemas de IA, éstos sí deberán cumplir con los requisitos del Reglamento pues se parte de la base de que éstos que se emplean ya han sido introducidos en el mercado o puestos en servicio.

En este punto puede surgir una pregunta si el modelo de IA y el sistema de IA se entrenan muy probablemente con grandes cantidades de datos, si estos datos están protegidos y, en su caso, qué tipo de protección tienen. Algunos estarán en el dominio público, otros serán de acceso abierto, otros protegidos por derechos de exclusiva (propiedad intelectual, secreto comercial, principalmente), por cláusulas contractuales (*private ordering*) y otros por la propia legislación como es el caso de los datos personales.

Por otro lado, el Reglamento prevé la creación de "sandboxes" o "espacios controlados de pruebas" para probar estos sistemas y modelos de IA. Los espacios controlados de pruebas para la IA generan un entorno controlado para probar, durante un tiempo limitado, tecnologías innovadoras sobre la base de un plan de pruebas acordado con las autoridades competentes, tanto en espacios reales, simulados, virtuales o híbridos (art. 3 apartado 55 y considerando núm. 138 RIA). Cuando se testan en el mundo real, deben establecerse toda una serie de salvaguardas (art. 57 RIA). En España disponemos de la primera regulación europea al respecto*: Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial*[7].

La fase de investigación se rige por criterios éticos y estándares profesionales, así como toda la normativa, como decía, referida a los datos que se empleen, máxime si están protegidos con derechos de exclusiva, como lo están la mayoría de ellos.

En materia de investigación es importante tener en cuenta que los datos pueden emplearse para usos primarios y para usos secundarios. Esto es particularmente relevante en el ámbito de la salud y de ello se ocupa específicamente

7. BOE núm. 268, de 9 de noviembre de 2023.

la Propuesta de reglamento del EEDS en la que me he entretenido en otro lugar[8].

3. MODELOS DE INTELIGENCIA ARTIFICIAL DE PROPÓSITO GENERAL

El RIA somete a los modelos de IA de propósito general a requerimientos y obligaciones específicas, a las que me referiré posteriormente, para mitigar en la medida de lo posible los riesgos y daños que se pudieran ocasionar debido precisamente a que, al tratarse de modelos que pueden implementarse en sistemas de IA con una finalidad general, se aplican a gran cantidad de contextos y pueden tener una gran cantidad de usos y aplicaciones, asegurando robustez, interoperabilidad, especificidades técnicas, costes, etc ... En concreto, estas obligaciones son las especificadas en el Capítulo V del RIA siendo el responsable principal de su cumplimiento el proveedor del modelo de IA.

Distinguiré, en primer término, los modelos de IA de propósito general con y sin riesgo sistémico (3.1.), y seguidamente me entretendré en los requerimientos y obligaciones de los mismos para poder ser comercializados (3.2.).

3.1. Modelos de inteligencia artificial de propósito general con y sin riesgo sistémico

El RIA diferencia entre modelos de IA de propósito general que representan un riesgo sistémico de aquellos que no lo representan para perfilar el conjunto de obligaciones que deben cumplir los proveedores de los mismos (art. 51 RIA). Precisamente los proveedores antes de introducir un modelo de IA de propósito general en el mercado de la UE, si están establecidos fuera de la UE deben designar mediante un mandato escrito a un representante autorizado (art. 54 RIA) que esté establecido en territorio de la Unión y que le permita desempeñar las funciones que el propio RIA le atribuye en el art. 52. Deberá depositarse una copia de este mandato por escrito en la oficina de IA, que depende de la Comisión, y se facultará con el mismo para comprobar que se ha elaborado la documentación técnica especificada en el anexo correspondiente al RIA y que se han cumplido las obligaciones referidas en los arts. 52 y 53, conservar una copia de la documentación técnica a disposición siempre de la Oficina de IA. A ésta también se le debe facilitar toda la información necesaria para demostrar el cumplimiento de las obligaciones que establece el RIA. Si el proveedor de un modelo lo integra en su propio sistema de IA para procesos internos que no afecten a personas físicas, estos requerimientos no deben aplicarse.

8. Navas Navarro (2023: 47).

Antes de nada, debe explicitarse qué entiende el legislador europeo por "riesgo sistémico". El art. 3 apartado 65 RIA indica que se entiende por riesgo sistémico a nivel de la UE. Se trata de "*un riesgo específico de las capacidades de alto impacto de los modelos de IA de propósito general, que tiene un impacto significativo en el mercado interior debido a su alcance, y con efectos negativos reales o razonablemente previsibles en la salud pública, la seguridad pública, los derechos fundamentales o la sociedad en su conjunto, que puede propagarse a escala a través de la cadena de valor*". Y por "capacidades de alto impacto" se consideran "*capacidades que igualan o superan las capacidades registradas en los modelos de IA de propósito general más avanzados*" (art. 3 apartado 64 RIA).

Según el art. 51.2 RIA se presumirá que un modelo de IA de propósito general tiene capacidades de alto impacto cuando la cantidad acumulada de cálculo utilizada para su entrenamiento medida en operaciones en coma flotante (FLOPs)[9] sea superior a 10^25", es decir, se trata del poder computacional usado para entrenar al modelo que, si lo alcanza, de acuerdo con ese umbral, puede conducir a presumir que es un modelo que presenta riesgos sistémicos. Este umbral debe poder ajustarse para reflejar los cambios tecnológicos e industriales, como mejoras algorítmicas o el aumento de la eficiencia del hardware (considerando núm. 111).

Para ello, la oficina de IA debería colaborar con la comunidad científica, la industria, la sociedad civil y otros expertos. Los umbrales, las herramientas y los puntos de referencia para la evaluación de las capacidades de alto impacto deberían ser sólidos predictores de la generalidad, sus capacidades y el riesgo sistémico asociado a estos modelos teniendo en cuenta la forma en que el modelo se comercializa y el número de usuarios a los que puede afectar[10]

Todas estas definiciones tienen como base el tratar de ser lo más *tecnológicamente neutras* posibles para que puedan seguir siendo válidas en el futuro en la medida en que se invente nueva tecnología que, ahora mismo, se desconoce. El considerando núm. 14 de la Decisión (UE) 2022/2481, del Parlamento europeo y del Consejo de 14 de diciembre de 2022 por la que se establece el programa estratégico de la Década Digital para 2030[11] advierte que: "La neutralidad tecnológica prevista en la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo (Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas, (DOUE L 321 de 17.12.2018, p. 36) es un principio que debe guiar las políticas nacionales y de la Unión respecto a las infraestructuras de conectividad digital del más alto rendimiento, resiliencia, seguridad y sostenibilidad, para beneficiarse de la prosperidad. Todas las tecnologías y sis-

9. El art. 3 apartado 67 RIA define la "operación de coma flotante" como "*cualquier operación matemática o asignación que implique números en coma flotante, que son un subconjunto de los números reales típicamente representado en los ordenadores por un número entero de precisión fija escalado por un exponente entero de base fija*".

10. Hacker (2023: 5).

11. DOUE L 323/4, 19.12.2022.

temas de transmisión capaces de contribuir a la consecución de la conectividad de gigabit, incluidos los avances actuales y futuros de la fibra, el satélite, la 5G o cualquier otro ecosistema futuro y el wifi de próxima generación, deben, por lo tanto, recibir el mismo trato cuando tengan un rendimiento de la red equivalente".

El art. 51.1 RIA establece cuándo se considera que un modelo de IA de propósito general presenta un riesgo sistémico, siempre y cuando cumpla uno de los siguientes criterios:

a) Tiene capacidades de alto impacto evaluadas sobre la base de herramientas técnicas y metodologías apropiadas, incluidos indicadores y puntos de referencia;
b) Se ha calificado así por la comisión europea o por un panel de expertos de oficio, o tras una alerta cualificada de la comisión técnica científica, de que un modelo de IA de propósito general tiene capacidades o repercusiones equivalentes a las de la letra a).

Debe publicarse una lista actualizada por la Comisión de los modelos de IA de propósito general que presenten un riesgo sistémico (art. 52.6 RIA).

Esta diferencia dentro de los modelos de IA de propósito general responde al revuelo que generó el ChatGPT que llevó a que, en la versión del RIA nacida del Parlamento europeo, se introdujeran obligaciones similares —casi idénticas— a las de los proveedores de sistemas de IA de alto riesgo, lo que no tenía demasiado sentido puesto que lo mismo se puede emplear para componer una invitación a una fiesta que para elaborar un medicamento o un tipo de droga. Es decir, lo importante es el uso que se hace de ese modelo[12]. En la última versión del RIA conocida, se ha optado por clasificar los modelos de IA según exista o no riesgo sistémico, lo que no siempre tendrá que ver con el uso que se haga de éste, sino en las "capacidades de alto impacto".

De todos modos, no deja de sorprender que los modelos que presentan un riesgo sistémico que puede afectar, por ejemplo, a derechos fundamentales de los individuos no sean considerado de alto riesgo o no se sometan a los requerimientos de éstos. De hecho, interpretado el art. 6.2 RIA *a contrario*, resulta que los sistemas de IA a los que se refiere el Anexo III son sistemas que suponen un riesgo significativo de daños para la salud, la seguridad o los derechos fundamentales de las personas físicas o pueden influir en la toma de decisiones y, de ahí que se les someta a requerimientos específicos y el elenco de obligaciones para los operadores económicos involucrados sea ciertamente importante (capítulo II del título I RIA). En cambio, en el caso de modelos de IA de propósito general con riesgo sistémico, que suele ser un componente del sistema de IA, no serían considerados de alto riesgo cuando se afectan bienes fundamentales idénticos. Tampoco existe una declaración específica en el RIA de que no son

12. Hacker, Engel, Mauer (2023: 27).

considerados de alto riesgo como, en cambio, sí que existía en la Propuesta que surgió del Parlamento europeo (considerando núm. 60 octies de la versión Parlamento europeo de 14 de junio de 2023).

El art. 52 RIA hace referencia al modelo de IA de propósito general cuando el riesgo sistémico tiene que ver con las capacidades de alto impacto en particular. En este caso el proveedor tiene que notificar este importante dato a la comisión, es decir, que el modelo puede presentar un riesgo sistémico y proporcionar argumentos sustanciales que permitan apreciar que, a pesar de presentar ese riesgo, no debe clasificarse como tal pues es altamente improbable que ese riesgo se llegue a producir. Si la Comisión considera que los argumentos ofrecidos no son sustanciales, lo clasificará de riesgo sistémico sin perjuicio de que se compruebe o se solicite por el proveedor que se compruebe si efectivamente sigue siendo de riesgo sistémico o no (art. 52 RIA).

3.2. Requerimientos y obligaciones en caso de comercialización de modelos de IA de propósito general

Las obligaciones generales de los proveedores en caso de modelos de IA de propósito general presenten o no un riesgo sistémico, son las que establece el art. 53 RIA. Por su parte, el art. 55 RIA se centra en las obligaciones de proveedores de modelos de IA de propósito general que presenten un riesgo sistémico, que advertía que los modelos fundacionales no podían considerarse sistemas de alto riesgo.

Asimismo, se elaborarán códigos de conducta y de buenas prácticas en las que participarán todos los actores interesados (art. 56 RIA). La autoridad de IA evaluará estos códigos y los aprobará formalmente y. en caso, de que se consideren inadecuados puede establecer reglas comunes para la implementación de las obligaciones requeridas en el RIA.

3.2.1. Para todo modelo de inteligencia artificial de propósito general

Con base en el art. 53 RIA, en general, los proveedores de modelos de IA de propósito general deben cumplir toda una serie de obligaciones que tienen carácter horizontal. Son las que se relatan a continuación:

a) deben redactar y guardar documentación técnica actualizada del modelo incluyendo del proceso de entrenamiento y testeo, así como de los resultados de su evaluación, la cual debe contener unos datos mínimos que se determinan en un anexo al reglamento;
b) deben redactar y guardar información actualizada para hacerla accesible a los proveedores de sistemas de IA que pretendan integrar el modelo de IA de propósito general en su sistema de IA. Sin perjuicio de preservar los derechos de exclusiva (propiedad intelectual, información empresarial confidencial y secretos comerciales), esta información debe permitir a los

proveedores de sistemas de IA un buen entendimiento de las capacidades y limitaciones de los modelos de IA de propósito general y cumplir con sus obligaciones de acuerdo con este reglamento. Asimismo, debe contener unos elementos mínimos establecidos en el anexo correspondiente del RIA.

c) deben aplicar mecanismos que respeten los derechos de autor en la UE incluyendo el estado del arte de las tecnologías, así como las reservas de derechos que se recogen en el art. 4.3 de la Directiva (UE) 2019/790, sobre derechos de autor.
d) redactar y hacer público un sumario lo suficientemente detallado sobre el contenido usado para entrenar al modelo de IA de acuerdo con un modelo de informe suministrado por la oficina de IA. Un sumario no técnicamente detallado, pero sí lo suficiente para hacerse una idea general debido a la protección del secreto comercial y el deber de confidencialidad.

De todos modos, estos deberes no se aplican, salvo lo que concierne a los derechos de autor y a elaborar y poner a disposición del público un resumen suficientemente detallado sobre el contenido utilizado para el entrenamiento del modelo, a aquellos proveedores de modelos de IA que se han hecho públicos bajo una licencia abierta y gratuita que permite el uso, acceso, modificación y distribución del modelo y cuyos parámetros, incluyendo los pesos, la información del modelo y del uso se han hecho públicos, salvo que se trate de modelos de IA que presenten riesgos sistémicos (art. 53 RIA).

3.2.2. Para el modelo de inteligencia artificial de propósito general que presente riesgos sistémicos

Cuando suponen un riesgo sistémico, los proveedores deben adicionalmente cumplir con una serie de obligaciones que se encuentran establecidas en el art. 55 RIA. Éstas son:

a) ejecutar la evaluación del modelo de acuerdo con protocolos estandarizados y herramientas que reflejen el estado del arte incluyendo documentación de que se han conducido un testeo del modelo para identificar y mitigar riesgos sistémicos,
b) evaluar y mitigar posibles riesgos sistémicos que pueden derivarse del desarrollo, puesta en el mercado o uso de estos modelos,
c) hacer el seguimiento y documentar e informar acerca de incidentes graves y posibles medidas correctivas a las autoridades competentes y a la autoridad de IA y
d) asegurar un nivel adecuado de ciberseguridad frente a estos posibles riesgos sistémicos y frente a las infraestructuras físicas.

Un "incidente grave" supone cualquier incidente o malfuncionamiento del sistema de IA que directa o indirectamente conduce a la muerte de una persona o daño a su salud, un daño irreversible del funcionamiento y operación de una infraestructura crítica y el incumplimiento de las obligaciones establecidas en el derecho de la UE que protegen los derechos fundamentales (art. 3 apartado 39 RIA). Esta parte de la regulación debe de cohonestarse, a mi juicio, con la Directiva (UE) 2022/2557 del Parlamento europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo[13]. Estas entidades críticas se relacionan en el anexo de la propia Directiva como, por ejemplo, la infraestructura sanitaria, financiera, aeroportuaria o el transporte público, etc…

4. MODELOS DE INTELIGENCIA ARTIFICIAL DE PROPÓSITO GENERAL Y RESPONSABILIDAD CIVIL

Tras reflejar el marco de referencia (4.1.) procedo a revisar de forma crítica la relación existente entre las Propuestas de Directiva relacionadas con la responsabilidad civil y los defectos de los modelos de IA y, en concreto, de la IAG (4.2.).

4.1. Marco de referencia

Como es conocido la UE ya ha puesto el foco en la regulación de los daños ocasionados por los sistemas de IA mediante dos Propuestas de Directivas: una que regula la responsabilidad civil extracontractual por los daños que ocasione el sistema, basada en la culpa (en adelante, Propuesta RC)[14], y otra que implica la modificación de la Directiva por los daños ocasionados por productos defectuosos (en adelante, Propuesta PLD[15]), de 28 de septiembre de 2022[16].

La primera Propuesta de Directiva se centra en los sistemas de alto riesgo y en los que no son de alto riesgo. Se hizo pública antes de que saliera al mercado el ChatGPT o se dieran a conocer otros modelos fundacionales, que en, la última versión del RIA, se conocen como modelos de IA de propósito general[17]. Por lo tanto, ya de entrada debe afirmarse, que no aparecen contemplados en su ámbito de aplicación. En el caso de la Propuesta PLD, el hecho de que el art. 4.1, aluda simplemente a los "programas informáticos", en cuanto "producto", y que, como establece el considerando núm. 12, se pretenda incluir en el precep-

13. DOUE L 333/164, 27.12.2022.
14. COM(2022) 496 final.
15. COM(2022) 495 final. El acrónimo PLD es corresponde con "Products Liability Directive".
16. En relación con estas Propuestas tuve ocasión de ocuparme en mi trabajo, (2022: 27-51). Recientemente, vid. Álvarez (2024: 20), Jorqui Azofra (2023: 65).
17. Navas Navarro (2023: 35).

to a los sistemas de IA, permitiría entender que quedan comprendidos los modelos de IA de propósito general y, en concreto, la IAG en su ámbito de aplicación. Este considerando advierte que: "los productos en la era digital pueden ser tangibles o intangibles. Los programas informáticos, como los sistemas operativos, los microprogramas, los programas de ordenador, las aplicaciones o *los sistemas de IA*, son cada vez más comunes en el mercado y desempeñan un papel cada vez más importante para la seguridad de los productos. Los programas informáticos pueden introducirse en el mercado como productos autónomos y, posteriormente, pueden integrarse en otros productos como componentes, y pueden causar daños por su ejecución. Por consiguiente, en aras de la seguridad jurídica, debe aclararse que los programas informáticos son un producto a efectos de la aplicación de la responsabilidad objetiva, independientemente de su modo de suministro o uso, y, por tanto, con independencia de si el programa informático está almacenado en un dispositivo o se accede a él a través de tecnologías en la nube. Sin embargo, el código fuente de los programas informáticos no debe considerarse un producto a efectos de la presente Directiva, ya que se trata de pura información. El desarrollador o productor de programas informáticos, *incluidos los proveedores de sistemas de IA* en el sentido del [Reglamento (UE) .../... (Reglamento sobre inteligencia artificial)], debe ser tratado como un fabricante".

Además, esta Propuesta PLD tiene en cuenta, como una de las circunstancias que puede hacer que un "producto" presente un defecto de seguridad, el hecho de que éste tenga capacidad de aprendizaje y se vaya alimentando de nuevos datos (art. 6 letra c), es decir, que podría aplicarse la Propuesta PLD a un modelo que pudiera presentar un defecto en el sentido que establece la misma, esto es, "no ofrece la seguridad que el público en general tiene derecho a esperar" (art. 6.1)[18].

Asimismo, debe tenerse en cuenta que la Propuesta RC permite que el demandado sea un usuario no profesional. Aunque principalmente, el demandado sea el proveedor o el usuario profesional, no impide en absoluto que lo pudiera ser aquél (art. 2.8 y art. 4.6) y los daños, respecto de los cuales se solicita una indemnización, pueden ser tanto daños materiales como daños morales (art. 2.5). En la exposición de motivos de la Propuesta RC se advierte que: "Con esta propuesta, la Comisión pretende garantizar que las víctimas de daños causados por la IA gocen de un nivel de protección equivalente en virtud de las normas de responsabilidad civil al de las víctimas de daños causados sin que medie IA. La propuesta permitirá una aplicación privada efectiva de los derechos fundamentales y protegerá el derecho a la tutela judicial efectiva cuando se materialicen los riesgos específicos de la IA. En particular, la propuesta contribuirá a proteger los derechos fundamentales, como el derecho a la vida (artículo 2 de la Carta), el derecho a la integridad física y mental (artículo 3) y el derecho a la propiedad (artículo 17). Además, en función del sistema y las tradiciones de Derecho civil

18. De Bruyne et al. (2022:36).

de cada Estado miembro, las víctimas podrán reclamar una indemnización por los daños causados a otros intereses jurídicos, como las violaciones de la dignidad personal (artículos 1 y 4 de la Carta), el respeto de la vida privada y familiar (artículo 7), el derecho a la igualdad (artículo 20) y la no discriminación (artículo 21)".

Finalmente, debe ponerse de relieve que ambas Propuestas reconocen la asimetría existente entre la víctima y el proveedor o implementador del sistema de IA desde el momento en que establecen normas relativas a la carga de la prueba en forma de presunciones iuris tantum del nexo causal, así como el derecho de acceso a información relevante en posesión de aquéllos (arts. 3 y 4 Propuesta RC, arts. 8 y 9 Propuesta PLD)[19]. Así, por ejemplo, el art. 8.1 Propuesta PLD estatuye que: "*Los Estados miembros garantizarán que los órganos jurisdiccionales nacionales estén facultados, a petición de una persona perjudicada que reclame una indemnización por los daños causados por un producto defectuoso («el demandante»), que haya presentado hechos y pruebas suficientes para respaldar la verosimilitud de la reclamación de indemnización, para ordenar al demandado que revele las pruebas pertinentes de que disponga*" y, en sentido muy similar el art. 3.1 Propuesta RC considera que: "*Los Estados miembros velarán por que los órganos jurisdiccionales nacionales estén facultados, ya sea a petición de un demandante potencial que haya solicitado previamente a un proveedor, a una persona sujeta a las obligaciones de un proveedor con arreglo al [artículo 24 o al artículo 28, apartado 1, de la Ley de IA], o a un usuario, que exhiba las pruebas pertinentes que obran en su poder sobre un determinado sistema de IA de alto riesgo del que se sospeche que ha causado daños, pero cuya solicitud haya sido denegada, o a petición de un demandante, para ordenar la exhibición de dichas pruebas a estas personas*".

4.2. Las Propuestas de Directiva y la inteligencia artificial generativa

A pesar de todo ello, estas Propuestas de Directivas, por lo que atañe a la IAG, presentan algunos aspectos cuestionables que podrían ser objeto de mejora:

i) El primero de ellos ya ha sido mencionado. La Propuesta RC aplica las reglas sobre la carga de la prueba y el derecho de acceso a información relevante a los sistemas de IA de alto riesgo. La cuestión radica en ver si la IAG puede encajar en el ámbito de aplicación de la Propuesta. De todos modos, si se tiene en cuenta, por un lado, que estos modelos de IA pueden presentar un riesgo sistémico y, por otro lado, la aproximación que considero que debería hacerse entre estos modelos de IA y los sistemas de IA de alto riesgo, puede proponerse que, en el recorrido legislativo de la Propuesta se incorpore a los modelos de

19. Navas Navarro (2022: 27-45), Peguera Poch (2023: 45).

IA de propósito general entre los cuales se halla la IAG que presenten riesgos sistémicos. En la versión del RIA salida del Parlamento europeo el 14 de junio de 2022, a pesar de que se indicaba que la IAG y otros modelos fundacionales, no eran considerados de alto riesgo; sí se establecía que, si se empleaban en los contextos de alto riesgo que se establecen en el Anexo III del RIA, los implementadores debían cumplir con los requerimientos y obligaciones que se exigían para los sistemas de alto riesgo e, incluso, se indicaba que una modificación sustancial de un modelo fundacional implicaba que se considerara de alto riesgo debiéndose cumplir con las obligaciones y requerimientos exigidos para éstos (art. 29).

Como he expuesto en el epígrafe 3 de este trabajo, se establecen reglas más estrictas para los modelos de IA que presentan riesgos sistémicos, como la evaluación y mitigación de los riesgos, gestión de los incidentes graves, medidas de ciberseguridad robustas o medidas de corrección de esos incidentes, entre las más relevantes. Esto incide en la línea de entender que finalmente se pudieran introducir en la Propuesta RC al menos a los modelos de IA de riesgo sistémico junto con los sistemas de alto riesgo.

ii) En la última versión del RIA se ha introducido el art. 6.2 que establece que un sistema de IA (*stand-alone-AI system*) usado en uno de los contextos del Anexo III no se considera automáticamente un sistema de alto riesgo. Solo lo será si presenta un "riesgo significativo" de causar daño a las personas, su salud, su vida, seguridad o en general a los derechos fundamentales. Un "riesgo" como aparece definido en el RIA (art. 3.1) es "*la combinación de la probabilidad de que se produzca un daño y la gravedad de ese daño*". Aunque no queda claro qué se entiende por "significativo", del art. 6.3 RIA se deduce que, si el sistema de IA se aplica en los supuestos que establece, se entenderá que no produce un daño significativo a la salud, la seguridad o los derechos fundamentales de las personas, incluida la influencia en la toma de decisiones. Así, si el sistema de IA está destinado a realizar una tarea procedimental determinada limitada, pretende mejorar un resultado de una actividad humana previamente ejecutada, está destinado a detectar patrones de toma de decisiones o desviaciones de patrones de toma de decisiones anteriores y no está destinado a sustituir o influir en la evaluación humana, previamente completada, sin la debida revisión humana, o bien el sistema de IA está destinado a realizar una tarea preparatoria de una evaluación pertinente a efectos de los casos de uso enumerados en el anexo III, no se considerará que su empleo produce un riesgo significativo de producir un daño. Hay una excepción que tiene que ver con los sistemas de IA que elaboran perfiles de personas que se considerarán siempre de alto riesgo.

Así pues, en la última versión del RIA se pone el acento en los usos del sistema de IA para determinar si puede considerarse de alto riesgo o no. A ello se añade que el art. 7 RIA da poder a la Comisión europea para añadir o eliminar usos específicos del sistema que puedan considerarse de alto riesgo.

Unas normas similares deberían establecerse para los modelos de IA, en particular para la IAG, en lugar de hacer una bipartición entre riesgo sistémico y riesgo no sistémico basada casi exclusivamente en el poder computacional

(FLOPs). En efecto, los riesgos de la IAG pueden variar mucho según el contexto, el uso que se haga de la misma o si aparecen riesgos externos. Debido a la cantidad de usos y aplicaciones que puede tener la IAG como categoría de modelo de IA de aplicación general, es importante que la norma, esto es, el RIA, sea más granular como lo ha sido con los sistemas de IA de alto riesgo y establezca normas en función de usos frecuentes en la práctica o, mejor dicho, en la vida real[20].

En definitiva, se trataría de regular de forma similar, sino idéntica, los sistemas de alto riesgo y los modelos de IA de propósito general con riesgo sistémico, aunque fuera en secciones o capítulos independientes. Esto facilitaría el camino hacia la aplicación de normas de responsabilidad civil idénticas y a que los implementadores de modelos de IA tuvieran la obligación de elaborar la evaluación de impacto sobre los derechos fundamentales a la que se ven obligados los proveedores de sistemas de IA de alto riesgo.

iii) Las Propuestas de Directivas parten de la base de que la responsabilidad puede surgir de dos fuentes diferentes, de la culpa o del defecto de seguridad siempre en función de los requerimientos que exige el RIA y las obligaciones que los operadores económicos deben cumplir. Sin embargo, desde el punto de vista técnico, en caso de desarrollo de la IAG, no siempre se podrán cumplir con esos requerimientos ya que se desconoce la finalidad específica antes de su adaptación[21], por lo que no siempre se podrá predecir si puede existir un riesgo significativo de causar daños. Y si no se puede cumplir con los requerimientos que establece el RIA tampoco se aplicará consiguientemente las nuevas normas de RC que se pretenden establecer en la UE si lo único que se hace es equiparar los modelos de IA de propósito general a los sistemas de IA de alto riesgo. De ahí que se recomiende la combinación de la culpa y el defecto con métodos específicamente diseñados para lidiar con los aspectos técnicos concretos que presentan los modelos de IA de propósito general y, en concreto, la IAG[22].

iv) Finalmente, en ambas Propuestas se establece que la presunción iuris tantum de nexo causal o de la existencia de un defecto no se aplicará cuando el demandado demuestre que el demandante podía acceder de forma razonable a todos los conocimientos especializados e información necesaria acerca del funcionamiento del sistema (art. 4.4 Propuesta RC, art. 9.5 Propuesta PLD).

Estos dos preceptos deberían tener una redacción similar. De hecho, el segundo debería recoger la redacción del primero que estatuye lo siguiente: *"en el caso de las demandas por daños y perjuicios relacionadas con sistemas de IA de alto riesgo, los órganos jurisdiccionales nacionales no aplicarán la presunción establecida en el apartado 1 cuando el demandado demuestre que el demandante puede acceder razonablemente a pruebas y conocimientos especiali-*

20. Novelli, et al. (2024: 2-3).
21. Bommasani, et al. (2022: 13).
22. Novelli, et al. (2024: 5-6).

zados suficientes para demostrar el nexo causal mencionado en el apartado 1". A estos conocimientos especializados y a las pruebas no alude el art. 9.5 Propuesta PLD.

Pues bien, en el caso de la IAG esta norma debe enlazarse con la obligación de transparencia del art. 51 RIA que corresponde al proveedor en virtud de la cual se tiene que informar al usuario, como mínimo, de que está tratando con un sistema de IA o que el contenido se ha generado artificialmente. Por lo tanto, el demandado tendrá aquí un argumento que le ayude a desvirtuar la presunción. El extremo, sin embargo, que no aclara el RIA, es la cuestión de cómo se notifica al usuario esa información y ello es importante, en este caso, a efectos de prueba.

De todos modos, quedaba en el aire en las Propuestas el contenido de esa información y conocimientos especializados, de ahí que se proponga que ambas establezcan un contenido que se cohoneste con lo que establece el RIA tanto para los sistemas de alto riesgo como para los modelos de IA que presenten riesgos sistémicos, los cuales, insistimos, deberían equipararse, en el RIA, a efectos de regulación. Me refiero, en concreto, a los requerimientos que se exigen en caso de sistemas de alto riesgo. En ellos se tiene la base para determinar el contenido de la documentación que permita dar información necesaria al usuario del sistema. Por otro lado, debería incentivarse que los proveedores e implementadores de IAG vayan informando a lo largo del ciclo de vida del sistema o modelo de IA, de los potenciales riesgos de daños que pudieran acaecer a los usuarios (art. 55 RIA). Esto ayudaría a refutar la presunción pues sí estaría al alcance de la víctima la información y conocimiento necesario acerca del sistema o modelo de IA al habérsela puesto el demandado a su disposición. El art. 53.1 RIA establece la obligación general para los proveedores de modelos de IA de propósito general, en los que se insertaría la IAG, de mantener actualizada toda la información relativa al funcionamiento del modelo y hacer público un sumario lo suficientemente detallado sobre el contenido usado para entrenar al modelo de IA que permita hacerse una idea general y siempre respetando los derechos de propiedad intelectual, industrial y secreto comercial. Es un paso en esa línea, pero no es suficiente pues debería complementarse desde la perspectiva de la víctima o potencial víctima con una regulación de este aspecto en las Propuestas de Directiva que trato.

5. CONCLUSIÓN

Los vaivenes de la regulación de la IAG desde que vio la luz ChatGPT no dejan de llamar la atención: de resultar inexistentes desde un punto de vista legal a regular los modelos fundacionales en el RIA hasta la actual redacción de los modelos de IA de propósito general. Todo ello está generando bastante desconcierto en la comunidad científica y, en particular, en la jurídica. Que habiéndose aprobado el RIA y estando ya en el último trámite se publique una versión corregida el 16 de abril de 2024 en la que se introducen cambios tan sustancia-

les pone en cuestión, en mi humilde opinión, la "*rule of law*" y el proceso democrático en la UE. No se trata simplemente de correcciones. La corrección de una norma en general —y de ésta en particular— no es una pura corrección de estilo, sino que es una modificación sustancial del texto, tan sustancial, que debería volver a analizarse, debatirse, estudiarse y votarse en el seno del Parlamento europeo. De la versión del RIA consensuada en el "trilogue" a la versión corregida hay casi un abismo del que quiero dejar constancia a modo de conclusión.

Por otro lado, en este trabajo abogo porque los sistemas de IA de alto riesgo y los modelos de IA de propósito general que presenten riesgos sistémicos reciban, a efectos especialmente de los daños ocasionados por ellos, el mismo tratamiento jurídico en las futuras Directivas que se van a cuidar de regular esta materia, si bien combinando los dos fundamentos de la responsabilidad: culpa y riesgo.

BIBLIOGRAFÍA

AA VV (2024). *Derecho de contratos, responsabilidad extracontractual e inteligencia artificial*. Álvarez, N. (coord.). APDC, Thomson Reuters.

Bommasani, R., et al. (2022). *On the Opportunities and Risks of Foundation Models*. arXiv. https://doi.org/10.48550/arXiv.2108.07258. Fecha de la consulta: junio 2024.

De Bruyne, J. et al., (2022). *The European Commission's Approach To Extra-Contractual Liability and AI – A First Analysis and Evaluation of the Two Proposals*. CiTiP Working Paper. KU Leuven Centre for IT & IP Law 6 October 2022, 36.

Hacker, P. (2023). *What's Missing from the EU AI Act: Addressing the Four Key Challenges of Large Language Models*, Verfassungsblog, diciembre, https://doi.org/10.17176/20231214-111133-0. Fecha de la consulta: mayo 2024.

Hacker, P., Engel, A., Mauer, M., (2023) *Regulating ChatGPT and other Large Generative AI Models*. working paper, arXiv:2302.02337v8. Fecha de la consulta: junio 2024.

Jorqui Azofra, M. (2023). *Responsabilidad por los daños causados por productos y sistemas de inteligencia artificial*. Dykinson.

Navas Navarro, S. (2022). *Régimen europeo en ciernes en materia de responsabilidad derivada de los sistemas de inteligencia artificial, Revista CESCO*. núm. 4. 27-51.

Navas Navarro, S. (2023). *Datos sanitarios electrónicos. El espacio europeo de datos sanitarios*. Reus.

Navas Navarro, S. (2023). *ChatGPT y otros modelos fundacionales. Aspectos jurídicos de presente y de futuro*. Reus.

Novelli, C., et al. (2024). *Generative AI in EU Law: Liability, Privacy, Intellectual property, and Cybersecurity*, working paper, 14 de enero de 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4694565. Fecha de la consulta: junio 2024, 2-3.

OECD (2019), "Scoping the OECD AI principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO)", *OECD Digital Economy Papers*, No. 291, OECD Publishing, Paris, https://doi.org/10.1787/d62f618a-en. Fecha de la consulta: junio 2024.

PEGUERA POCH, M. (coord.) (2023). *Perspectivas regulatorias de la inteligencia artificial en la Unión europea*. Reus.

II. Empresa y actividad

Reglamento de mercados digitales: ¿Una solución a los problemas del art. 102 TFUE?[1]

Carles Górriz López
Profesor titular de Derecho mercantil
Universitat Autònoma de Barcelona

ABSTRACT:
The European Union has a reputation for standing up to big companies and fighting their abuses, using tools such as Article 102 of the TFEU. However, this provision has proved insufficient to confront the technological giants, which is why the Digital Markets Act was adopted. I compare these two rules to identify the strengths and weaknesses of the latter. Among the former ones, the preventive control and short deadlines stand out. However, it does not extend the Commission's powers to control mergers in the digital sector and lacks provisions for private enforcement.

Keywords: Digital Markets Act – Abuse of a dominant position – Gatekeepers – Core platform services

Palabras clave: Reglamento de Mercados Digitales – Abuso de posición de dominio – Guardianes de acceso – Servicios básicos de plataforma

1. Se ha accedido por última vez a las páginas web citadas el 13 de junio de 2024.

1. INTRODUCCIÓN

El Derecho de la competencia es esencial no sólo para la economía de un país sino para su democracia puesto que, como explicó el juez Louis Brandeis, los ciudadanos no son realmente libres si viven esclavizados por sus condiciones económicas[2]. De ahí que sea vital contar con leyes que velen para que exista competencia en el mercado y eviten que las grandes empresas abusen de su poder económico. Entre ellas destaca el artículo 102 del Tratado de Funcionamiento de la Unión Europea (TFUE) que prohíbe que una o varies empresas abusen de su posición de dominio en el mercado interior, en la medida en que afecte o pueda afectar al comercio entre Estados miembros. Sin embargo, se trata de una norma parca y vetusta. Parca porque no define qué debe entenderse por posición de dominio ni por abuso; simplemente proporciona cuatro ejemplos del último, cuya eficacia se ha visto reducida desde que en 2008 la Comisión abandonase la aproximación formal (*form-based approach*) en favor de la efectista (*effects-based approach*)[3]. Y vetusta porque desde que en 1957 se aprobara el Tratado de la Comunidad Económica Europea, cuyo artículo 86 constituía el antecedente del 102 actual, su contenido apenas ha variado. De ahí que suscite dudas su adecuación a la nueva realidad económica; sobre todo, a los mercados digitales[4]. La importancia que tienen en ellos las economías de escala, los efectos de red, la bi- o multilateralidad, los datos y la integración vertical determinan que estén muy concentrados y gobernados por un grupo reducido de empresas que detentan un gran poder económico y social[5].

2. Wu, 2018, 42 y 55.

3. Orientaciones sobre las prioridades de control de la Comisión en su aplicación del artículo 82 del Tratado CE a la conducta excluyente abusiva de las empresas dominantes (2009/C 45/02).

4. Podszun, 2023, 2 y 5; Budzinski y Mendelsohn, 2021, 5.

5. Crémer, De Montjoye y Schweitzer, 2019, 2 y 20; Furman, 2019, 22 ss.; Stigler Center for the Study of the Economy and the State, 2019; Federal Ministry for Economic Affairs and Energy, 2019, 13 ss.; Khan, 2017, 710; Baker, 2019, 122 ss.; Competition and Markets Authority, 2020, 16 ss.; Tirole, 2018, 406 ss.; Ezrachi y Robertson, 2019, 5. En sentido crítico, Díez Estella, 2021, 111. Igualmente, la professora Herrero (2021, 111) relativiza la existencia de barreras de acceso al tratarse de mercados muy dinámicos y la competencia basarse más en la innovación que en el precio.

Ante esta disyuntiva, la Unión Europea tenía esencialmente dos opciones: revisar el artículo 102 y adecuarlo a la evolución económica o mantenerlo como está y confiar en que la Comisión y el Tribunal de Justicia fueran adecuando su interpretación a los cambios socioeconómicos. Parece haber tirado por la vía de en medio al aprobar una disposición nueva que no deroga la anterior: el Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (en adelante "Reglamento de Mercados Digitales", pero más conocido en la práctica como "*Digital Markets Act*")[6]. Su finalidad es conseguir que exista competencia leal en los mercados digitales que se hallan controlados por gigantes tecnológicos. Según el Comisario europeo de Mercado Interior, Thierry Breton, constituye una ley armonizadora, que impone un control preventivo, mejora la aplicación al hacerla más eficiente y cuenta con sanciones desincentivadoras para aumentar la seguridad, la confianza, la innovación y la igualdad de oportunidades en el sector digital[7].

El objeto de este trabajo es comprobar si las palabras de Thierry Breton son ciertas; es decir, si, y en qué medida, el Reglamento de Mercados Digitales va a suponer una mejora respecto del artículo 102 TFUE. Para ello, nos posicionamos brevemente sobre su naturaleza jurídica, analizamos su ámbito de aplicación, comparamos la posición de dominio con los guardianes de acceso, explicamos en qué consiste el control *ex ante* que introduce y en qué se diferencia del abuso de posición de dominio y pasamos revista a los principales hitos de los procedimientos, remedios y sanciones que se pueden imponer a la luz de las dos normas. Terminamos con las conclusiones preceptivas.

2. NATURALEZA JURÍDICA

Las diferencias entre las dos normas objeto de análisis parecen evidentes por lo que respecta a su naturaleza: el artículo 102 TFUE forma parte del Derecho primario de la Unión Europea, mientras que el Reglamento de Mercados Digitales del secundario. Sin embargo, las consecuencias de esta diferencia son mínimas en la praxis, ya que los reglamentos comunitarios tienen efecto directo: no sólo vinculan a las Administraciones Públicas sino que los tribunales de los Estados miembros tienen que aplicarlos cuando un litigio entra dentro de su ám-

6. Aunque entró en vigor el 1 de noviembre de 2022, su eficacia se retrasó hasta el 2 de mayo de 2023 o el 25 de junio de 2023. *Cfr* su artículo 54. Véase un análisis económico de la propuesta en Cabral, Haucap, Parker, Petropoulos, Valletti y Van Alstyne, 2021, y una comparación con las iniciativas británica y alemana en Botta, 2021, 500 ss.

7. Comisión Europea, 2020a. Es también la posición de buena parte de la doctrina; por ejemplo Monti, 2021, 1 ss., Ibáñez, 2021, 574 y Vilà, 2022, 217 s., quien predica el "efecto Bruselas" de los Reglamentos de Mercados Digitales y de Servicios Digitales. En cambio, Portuese (2022, 3 ss./24) denuncia que el Reglamento incrementará la fragmentación legislativa de los mercados digitales.

bito de aplicación. Por lo tanto, si una empresa incumple los deberes que le impone el Reglamento, los perjudicados podrán acudir a los tribunales nacionales y solicitar la indemnización de los daños sufridos[8]. Ahora bien, esa norma carece de previsiones sobre su aplicación privada, que no se regirá por el Título VI de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia (en adelante, LDC), ni por los arts. 283 bis a) ss. de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. La razón es que estas normas derivan de la Directiva 2014/104/UE[9], que circunscribe su eficacia a las indemnizaciones de daños y perjuicios que deriven de la infracción de los artículos 101 y 102 del TFUE o del Derecho nacional en materia de competencia (*cfr.* art. 2.1). Y el legislador español ha confinado la eficacia del Título VI de la LDC a la infracción de los citados preceptos y de sus artículos 1 y 2[10]. Por lo tanto, el plazo para ejercitar la acción de indemnización por incumplirlo no serán los 5 años previstos en el art. 74.1 LDC, sino 1 año al tratarse de una acción de responsabilidad extracontractual. Y tampoco será de aplicación la presunción de que han existido las infracciones de Derecho de la competencia derivadas de las resoluciones de las autoridades competentes en la materia (*cfr.* art. 75 LDC).

La adscripción del Reglamento de Mercados Digitales genera dudas, a diferencia del artículo 102 que forma parte del Derecho de la competencia. La mayoría de la doctrina considera que tiene naturaleza regulatoria, similar a las telecomunicaciones o sector financiero, por ejemplo[11]. Más minoritaria es la opinión de que se trata de normas especiales de Derecho de la competencia, aunque también cuenta con argumentos sólidos que la sustentan[12]. Y tampoco faltan los autores que adoptan una posición intermedia[13].

Nos alineamos con la primera tesis en base a tres argumentos. El primero es el fundamento jurídico de la norma objeto de análisis, pues reside en el artículo 114 TFUE, que forma parte del Capítulo dedicado a la aproximación de las legislaciones de los Estados miembros. Si el Reglamento se inscribiera dentro del Derecho de la competencia, su fundamento sería el artículo 103 del TFUE, que permite al Consejo desarrollar legislativamente los artículos 101 y 102 del TFUE. Con todo, hay que tener en cuenta las objeciones que se han hecho a la utiliza-

8. Bueso, 2023, 106 ss.

9. Directiva 2014/104/UE del Parlamento Europeo y del Consejo, de 26 de noviembre de 2014, relativa a determinadas normas por las que se rigen las acciones por daños en virtud del Derecho nacional, por infracciones del Derecho de la competencia de los Estados miembros y de la Unión Europea.

10. Nos sumamos a la propuesta del profesor Ruiz Peris (2023, 37/37) de reformar la LDC para dar cabida a las acciones de daños por la violación del Reglamento de Mercados Digitales, a imagen de lo que ha hecho el legislador alemán.

11. Cappai, Colangelo, 2023, 444; Kerber, 2021, 2 ss y 10 s/13; Podszun, 2023, 6 ss.; Budzinski y Mendelsohn, 2021, 2 15 ss.; Van Den Boom, 2023, 63-65; Ibáñez, 2021, 561 s.

12. Petit, 2021, 2 y 4 s/24. Parece también la posición de Andriychuk, 2021, 263 ss., quien defiende que el objetivo principal es conseguir que exista competencia entre plataformas (también 274 ss.

13. Bueso, 2023, 106; Larouche, De Streel, 2021, 543 ss.; Beems, 2023 y Massa, 2022, 113.

ción del artículo 114 como base jurídica y que podrán servir de defensa a los guardianes de acceso hasta que el Tribunal de Justicia se pronuncie al respecto[14]. El segundo argumento reside en los apartados 5 y 6 del artículo 1 del Reglamento de Mercados Digitales. Resulta harto significativo que el primero prohíba a los Estados miembros aprobar normas que impongan deberes a los guardianes de acceso cuya finalidad sea conseguir mercados disputables y equitativos, pero que salve la eficacia de las normas de la competencia, tanto europeas como de los Estados miembros[15]. Es decir, no podrán adoptar leyes, en sentido amplio, que tengan el mismo objeto y finalidad que el Reglamento, salvo si forman parte del Derecho de la competencia. La última razón tiene que ver con la finalidad de la norma; o mejor, dicho, con la explicación que el legislador comunitario da al respecto. El artículo 1.1 establece claramente que es garantizar la disputabilidad y la equidad de los mercados en el sector digital, lo que puede interpretarse en el sentido de que se desea que reine la competencia leal en ellos[16]. La doctrina ha debatido sobre si este objetivo es propio o ajeno al Derecho de la competencia, pues se trata de conseguir que exista competencia en el sector digital; y la iniquidad (que también podría traducirse como "deslealtad") puede considerarse como una forma de abuso del poder económico. A pesar del interés del debate, resulta más relevante el considerando 11, según el cual la finalidad del Reglamento no es la misma que la de los arts. 101 y 102 TFUE sino distinta y complementaria. La *ratio* de esta declaración es sortear la prohibición del *non bis in idem*. De la última jurisprudencia del Tribunal de Justicia se desprende que el artículo 50 de la Carta de Derechos Fundamentales de la Unión Europea rige la aplicación pública del Derecho de la competencia[17]. Y también que difícilmente dos sanciones en esta materia podrán beneficiarse de la excepción prevista en el artículo 52 de la misma norma. En cambio, sí pueden escapar a la prohibición dos procedimientos o sanciones que protejan intereses jurídicos diferentes mas complementarios.

La diferente adscripción del Reglamento de Mercados Digitales respecto del Derecho de la competencia determina que la jurisprudencia y práctica administrativa de esta última no vinculen a la Comisión al aplicar aquella norma[18]. Por ejemplo, la atribución de la condición de guardián de acceso no precisa delimitar previamente el mercado relevante ni probar la existencia de una posición de dominio en él. Igualmente, los posibles efectos procompetitivos de la actividad

14. Véase Lamadrid, Bayón, 2021, 578-586. Esencialmente afirmaron que la propuesta de Reglamento no tenía por finalidad terminar con la fragmentación legislativa y que era desproporcionada.

15. Respecto de la interpretación de estos dos preceptos, Van Den Boom, 2023, 68 a 77.

16. Cfrs. los considerandos 32 y 33 del Reglamento, así como Schweitzer, 2021, 7 ss.; Díez Estella, 2023, 59 ss.; Andriychuk, 2021, 261, 264 y 274 ss.; Larouche y De Streel, 2021, 553. Críticamente Budzinski y Mendelsohn, 2021, 17 s.

17. Analizo esta cuestión en Górriz, 2024. Respecto del Reglamento de Mercados Digitales, Ribera Martínez, 2023 y Cappai y Colangelo, 2023.

18. Ibáñez, 2021, 568 y 572.

no liberan a los guardianes de acceso de cumplir las obligaciones y prohibiciones previstas en los artículos 5 a 7.

3. ÁMBITO DE APLICACIÓN

Los ámbitos de aplicación del artículo 102 TFUE y del Reglamento de Mercados Digitales son diferentes, resultando mucho más amplio el primero. En efecto, su destinatario es la empresa, que ha sido definida como una unidad económica que ofrece bienes y servicios en un mercado, siendo indiferente la forma jurídica, su financiación o la atribución de personalidad[19]. El artículo 102 rige en todos los mercados, con independencia de que existan normas sectoriales que se apliquen concurrentemente[20]. Existen dos requisitos de internacionalidad. De un lado, la empresa debe detentar una posición dominante en, al menos, una parte sustancial del mercado interior. De otro, la conducta objeto de análisis debe afectar, actual o potencialmente, al comercio entre Estados miembros.

El Reglamento de los Mercados Digitales ciñe esencialmente su eficacia a los "servicios básicos de plataformas" prestados por "guardianes de acceso" cuando sus destinatarios estén establecidos en la Unión Europea (artículo 1.2). El apartado 2 del artículo 2 enumera taxativamente los primeros: a) servicios de intermediación en línea; b) motores de búsqueda en línea; c) servicios de redes sociales en línea; d) servicios de plataformas de distribución de vídeos; e) servicios de comunicaciones interpersonales independientes de la numeración; f) sistemas operativos; g) navegadores web; h) asistentes virtuales; i) servicios de computación en nube; y j) servicios de publicidad en línea[21]. Se caracterizan por el impacto que tienen en ellos las economías de escala, los efectos de red, la importancia de los datos, su operatividad en mercados con dos o más lados, la

19. Por ejemplo, STJUE 6.10.2021, *Sumal* (C882/19), ECLI:EU:C:2021:800, párr. 41.

20. Giorgio Monti (2008, 123) se refiere a la STJUE 11.11.1997, *Comisión y Francia / Ladbroke Racing* (C-359/95 P y C-379/95 P), ECLI:EU:C:1997:531. Sin embargo, él se posiciona en sentido contrario al considerar que puede haber casos en que las normas de la competencia deban ceder el paso a las regulatorias. A nuestro modesto entender, el fallo referido no sirve de sustento a la afirmación de la primacía del Derecho europeo de la competencia sobre las normas regulatorias puesto que se refiere a las nacionales. El Tribunal de Justicia explica que los arts. 85 y 86 del Tratado de la Comunidad Económica Europea (actualmente 101 y 102 TFUE) se aplican sólo a los comportamientos de las empresas adoptados libremente, pero no a los que vengan impuestos por la normativa nacional. En este último caso, no debe analizarse la legitimidad de los acuerdos o prácticas unilaterales sino de la legislación del Estado miembro en cuestión; en particular, su compatibilidad con las normas *antitrust* de la Unión Europea (párrs. 20, 21 y 33 a 36).

21. Los apartados 3 y 4 del artículo 1 matizan el alcance de la lista al excluir determinados servicios; esencialmente las redes de comunicaciones electrónicas y los servicios de comunicaciones electrónicas. Pero sí quedan sometidos al Reglamento los servicios de comunicaciones interpersonales independientes de la numeración, a pesar de que puedan ser calificados como servicios de comunicaciones electrónicas.

facilidad de aprisionar a los consumidores y de que éstos se atrincheren en una único dispositivo, red, plataforma o ecosistema, así como la posibilidad de integración vertical[22]. Estas características determinan que la disputabilidad sea mínima y el riesgo de deslealtad muy elevado[23].

El listado presenta el riesgo consustancial a toda enumeración: la obsolescencia. Más aún si tenemos en cuenta la vertiginosa velocidad a la que evoluciona la tecnología. Consciente de ese problema, el legislador europeo ha introducido una previsión para neutralizarlo. El artículo 19 permite a la Comisión ampliar o modificar la lista si considera que no se adapta a la realidad económica.

El Reglamento de Mercados Digitales no se aplica a cualquier empresa que preste servicios básicos de plataforma; ni siquiera a las grandes o a las que detentan una posición de dominio. Su eficacia aparece constreñida a los "guardianes de acceso", que el art. 2.1 define como las empresas prestadoras de servicios básicos de plataforma designadas por la Comisión conforme al artículo 3, que analizaremos en el epígrafe siguiente. Por ahora basta con indicar que su apartado 2 establece unos umbrales económicos cuya superación genera la presunción de que la sociedad en cuestión reúne los requisitos que exige el apartado 1 para calificarla como guardián de acceso. Se trata de unos umbrales tan elevados que sólo seis gigantes tecnológicos los superaron a fecha de 6 de septiembre de 2023: Alphabet, Amazon, Apple, Bytedance, Meta y Microsoft; a los que se añadió Booking el 13 de mayo de 2024[24]. Y no se espera que en el futuro sean muchas más.

El tercer elemento del ámbito de aplicación es territorial: el artículo 1.2 exige que los usuarios de los servicios básicos de plataforma residan en territorio comunitario. El Reglamento distingue dos tipos: los profesionales y los finales. Los números 20 y 21 del art. 2 los definen de forma un tanto tautológica: mientras describe los últimos de forma negativa, por no ser consumidores profesionales, éstos aparecen identificados por utilizar servicios básicos de plataforma para proporcionar productos o prestar servicios a los consumidores finales, o bien para integrarlos en actividades empresariales dirigidas a éstos. Sin embargo, la idea está clara: el Reglamento de Mercados Digitales sólo se aplica cuando los destinatarios de los servicios básicos de plataforma —sean consumidores finales o profesionales— residan en la Unión Europea. Igualmente, carece de importancia su nacionalidad, incluso cuando es la de un tercer país. Y lo mismo sucede con la nacionalidad o el establecimiento de los guardianes de acceso: carecen de pertinencia, lo cual es un acierto, pues la inmensa mayoría no son europeos —normalmente son estadounidenses o chinos—. El único dato relevante es el

22. Véase De Streel, Feasey, Kraemer y Monti, 2021, 9 ss.

23. Van Den Boom, 2023, 60 y Massa, 2022, 111.

24. https://digital-markets-act.ec.europa.eu/gatekeepers_en y https://digital-markets-act.ec.europa.eu/commission-designates-booking-gatekeeper-and-opens-market-investigation-x-2024-05-13_en.

domicilio o el establecimiento de los destinatarios de los servicios básicos de plataforma prestados por los guardianes de acceso.

4. POSICIÓN DE DOMINIO VS GUARDIÁN DE ACCESO

El Reglamento de Mercados Digitales tiene como protagonista al guardián de acceso. Aunque las empresas que reciben esa calificación pueden tener una posición de dominio, se trata de dos estatutos diferentes. Para comprobarlo conviene recordar en que consiste la última figura. La jurisprudencia comunitaria la ha caracterizado como

… una situación de poder económico en que se encuentra una empresa y que permite a ésta impedir que haya una competencia efectiva en el mercado de referencia, confiriéndole la posibilidad de comportarse con un grado apreciable de independencia frente a sus competidores, sus clientes y, finalmente, los consumidores …[25].

La falta de concreción de esta definición lleva a la Comisión y a los órganos judiciales europeos a utilizar factores estructurales y de comportamiento para evaluar si una empresa tiene suficiente poder económico para impedir que exista competencia eficiente en el mercado y comportarse de forma independiente. El más importante es la cuota de mercado; sobre todo de la empresa investigada. Ahora bien, la de los competidores también desempeñan un papel capital para evaluar la autonomía de comportamiento. Otros elementos relevantes son las estructuras del mercado y de la compañía en cuestión, la existencia de barreras de entrada y expansión, así como la falta de contrapoder de proveedores y consumidores.

Para determinar si una empresa detenta una posición de dominio resulta necesario delimitar el mercado relevante, pues permite valorar a qué presiones concurrenciales se halla sometida[26]. Constituye una tarea muy compleja, no sólo porque requiere conocimientos de economía, sino también porque existe una multiplicidad de productos y empresas que ofrecen bienes y servicios muy distintos, así como diversos niveles de sustitución[27]. La dificultad aumenta al analizar sectores nuevos, como el digital, porque los criterios tradicionales pueden

25. STJUE de 13.2.1979, *Hoffmann-La Roche v. Commission* (C-85/76), ECLI:EU:C:1979:36, párr. 38.

26. El Tribunal de Justicia lo considera un requisito necesario para valorar si una sociedad tiene una posición de dominio. Por ejemplo, sentencia de 30.1.2020, *Generics (UK) Ltd* (C-307/18), ECLI:EU:C:2020:52, párr. 127.

27. Ezrachi (2014, 33) explica que esta complejidad determina que la revisión que hace el Tribunal de Justicia de la delimitación del mercado relevante hecha por la Comisión sea muy limitada. El Tribunal General expresa la misma opinión en la sentencia de 9.9.2009 *Clearstream / Comisión* (T-301/04), ECLI:EU:T:2009:317. Sin embargo, en el párrafo 47 la matiza:

haber perdido importancia. Es el caso de la cuota de mercado: pese a continuar teniendo gran relevancia hoy en día, existen otros factores, como la innovación o la privacidad, que condicionan la reacción de los incumbentes a la aparición de nuevos operadores[28]. Por otra parte, no existe ninguna norma legal que especifique cómo llevar a cabo esta operación. La Comisión ha explicado su práctica en dos Comunicaciones: la primera se remonta a 1997[29] y la segunda, que sustituye a la anterior, data de 2024[30]. Esta publicación evidencia la preocupación de la autoridad europea de la competencia por los mercados digitales, pues contiene diversas previsiones específicas para ellos. Por ejemplo, destaca que la innovación o la privacidad pueden ser elementos tan importantes como el precio de las mercancías. Declara que el número de usuarios activos, de visitas a páginas web o de transmisiones en directo, las descargas y actualizaciones o el número de interacciones pueden ser factores relevantes para calcular el poder que una empresa tiene en el mercado. Y contiene normas especiales para los mercados en los que operan plataformas multilaterales y los ecosistemas digitales, entre otros. Ahora bien, la Comunicación de 2024 no va a resolver todos los problemas, ni mucho menos. La delimitación del mercado relevante sigue siendo tremendamente difícil y, a buen seguro, fuente de enfrentamientos entre la Comisión y las grandes tecnológicas.

El artículo 3.1 del Reglamento de Mercados Digitales caracteriza a los guardianes de acceso por tres notas: i) tener una fuerte influencia en el mercado interior, ii) proporcionar servicios de plataforma básicos que constituyan una puerta de entrada para que los usuarios profesionales lleguen a los usuarios finales, y iii) tener una posición de mercado arraigada y duradera[31]. Como estas

---

… el juez comunitario no puede abstenerse de controlar la interpretación de los datos de carácter económico efectuada por la Comisión. Al respecto, debe verificar la exactitud material, la fiabilidad y la coherencia de los elementos probatorios en los que la Comisión ha basado su apreciación, y que tales elementos constituyen el conjunto de datos pertinentes que deben tomarse en consideración para apreciar una situación compleja y sean adecuados para sostener las conclusiones que se deducen de los mismos.

28. El Tribunal General se ha hecho eco de esa realidad y, en la sentencia de 14.9.2022, *Google Android* (T-604/18), ECLI:EU:T:2022:541, párr. 115, afirmó:

… where traditional parameters such as the price of products or services or the market share of the undertaking concerned may be less important than in traditional markets, compared to other variables such as innovation, access to data, multi-sidedness, user behaviour or network effects.

29. Comunicación de la Comisión relativa a la definición de mercado de referencia a efectos de la normativa comunitaria en materia de competencia (Diario Oficial C 372, de 9 de diciembre de 1997).

30. Comunicación de la Comisión relativa a la definición de mercado de referencia a efectos de la normativa de la Unión en materia de competencia (Diario Oficial C/2024/1645, de 22 de febrero de 2024). Al respecto, Eben, 2024.

31. Sobre la designación del guardián de acceso, Geradin, 2021, 5/20, quien subraya que el aspecto central de la condición de guardián de acceso es la dependencia que tienen los usuarios profesionales y la diferencia de poder económico. De ahí que atribuya gran importancia al hecho que los consumidores utilicen una o varias plataformas (*multi- o singlehoming*). Téngase en cuenta también la crítica de Díez Estella, 2023, 66 ss.

características tienen un alto grado de abstracción, el apartado 2 establece unos umbrales económicos cuya superación genera la presunción de que la empresa en cuestión reúne los requisitos del apartado 1[32]. Se trata, empero, de una presunción relativa que puede ser quebrada. A esos efectos, la empresa afectada debe proporcionar a la Comisión los argumentos necesarios para convencerla de que, pese a superar las cifras previstas en el apartado 2, no debe ser calificada como "guardián de acceso" (art. 3.5). La Comisión deberá valorar esos argumentos y decidir si tienen fundamento suficiente como para rechazar la presunción existente[33]. En caso de que considere que sí lo tienen, abrirá una investigación de mercado conforme al artículo 17.1 para adoptar la decisión definitiva. Y lo mismo puede suceder en sentido inverso: la Comisión puede designar "guardián de acceso" a una empresa que no alcance los umbrales económicos pero reúna las características del apartado 1 del artículo 3. A esos efectos, iniciará una investigación de mercado en la que valorará los elementos previstos en el segundo párrafo del art. 3.8.

La posibilidad de excluir la presunción del apartado 2 tiene carácter excepcional, de modo que procede una interpretación restrictiva de la misma. Así resulta de la letra del apartado 5 que introduce con el adverbio "excepcionalmente" la posibilidad de demostrar que, pese a superar los umbrales referidos, una empresa no reúne los requisitos para ser considerada guardián de acceso. Y también apoya esa exégesis la diferencia con el apartado 8, que carece de una precisión similar para la hipótesis inversa.

Es importante hacer hincapié en dos aspectos al comparar el guardián de acceso con la posición de dominio. Primero, es necesario un acto de designación por parte de la Comisión para que una empresa merezca aquella consideración y deba cumplir determinados deberes en relación con los servicios de plataforma que se le asignan. Hasta que no se produzca ese acto, la empresa no será un guardián de acceso ni tendrá obligación o prohibición especial. Eso sí, cuando un prestador de servicios básicos de plataforma supere las cifras previstas en el apartado 2, deberá notificar esa situación "sin demora" a la Comisión, proporcionándole la información correspondiente.

En segundo lugar, la designación como guardián de acceso es independiente de la posesión de una posición dominante. La Comisión impondrá esa condición a una empresa sobre la base de las características del apartado 1 del artículo 3 y los umbrales económicos del apartado 2. No es necesario que pruebe que detenta suficiente poder económico para influir de forma determinante en

32. Véase la crítica de Geradin, 2021, 13-15/20.

33. Ha sido el caso de Bytedance Ltd, propietaria de la plataforma de entretenimiento TikTok. El 5 de septiembre de 2023 la Comisión europea la designó guardiana de acceso al superar los umbrales del artículo 3.2 y no haber proporcionado pruebas de que no reunía los requisitos del artículo 3.1. La empresa ha recurrido solicitando la nulidad de la designación y la adopción de medidas cautelares en ese sentido que fueron desestimadas por el Tribunal General mediante Auto de 9.2.2024 (T-1077/23), ECLI:EU:T:2024:94. En la sentencia de 17 de julio de 2024 (T-1077/23 - ECLI:EU:T:2024:478), el Tribunal General ha rechazado la petición de Bytedance.

el mercado y actuar con independencia de cómo reaccionen sus clientes, proveedores y rivales[34]. Igualmente, no tiene que delimitar el mercado relevante, con todas las dificultades que esta operación conlleva. Simplemente designará a una empresa como guardián de acceso a la luz de la información que ésta le proporcione o bien de una investigación de mercado[35].

5. DEBERES DE LOS GUARDIANES DE ACCESO

5.1. Abuso de posición de dominio

La clave del Reglamento de Mercados Digitales reside en la imposición de obligaciones y prohibiciones a los guardianes de acceso (arts. 5 a 15). Para valorarlas correctamente, conviene recordar la prohibición del artículo 102 TFUE. Como es por todos bien conocido, este precepto no veta la posición de dominio sino solamente su abuso. Ahora bien, no define este elemento; su apartado segundo alude a cuatro conductas que han sido consideradas por la jurisprudencia comunitaria como simples ejemplos de comportamientos ilícitos. Por lo tanto, las instituciones han tenido que construir el concepto y, como es natural, las dificultades han sido múltiples; entre otras razones, porque el criterio utilizado ha ido variando a lo largo del tiempo[36]. Ahora bien, desde hace algún tiempo, el Tribunal de Justicia utiliza la misma definición de "abuso", que gira alrededor de la llamada "competencia en méritos"[37]. Una empresa explota ilícitamente su posición de dominio cuando recurre a métodos diferentes de los que rigen una competencia normal o basada en sus méritos; es decir, no intenta mantener o

---

34. Petit (2021, 6 ss y 9/24) afirma que estas mismas razones están detrás de la ausencia de medidas de tutela en el proceso de designación de una empresa como guardián de acceso; pero pronostica que esta ausencia originará litigios en el futuro. Por su parte, Heimann (2022) subraya que la calificación de 'guardián' es menos compleja que establecer que una empresa tiene una posición dominante, por lo que la Comisión no necesitará dedicar tantos recursos al control.

35. En caso de que una empresa incumpla su obligación de notificar que supera los umbrales del artículo 3.2 o no proporcione toda la información pertinente, la Comisión podrá también designarla como guardián de acceso en virtud de la información de que disponga. Así lo establece el segundo párrafo del art. 3.3.

36. O'Donoghue y Padilla, 2020, 264 ss.

37. En la sentencia de 17.2.2011, *TeliaSonera* (C-52/09), ECLI:EU:C:2011:83, el Tribunal de Justicia explica que el abuso:

…es un concepto objetivo que tiene por objeto los comportamientos de una empresa en posición dominante que, en un mercado donde la competencia ya está debilitada, precisamente por la presencia de la empresa en cuestión, tienen por efecto impedir, por medios distintos de los que rigen una normal competencia entre productos o servicios sobre la base de las prestaciones de los agentes económicos, el mantenimiento del grado de competencia que aún existe en el mercado o su desarrollo (…) (párr. 27).

En el mismo sentido sentencias de 14.10.2010, *Deutsche Telekom* v *Commission* (C-280/08 P), ECLI:EU:C:2010:603, párr. 174 y de 30.1.2020, *Generics (UK) y otros* (C-307/18), ECLI:EU:C:2020:52, párr. 148.

incrementar su poder ofreciendo mejores productos, más económicos, más innovadores o un mayor rango. A pesar de tratarse de un criterio ampliamente adoptado, su aplicación es harto difícil debido a la multiplicidad de factores que pueden influir la decisión final y, por lo tanto, a la dificultad de justificar satisfactoriamente la inclusión o exclusión de una práctica en ese criterio[38].

Por si fuera poco, en 2008 la Comisión cambió su aproximación al análisis de la conducta de las dominantes. En sus Orientaciones sobre las prioridades de control respecto de las prácticas excluyentes[39], explicó que abandonaba la aproximación formal en favor de una basada en los efectos de las conductas, de modo que a partir de entonces iba a valorar el impacto económico del comportamiento analizado sobre la competencia existente en el mercado. El cambio implicaba negar que existieran prácticas que fueran por sí mismas abusivas; era necesario sopesar sus consecuencias, tanto positivas como negativas[40].

Por último, interesa recordar que la Comisión tiene la carga de probar que la conducta en cuestión es abusiva. A esos efectos, el Tribunal de Justicia ha explicado que debe demostrar que perjudica a los consumidores, dado que su bienestar es el fin último del Derecho de la competencia[41]. Con todo, no necesita acreditar expresamente este extremo, sino que le basta con evidenciar que la dominante ha socavado la estructura de la competencia existente en el mercado a través de medios diferentes a los que corresponde a una competencia en méritos. Pero, incluso en esta situación, la dominante puede probar la existencia de justificaciones objetivas. Se exonera de responsabilidad si acredita que la conducta era necesaria o que sus efectos positivos neutralizaban los daños a la estructura del mercado o al bienestar de los consumidores. Cabe añadir que la Comisión no tiene que demostrar que los perjuicios son reales, sino basta con probar que la práctica potencialmente podía perjudicar la competencia.

38. OCDE, 2006, 2/7. También, Van de Gronden y Rusu, 2021, 128 s.

39. *Supra* nota 2. El 28 de marzo de 2023 la Comisión modificó las Orientaciones para explicar su práctica actual. Introdujo cambios debido a la experiencia que había ido adquiriendo, para ajustarse la evolución de los mercados y para adaptarse a la doctrina del Tribunal de Justicia. Al respecto, McCallum *et al.*, 2023, 2/8 y Raedts, 2023, quien sugiere que es la respuesta a las derrotas que la Comisión ha sufrido en casos tan importantes como *Qualcomm* e *Intel*.

40. En la sentencia de 6.9.2017, *Intel / Comisión* (C-413/14P), ECLI:EU:C:2017:632, el Tribunal de Justicia reprochó al Tribunal General ser demasiado formalista por considerar que los pagos exclusivos eran *per se* abusivos. Según el primero, si la empresa enjuiciada probaba que había habido eficiencias o que su comportamiento estaba objetivamente justificado, la Comisión debía demostrar que la conducta era abusiva. Como el Tribunal General no había valorado todas las alegaciones de Intel, anuló la sentencia.

41. STJUE de 12.3.2022, *Servicio Elettrico Nazionale y otros* (C-377/20), ECLI:EU:C:2022:379, párrs. 44 ss. En el mismo sentido, sentencia *TeliaSonera* (nota 36), párr. 24.

5.2. Deberes de los guardianes de acceso

5.2.1. Obligaciones y prohibiciones de los artículos 5, 6 y 7

El Reglamento de Mercados Digitales se diferencia del artículo 102 TFUE en que impone un control preventivo y no represivo[42]. En efecto, los artículos 5, 6, 7, 14 y 15 establecen los deberes, bien positivos bien negativos, que deben cumplir los guardianes de acceso por el mero de haber sido designados. Buena parte de los previstos en los tres primeros preceptos provienen de casos de abuso de posición de dominio. Es decir, tienen su origen en expedientes en que la Comisión ha considerado que las prácticas incumplían el artículo 102, de ahí que las prohibiera o que aceptara el compromiso de la empresa implicada de no volver a llevarlas a cabo. Sin embargo, esas decisiones todavía no son firmes, pues la dominante ha recurrido la Decisión o bien se han cerrado con un compromiso[43]. Es el caso, por ejemplo, de la prohibición de autopreferencia prevista en el artículo 6.5 del Reglamento de Mercados Digitales. Deriva del caso *Google Search Shopping*, que fue objeto de la Decisión de la Comisión de 27 de junio de 2017. El Tribunal General confirmó su validez en la sentencia de 10.11.2021 (T-612/17). Pero la propietaria del motor de búsqueda más popular ha recurrido ante el Tribunal de Justicia. Aunque es probable que este órgano confirme la resolución de la primera instancia, no sería la primera vez que la anula bien por cuestiones de fondo bien por razones de forma[44]. Si así sucediera, la legitimación del art. 6.5 generaría dudas. No obstante, a nuestro modesto entender, los deberes de los artículos 5 a 7 son lícitos puesto que su objetivo es la disputabilidad y equidad de los sectores digitales y no castigar la explotación abusiva de un gran poder económico[45].

Los deberes previstos en los artículos 5, 6 y 7 presentan un diverso grado de concreción y eficacia. Los de los dos primeros preceptos tienen carácter general y heterogéneo. Los del artículo 7 persiguen la interoperatiblidad de los servicios de comunicaciones interpersonales independientes de la numeración. Todos ellos presentan carácter automático (*auto-executive*): los guardianes de acceso deben cumplirlos respecto de cada servicio básico de plataforma a partir de los

42. Coincidimos con Lamadrid y Bayón (2021, 585) y Franck y Peitz (2024, 308) en que este cambio libera a la Comisión de la carga de probar la abusividad de la conducta del guardián de acceso y de tomar en consideración sus eficiencias. En cuanto a la diferencia entre el control preventivo y represivo, Geradin (2021, 7/20) lo resume muy bien cuando explica que la aplicación del artículo 102 acostumbra a ir referida a casos en que la exclusión de los competidores lleva a la explotación de los consumidores. En cambio, el problema de los guardianes de acceso es que la explotación de los consumidores conduce a la exclusión de posibles rivales.

La doctrina critica la sistematización y concordancia de los deberes previstos en los arts. 5 a 7. Véase De Streel, Fearsey, Kraemer y Monti, 2021, 43 ss.; Monti, 2021, 2; Podszun, Bongartz y Langenstein, 2021, 4; Budzinski y Mendelsohn, 2021, 12 ss. y 22 ss.; Massa, 2022, 123.

43. En sentido similar, Larouche y De Streel, 2021, 548.

44. También Lamadrid y Bayón, 2021, 585.

45. Ibáñez, 2021, 568.

seis meses de su designación (*cfr.* art. 3.10)[46]. El art. 8.1 les exige que adopten las medidas necesarias al respecto, que además deberán ser conformes con la legislación sobre protección de datos y la intimidad en el sector de las telecomunicaciones, sobre seguridad cibernética, protección de los consumidores y sobre seguridad de los productos[47]. Además, deberán informar a la Guardiana de los Tratados acerca de las medidas que hayan adoptado para cumplir con los deberes que les competen. Por lo tanto, no es necesario que ésta demuestre que no se ajustan al modelo de competencia en méritos o que perjudican el bienestar del consumidor, ni que les conmine a ejecutarlas.

Ahora bien, a pesar de que las obligaciones y prohibiciones referidas son autoejecutables, la Comisión puede detallar las medidas que deben adoptar los guardianes de accesos para dar cumplimiento a las previstas en los artículos 6 y 7. El artículo 8 así lo dispone, estableciendo que, a esos efectos, podrá adoptar un acto de ejecución en un plazo de 6 meses a partir de la incoación del procedimiento. Igualmente, será necesario que las medidas impuestas por la Comisión vayan dirigidas a conseguir los objetivos impuestos por el Reglamento y que sean proporcionales a las circunstancias específicas del guardián de acceso, quien podrá solicitar participar en el procedimiento; sobre todo para convencer a la autoridad europea de la competencia de que las medidas que ha propuesto son suficientes. Sin embargo, la Comisión tiene la última palabra. El apartado 3 del artículo 8 le otorga discrecionalidad para decidir al respecto; eso sí, deberá respetar los principios de igualdad de trato, proporcionalidad y buena administración.

El artículo 13 complementa los arts. 5 a 7 al vetar las medidas antielusión. La prohibición tiene dos vertientes. La primera se refiere a la condición de guardián de acceso y significa que no son lícitas las medidas dirigidas a sortear los umbrales cuantitativos previstos en el artículo 3.2. La segunda tiene por objeto los deberes de los arts. 5 a 7[48]. El apartado 4 intenta ser lo más amplio posible al incluir dentro de la prohibición los aspectos contractuales, comerciales técnicos "o de cualquier otra naturaleza".

La Comisión puede dejar sin efecto las obligaciones y prohibiciones referidas en dos casos. El primero es cuando su cumplimiento pone en duda la viabilidad económica del guardián de acceso en la Unión Europea[49]. El art. 9 permite a la Comisión suspender total o parcialmente el cumplimiento de un deber específico de los arts. 5 a 7. Para ello es necesario que la causa de la amenaza a la viabilidad económica de la empresa sea una circunstancia excepcional que escape al control del guardián de acceso. Igualmente, basta con que la crisis afecte

46. Komninos, 2022, 3/8.

47. Barczentewicz (2024) advierte que cumplir los deberes de los artículos 5 a 7 puede generar problemas de seguridad y privacidad.

48. Al respecto, Franck y Peitz, 2024, 299 ss.

49. El Tribunal General considera que es lo que Bytedance Ltd debería haber hecho en relación con las letras b) y c) del art. 5.2, en lugar de solicitar medidas cautelares relativas a la anulación de su designación como guardián de acceso. Véase *supra* nota 32.

a la pervivencia de la empresa en cuestión en la Unión Europea, aunque pueda seguir existiendo fuera de ella. El apartado 1 del precepto citado se refiere a "una obligación específica"; por lo tanto, no está previsto para todos los deberes y prohibiciones impuestos a un guardián de acceso, sino que la Comisión deberá indicar a cuál priva de eficacia. En particular, deberá tratarse de aquél o aquélla que ponga en riesgo la viabilidad económica del guardián de acceso. A pesar de que la norma se refiere a una obligación o prohibición, su finalidad permite interpretar que podrán ser varias. Interesa subrayar el carácter excepcional de la medida. Se trata de suspender la obligación de cumplir alguno de los deberes relacionados con un servicio básico de plataforma de un guardián de acceso. La Comisión deberá fijar su duración y alcance, pudiendo además imponer condiciones para su disfrute. Revisará su decisión al cabo de un año, salvo que haya fijado un plazo menor.

El artículo 10 contempla el segundo supuesto: motivos de salud pública o seguridad pública. Bien debido a una petición motivada, bien *motu proprio*, el Ejecutivo comunitario puede adoptar un acto de ejecución en el que exima a un guardián de acceso de cumplir un deber relativo a un servicio básico de plataforma. No se prevé que deba especificar la duración de la exención ni que pueda someterla a condiciones, lo que diferencia este supuesto del anterior. Ahora bien, deberá estar pendiente de esta medida y revisarla anualmente, o antes si desaparece el motivo de exención.

Interesa subrayar que el Reglamento de Mercados Digitales no permite excluir la obligación de cumplir con los artículos 5 a 7 en virtud de las eficiencias de las conductas de los guardianes de acceso, lo que constituye una diferencia importante con el artículo 102 TFUE. En efecto, al aplicar esta disposición, la Comisión debe tomar en consideración tanto los efectos positivos como los negativos de la práctica analizada. Y no podrá imponer remedio ni sanción alguno, si los primeros superan a los segundos. En cambio, las posibles eficiencias de las conductas de los guardianes de acceso no eximen del cumplimiento de los deberes que comporta su designación[50].

5.2.2. Concentraciones y técnicas de elaboración de perfiles

El Capítulo III impone dos deberes más a los guardianes de acceso. El artículo 14 les exige informar a la Comisión acerca de todas las concentraciones que deseen llevar a cabo. La finalidad es que las autoridades de la competencia tengan conocimiento de estas operaciones para poder prohibirlas si tienen consecuencias perjudiciales para la competencia y la economía. Y es que las grandes empresas recurren a ellas para conseguir activos claves para el futuro, impedir

50. Podszun, 2023, 8 y Komninos, 2022, 2/8. Portuese (2022, 6 ss./24) se muestra muy crítico con los deberes impuestos por el Reglamento al considerar que desincentivan la innovación y la eficiencia competitiva, violan el principio de proporcionalidad y conculcan derechos fundamentales de los guardianes de acceso. En sentido parecido Díez Estella, 2023, 70.

una nueva tecnología o neutralizar un posible competidor que ponga fin a su reinado. De ahí que la institución europea comparta la información obtenida con las autoridades nacionales, que podrán tomar las medidas oportunas o remitir el control a la primera conforme al art. 22 del Reglamento Comunitario de Concentraciones. Ahora bien, el Reglamento de Mercados Digitales carece de ulteriores previsiones al respecto; es decir, no concede poder alguno a la Comisión en relación con estas operaciones. Solamente podrá intervenir cuando superen los umbrales previstos en los apartados 1 y 2 del artículo 1 del Reglamento Comunitario de Concentraciones o los organismos competentes de los Estados miembros le remitan el expediente[51].

La obligación de notificación de los guardianes de acceso aparece condicionada por dos parámetros. El primero es que se trate de una concentración. El artículo 3 del Reglamento Comunitario de Concentraciones la define como una toma de control externa con vocación de duración. Aunque se refiere a las fusiones, a la adquisición de acciones, participaciones u otros elementos del activo y a la creación de una empresa en participación, hay que interpretar esa definición en función del resultado de modo que comprenda todas las operaciones por las que una empresa pasa a controlar otra. La segunda condición es que la concentración afecte a los mercados digitales. El artículo 14 se refiere a negocios entre empresas que presten servicios básicos de plataforma, otros servicios en el sector digital, o simplemente permitan la recogida de datos. Ahora bien, no es necesario que la operación tenga dimensión "comunitaria". Es decir, el deber de comunicarla no aparece condicionado a que supere los umbrales previstos en los apartados 2 y 3 del artículo 1 del Reglamento Comunitario de Concentraciones.

La segunda obligación es el deber de informar a la Comisión sobre las técnicas de elaboración de perfiles de los consumidores que los guardianes de acceso utilicen al prestar servicios básicos de plataforma. El artículo 15 obliga a los últimos a proporcionar una descripción en el plazo de 6 meses de su designación, y además a publicar un resumen. Deberán actualizar tanto la información como el resumen al menos una vez al año. Interesa subrayar que la descripción de las técnicas de elaboración de perfiles deberá haber sido auditada por profesionales independientes. De ahí que el precepto tenga por título "obligación de auditoría".

6. AUTORIDAD COMPETENTE, PODERES Y SANCIONES

6.1. Competencia para aplicar el Reglamento

Una de las grandes diferencias entre el art. 102 TFUE y el Reglamento de Mercados Digitales reside en la competencia para aplicarlos, pues el primero

51. Caffara (2021) considera que la previsión es insuficiente ya que es precisamente el control de las concentraciones el punto débil de la lucha contra los gigantes tecnológicos.

sigue el modelo descentralizado y el último el centralizado. En efecto, tanto la Comisión Europea como las autoridades nacionales de la competencia, además de los jueces y tribunales de los veintisiete, están legitimados para valorar si una empresa ha abusado de su posición de dominio y, en el caso de las autoridades de la competencia, sancionarla por ello. Es más, cuando conozcan de un caso que caiga dentro del radio de eficacia del artículo 102, los órganos nacionales deberán aplicarlo juntamente con la legislación interna, que podrá ser más exigente (artículo 3 del Reglamento 1/2003). En cambio, no tienen competencia para aplicar el Reglamento de Mercados Digitales. El articulado de éste otorga los poderes de investigación y sanción a la Comisión en exclusiva, dado que las grandes tecnológicas no operan de forma aislada en los Estados miembros, sino que su estrategia es global[52]. Ahora bien, contiene diversas medidas para paliar los riesgos que esta situación entraña.

De un lado, el Reglamento crea dos órganos que asisten a la Comisión. El primero es el Grupo de Alto Nivel, que está compuesto por representantes de reguladores y supervisores sectoriales además de la Red Europea de Competencia. El segundo es el Comité Consultivo sobre Mercados Digitales. De otro lado, los artículos 37 ss. regulan la cooperación de la Comisión con las autoridades nacionales de los Estados miembros en general, y en particular con las encargadas de aplicar las normas de la competencia, así como con los órganos jurisdiccionales[53]. De ahí que se haya afirmado que la Comisión podrá apoyarse en todas ellas a efectos de investigación[54].

Los tribunales nacionales de los Estados miembros también pueden aplicar el Reglamento, como hemos visto (*supra* § 2). De ahí que tenga gran importancia el artículo 39, que les permite pedir al Ejecutivo comunitario información sobre cuestiones relativas a la eficacia de la norma. Igualmente, obliga a los Estados miembros a remitirle una copia de las sentencias nacionales que la apliquen. También le habilita a formular observaciones escritas u orales cuando sea necesario para asegurar la coherencia en su aplicación. Por último, prohíbe a los órganos jurisdiccionales nacionales adoptar resoluciones que sean contrarias a una decisión adoptada por la Comisión en este ámbito.

52. Bueso, 2023, 96 s. Respecto de las ventajas y desventajas de la centralización, Larouche y De Streel, 2021, 558; Budzinski y Mendelsohn, 2021, 21. A favor de la centralización, Monti, 2021, 4 s.

53. Interesa destacar que cuando una autoridad nacional desee iniciar un procedimiento contra un guardián de acceso en virtud de su Derecho de la competencia (art. 1.6 del Reglamento de Mercados Digitales), deberá informar por escrito acerca de su primera medida de investigación (art. 38.3). Igualmente, la información intercambiada sólo se utilizará para coordinar la ejecución del Reglamento y de las normas de la competencia nacionales. Quedan excluidas, por tanto, otras normas reglamentarias sectoriales —tanto nacionales como europeas.

54. Ruiz Peris, 2023, 26/37

6.2. Poderes de investigación

El régimen de los procedimientos y de la sanción guarda parecido, aunque el Reglamento de Mercados Digitales es más expeditivo (plazos más breves y posibilidad de sanciones más altas)[55]. Su Capítulo IV faculta a la Comisión para realizar investigaciones de mercado con tres finalidades diferentes. La primera es la designación de guardianes de acceso y sus servicios básicos de plataforma. Ahora bien, no se trata de la designación ordinaria, sino de dos supuestos especiales: la atribución de esa condición cuando la empresa no supera los umbrales previstos en el art. 3.2 pero reúne las características del apartado 1, y su negación pese a superarlos. La segunda investigación está destinada a evaluar si un guardián de acceso ha incumplido sistemáticamente sus deberes (art. 18). Y la tercera a decidir la actualización de los servicios básicos de plataforma enumerados en el art. 2.2 o identificar nuevas prácticas perniciosas a combatir —por ejemplo, añadiendo nuevas obligaciones y prohibiciones en los arts. 5 a 7[56]. Su resultado será una propuesta legislativa que podrá consistir en modificar el Reglamento o adoptar un acto delegado que lo complemente. Por otra parte, el Reglamento contempla tres procedimientos que la Comisión puede incoar para determinar si las medidas propuestas por un guardián de acceso para cumplir sus deberes son adecuados, para sancionar su incumplimiento y para imponer una multa coercitiva para forzar al guardián de acceso a cumplir las obligaciones del artículo 31.1.

Los poderes de investigación son muy similares a los que detenta la Comisión en virtud del Reglamento 1/2003. Por ejemplo, puede exigir a las empresas y asociaciones de empresas que le proporcionen información —incluidos datos y algoritmos—, tomar declaraciones, realizar entrevistas e inspecciones —dentro de las cuales se halla la posibilidad de exigir acceso y explicaciones sobre el funcionamiento del sistema informático y algoritmos—, así como adoptar medidas cautelares para tutelar a los usuarios profesionales y finales en caso de urgencia y cuando considere que *prima facie* la plataforma ha incumplido sus obligaciones. Asimismo, deberá adoptar las medidas necesarias para controlar que los guardianes de acceso realizan sus deberes y convertir en obligatorios los compromisos propuestos para poner fin a un presunto incumplimiento y garantizar el respeto de los arts. 5 a 7 (art. 25 y 26).

La principal diferencia con el Reglamento 1/2003 es la mayor brevedad de los plazos del Reglamento de Mercados Digitales. Resulta significativo el contraste que existe respecto del tiempo para tramitar un procedimiento por incumplimiento. La primera norma no establece ningún término, lo que deriva en expedientes extremadamente largos. Por ejemplo, la Comisión necesitó 77 meses para instruir el caso *Google Search Shopping*, 32 para *Google Search* y 25 para *Google*

55. Respecto de los mecanismos para la aplicación efectiva del Reglamento de Mercados Digitales, Bueso, 2023, 92 ss.

56. Podszun, Bongartz y Langenstein, 2021, 7.

Android[57]. En cambio, el art. 29 del Reglamento de Mercados Digitales fija un máximo de 12 meses para determinar el incumplimiento de las obligaciones previstas en los artículos 5 a 7.

La mayor brevedad de los procedimientos representa, sin duda, un avance importante respecto del régimen del abuso de posición de dominio[58]. Pero conlleva dos riesgos mayúsculos. El primero es que la calidad de los actos jurídicos puede deteriorarse, pues la Guardiana de los Tratados no tendrá mucho tiempo para adoptarlos ni revisarlos. El segundo es que los derechos de defensa de los guardianes de acceso queden lesionados[59]. Es cierto que el Reglamento de los Mercados Digitales reconoce expresamente los derechos a ser oído (art. 34.1 a .3) y de acceso al expediente (art. 34.4). Ahora bien, la referencia a ellos no agota sus poderes de defensa; entre otras razones porque el Reglamento de Mercados Digitales entra dentro del "marco del Derecho comunitario", con lo que se aplica la Carta de Derechos Fundamentales de la Unión Europea. Consecuentemente, los guardianes de acceso tienen los derechos y libertades reconocidos en ella[60].

De otro lado, el Reglamento de Mercados Digitales exige a los guardianes de acceso que nombren "agentes de cumplimiento" que se encarguen de hacer cumplir a su empresa los deberes que derivan de esa norma y las medidas impuestas por la Comisión. El art. 28 demanda que se trate de "… un alto directivo independiente con responsabilidad específica por lo que respecta a dicha función de comprobación". No existe una previsión similar en el Reglamento 1/2003, si bien pudiera tener cabida en su artículo 7.

6.3. Remedios y sanciones

Los regímenes sancionadores de los Reglamentos 1/2003 y 2022/1925 también son similares. Cabe recordar que el artículo 7 del primero permite a la Comisión imponer cualquier remedio estructural o de comportamiento que sea necesario y adecuado para poner fin efectivo a la infracción y que los artículos 23 y 24 establecen las multas sancionadoras y coercitivas. En la práctica, lo más habitual es exigir a la dominante que cese en la conducta infractora, prohibirle que la repita en el futuro e imponerle una multa, cuyo límite es el diez por ciento del volumen de negocios total realizado en el ejercicio anterior (art. 23.2).

El Reglamento de Mercados Digitales dedica a estas cuestiones los artículos 29 a 33. El primero de ellos establece los incumplimientos que pueden ser objeto de sanción y dispone que la Comisión ordenará al guardián de acceso cesar en la infracción y explicar las medidas que adoptará para cumplir esa decisión.

57. Witt, 2023, 629.
58. En sentido contrario Podszun, Bongartz y Langenstein, 2021, 9.
59. Podszun, 2023, 10.
60. Mangas, 2008, 820 y Aguilar, 2018, 980 ss.

El artículo 30 tiene por objeto las multas sancionadoras, que sólo podrán imponerse cuando el incumplimiento sea intencionado o negligente. A imagen del Reglamento 1/2003, fija un límite del diez por ciento del volumen de negocios total a nivel mundial del ejercicio anterior; pero lo eleva al veinte por ciento cuando el guardián de acceso haya cometido la misma infracción u otra similar en relación con el mismo servicio básico de plataforma durante los ocho años anteriores. El apartado 4 establece los elementos que la Comisión deberá tener en cuenta al graduar las multas: gravedad, duración, reiteración y, respecto del último tipo de sanciones, la demora causada al procedimiento. El art. 31 prevé la posibilidad de adoptar multas coercitivas para obligar a los guardianes de acceso, a las empresas y a las asociaciones de empresas a cumplir las obligaciones impuestas. Estas multas no podrán exceder del 5% del promedio diario del volumen de negocios a nivel mundial en el ejercicio anterior. Por último, la Comisión dispone de un plazo de 5 años de prescripción para imponer las sanciones (art. 32). Se cuenta desde el momento en que se cometió la infracción; pero en caso de que sea continúa o reiterada, el cómputo empieza en el momento del cese de la infracción. Y el mismo plazo rige para hacer cumplir las sanciones impuestas, empezando el cómputo el día en que la decisión deviene definitiva (art. 33).

El Reglamento de Mercados Digitales establece soluciones específicas para el incumplimiento sistemático de las obligaciones previstas en los artículos 5 a 7. Es decir, cuando se hayan adoptado, al menos, tres decisiones de incumplimiento *ex* art. 29 dentro de los ochos años anteriores a la adopción de la decisión de apertura de esta investigación. El art. 18 permite a la Comisión adoptar medidas correctoras, que podrán ser tanto estructurales como de comportamiento[61]. Eso sí, deberán ser proporcionadas y necesarias para garantizar el cumplimiento efectivo de la norma. El apartado 2 del artículo 18 pone como ejemplo la prohibición de tomar parte en concentraciones relacionadas con el sector digital y la Comisión ha aludido a la desinversión de ciertos negocios[62]. Estos remedios no son inmutables; al contrario, deberán ser revisados periódicamente para comprobar si todavía son eficaces y necesarios.

A pesar de las diferencias existentes, lo más probable es que los remedios y sanciones que se impongan conforme al Reglamento de los Mercados Digitales sean los mismos que los que la Comisión adopta en virtud del Reglamento 1/2003. Primero, parece difícil que un mismo órgano instructor y sancionador varíe su política sancionadora al estar aplicando una norma diferente cuando su contenido es parecido a otra. Segundo, el hecho de que el Reglamento de los Mercados Digitales no prevea la posibilidad de adoptar medidas estructurales —salvo en caso de incumplimiento sistemático— no va a suponer cambio algu-

61. Buzinski y Mendelsohn (2021, 10) critican la falta de precisión de los remedios establecidos para el incumplimiento sistemático. Y Larouche y De Streel (2021, 553) que no se haya aprovechado la ocasión para otorgar a la Comisión la posibilidad de adoptar los remedios propios de la regulación en lugar de los típicos del Derecho de la competencia.

62. Comisión Europea, 2020a.

no respecto de su política anterior, puesto que la autoridad europea de la competencia no ha adoptado nunca este tipo de medidas en relación con el art. 102[63]. Y tercero, tampoco parece que la elevación del límite sancionador del 10% al 20% del volumen de negocios del autor de la infracción vaya a constituir una novedad, pues las multas que acostumbran a imponerse por infringir el artículo 102 TFUE suelen quedarse muy lejos de ese umbral.

7. CONCLUSIONES

1. El Reglamento de Mercados Digitales ha sido creado para conseguir que exista disputabilidad y equidad en el sector digital debido a que el artículo 102 TFUE se ha mostrado insuficiente para luchar contra los abusos de las grandes tecnológicas. Las principales razones han sido la extraordinaria dilación del procedimiento, el aprovechamiento en las oportunidades de defensa que ofrece el Derecho de la Unión y la insuficiencia de los remedios y sanciones aplicados a empresas con tanto poder económico.

2. El ámbito de aplicación del Reglamento de Mercados Digitales es muy reducido pues se ciñe a los servicios básicos de plataforma que prestan los guardianes de acceso a consumidores domiciliados en la Unión. No se espera que muchas empresas reciban la consideración de guardián de acceso, lo que facilitará el trabajo de la Comisión.

3. La designación de los guardianes de acceso es mucho más fácil que la determinación de una posición de dominio. Esencialmente se basa en criterios cuantitativos: la superación de los umbrales previstos en el artículo 3.2 genera la presunción de que la empresa en cuestión cumple los requisitos previstos en el artículo 3.1. Además ella deberá informar a la Comisión de que supera esos umbrales.

4. Otro cambio crucial es sustituir el control represivo por uno preventivo. La Comisión no necesitará demostrar que una determinada práctica es contraria a las exigencias de la competencia en méritos y que sus efectos negativos superan los positivos. Con el nuevo sistema, los guardianes de acceso deberán cumplir las obligaciones y prohibiciones previstas en el Reglamento por el mero hecho de haber sido designados, sin que la prueba de la justificación de su conducta o de sus eficiencias les exonere de responsabilidad.

5. Respecto de los procedimientos, remedios y sanciones, destaca la centralización de la aplicación del Reglamento de Mercados Digitales en la Comisión, la brevedad de los plazos, la posibilidad de doblar las sanciones que se pueden imponer y la ausencia de medidas estructurales, salvo en el caso de los incumplimientos sistemáticos. Con todo, estos aspectos pueden tener un lado oscuro. La centralización del poder puede resultar peligrosa si no conlleva el aumento de recursos de que dispone la Comisión para luchar contra las grandes tecnoló-

63. Comisión Europea, 2020b, párr. 172.

gicas. No obstante, las exigencias que comporta la aplicación del Reglamento de Mercados Digitales parecen mínimas debido a la reducción del ámbito de aplicación, al sistema de designación de los guardianes de acceso y a la sustitución del control *ex post* por uno *ex ante*. La brevedad de los plazos determina que los procedimientos sean más expeditivos; pero comprometerá la rigurosidad en la actuación de la Comisión y el respeto de los derechos de los guardianes de acceso, lo que puede constituir un arma defensiva muy poderosa. La posibilidad de duplicar el montante de las sanciones no parece eficaz puesto que las multas que actualmente impone la Comisión distan mucho de llegar a los máximos posibles. Y en cuanto a la escasa importancia otorgada a los remedios estructurales, resulta lógica si tenemos en cuenta que la propia finalidad del Reglamento, y sobre todo de los deberes previstos en los artículos 5 a 7, es conseguir que exista competencia leal en los mercados digitales.

6. Si bien la valoración global del Reglamento es positiva y debe aplaudirse la valentía de la Comisión de continuar luchando contra los gigantes digitales, existen tres aspectos mejorables. El primero es la ausencia de medidas más contundentes para controlar las concentraciones. El segundo es no haber regulado la aplicación privada del Reglamento de Mercados Digitales. A pesar de que tiene efectos directos, hubiera sido deseable que se hubiera incluido dentro del radio de eficacia de la Directiva de Daños[64]. Y el tercero es el garantismo consustancial al Derecho de la Unión Europea. Aunque su sistema de derechos fundamentales es encomiable, las grandes empresas se aprovechan del mismo para minar la eficacia del Derecho de la competencia y de las normas complementarias. Ninguna duda cabe de que la solución es harto compleja, por lo que quizás sea más realista pedir la ampliación de los recursos y activos de que disponen las autoridades de la competencia.

BIBLIOGRAFÍA

AGUILAR, A. (2018). La aplicación nacional de la Carta de Derechos Fundamentales de la UE: una simple herramienta de interpretación de la eficacia de las directivas. *Revista de Derecho Comunitario Europeo, 61*, 973-1011.

ANDRIYCHUK, O. (2021). Shaping the New Modality of the Digital Markets: The Impact of the DSA/DMA Proposal on Inter-Platform Competition, *World Competition*, 44 (3).

BAKER, J.B. (2019). *Antitrust Paradigm: Restoring a Competitive Economy.* Harvard University Press.

64. Directiva 2014/104/UE del Parlamento Europeo y del Consejo, de 26 de noviembre de 2014, relativa a determinadas normas por las que se rigen las acciones por daños en virtud del Derecho nacional, por infracciones del Derecho de la competencia de los Estados miembros y de la Unión Europea.

BARCZENTEWICZ, M. (2024). *Does the DMA Let Gatekeepers Protect Data Privacy and Security?* . Disponible en https://truthonthemarket.com/2024/04/04/does-the-dma-let-gatekeepers-protect-data-privacy-and-security/.

BEEMS, B. (2023). The DMA in broader regulatory landscape of the EU: an institutional perspective. *European Competition Journal, 19*(1), 1-29. https://doi.org/10.1080/17441056.2022.2129766.

BOTTA, M. (2021). Sector Regulation of Digital Platforms in Europe: Uno, Nessuno e Centomila. *Journal of European Competition Law & Practice, 12* (7), 500-512.

BUDZINSKI, O. y MENDELSOHN, J. (2021). Regulating Big Tech: From Competition Policy to Sector Regulation?. *Ilmenau Economics Discussion Papers, 27* (154), 36 páginas. https://dx.doi.org/10.2139/ssrn.3938167.

BUESO GUILLÉN, P.J. (2023). Mecanismos de aplicación del Reglamento de Mercados Digitales, su aplicación privada y responsabilidad civil de los guardianes de acceso: una primera aproximación. En E. Hernández Sainz, L.C Mate Satué y M.T. Alonso Pérez (dir.). *La responsabilidad civil por servicios de intermediación prestados por plataformas digitales* (81-110). A Coruña: Colex.

CABRAL, L.; HAUCAP, J.; PARKER, G; PETROPOULOS, G.; VALLETTI, T y VAN ALSTYNE, M (2021). *The EU Digital Markets Act: A Report form a Panel of Economic Experts*. Publications Office of the European Union.

CAFFARRA, C. (2021). *What are we regulating for?*. Disponible en https://cepr.org/voxeu/blogs-and-reviews/what-are-we-regulating.

CAPPAI, M. y Colangelo, G. (2023). A unified test for the European *ne bis in idem* principle: the case study of digital market regulation, *Common Market Law Review*, 60(2), 431-455.

Comisión Europea (2020a). *Europe fit for the Digital Age: Commission proposes new rules for digital platforms*. Disponible en https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347.

Comisión Europea (2020b). *DMA Impact Assessment Report. Part 1/2*. SWD(2020) 363 final

Competition and Markets Authority (2020). *A new pro-competition regime for digital markets. Advice of the Digital Markets Taskforce.*

CRÉMER, J.; DE MONTJOYE, Y.-A y SCHWEITZER, H. (2019). *Competition policy for the digital era*. European Commission, Directorate-General for Competition.

DE STREEL, A., FEASEY, R., KRAEMER, J., MONTI, G. (2021). Making the Digital Markets Act More Resilient and Effective. *CERRE Recommendations Paper*. https://dx.doi.org/10.2139/ssrn.3853991.

DÍEZ ESTELLA, F. (2021). El abuso de dominio por las plataformas digitales: Google en el banquillo. En J. Martí (dir.). *Competencia en mercados digitales y sectores regulados*. Tirant lo Blanch.

DÍEZ ESTELLA, F. (2023). La DMA: ¿un nuevo Reglamento para —o contra— los mercados digitales en la UE?. En E. Hernández Sainz, L.C Mate Satué y

M.T. Alonso Pérez (dir.). *La responsabilidad civil por servicios de intermediación prestados por plataformas digitales* (51-79). A Coruña: Colex.

EBEN, M. (2024). The New Market Definition Notice: Embracing Change. Disponible en https://competitionlawblog.kluwercompetitionlaw.com/2024/02/28/the-new-market-definition-notice-embracing-change/.

EZRACHI, A. (2014). *EU Competition Law. An Analytical Guide to the Leading* Cases (4 ed.). Oxford y Portland: Hart Publishing.

EZRACHI A y ROBERTSON, V (2019). Competition, Market Power and Third-Party Tracking. *World Competition*, 42(2).

Federal Ministry for Economic Affairs and Energy (2019). *A new competition framework for the digital economy. Report by the Commission 'Competition Law 4.0'*

FRANCK, J. U. y Peitz, M. (2024). *The Digital Markets Act and the Whack-A-Mole Challenge. Common Market Law Review, 61, 299-344.*

FURMAN, J. (2019). *Unlocking digital competition. Report of the Digital Competition Expert Panel.*

GERADIN, D. (2021). What is a Digital Gatekkeper? Which Platforms Should Be Captured by the EC Proposal for a Digital Market Act?. *SSRN*. Disponible en https://ssrn.com/abstract=3788152. https://dx.doi.org/10.2139/ssrn.3788152.

GÓRRIZ, C. (2024). Interpretació jurisprudencial del *ne bis in idem* i eficàcia del Dret de la competencia europeu. *Revista Catalana de Dret Públic*, en prensa.

HEIMANN, F. (2022). *The Digital Markets Act – We gonna catch 'em all?*. Disponible en https://competitionlawblog.kluwercompetitionlaw.com/2022/06/13/the-digital-markets-act-we-gonna-catch-em-all/.

HERRERO, C. (2021). Gigantismo empresarial en los mercados digitales. ¿Una vuelta a los orígenes y … nuevos desafíos. *Revista de Estudios Europeos, 78*.

IBÁÑEZ COLOMO, P. (2021). The Draft Digital Markets Act: A leal and Institutional Analysis. *Journal of European Competition Law & Practice, 12(7)*, 561-575.

KERBER, W. (2021). Taming Tech Giants with a Per-Se Rules Approach? The Digital Markets Act from the 'Rules vs. Standard' Perspective (June 7, 2021). *Concurrences, 3*, 28-34.

KHAN, L. (2017). Amazon's Antitrust Paradox. *The Yale Law Journal*, 126

KOMNINOS, A. (2022). The Digital Markets Act: How Does it Compare with Competition Law?. *SSRN*. https://dx.doi.org/10.2139/ssrn.4136146.

LAMADRID DE PABLO, A. y BAYÓN FERNÁNDEZ, N. (2021). *Why the Proposed DMA Might Be Illegal under Article 114 TFEU, and how to fix it. Journal of European Competition Law & Practice, 12(7)*, 576-589. https://doi.org/10.1093/jeclap/lpab059.

LAROUCHE, P. y DE STREEL, A. (2021). The European Digital Markets Act: A Revolution Grounded on Traditions. *Journal of European Competition Law & Practice* 12(7), 542-560.

MANGAS, A. (2008). Artículo 51. Ámbito de aplicación. En A. Mangas (dir.). *Carta de los derechos fundamentales de la Unión Europea. Comentario artículo por artículo* (809-825). Bilbao: Fundación BBVA.

MASSA, C. (2022). The Digital Markets Act between the EU Economic Constitutionalism and the EU Competition Policy. *Yearbook of Antitrust and Regulatory Studies, 15*, 103-130. https://doi.org/10.7172/1689-9024.YARS.2022.15.26.5.

MCCALLUM, L., BERNAERTS, I., KADAR, M., HOLZWARTH, J., KOVO, D., LAGRUE, M., PEREIRA ALVES, I., LEDUC, E., MANIGRASSI, L., MARCOS RAMOS, J., POZZATO, V., STAMOU, P. (2023). A dynamic and workable effects-based approach to abuse of dominance. *Competition Policy Brief, 1*.

MONTI, G. (2008). Managing the Intersection of Utilities Regulation and EC Competition Law. *The Competition Law Review, 4*(2), 123-145.

MONTI, G. (2021). *The Digital Markets Act – Institutional Design and Suggestion for Improvement*. TILEC Discussion paper No. 2021-04. https://dx.doi.org/10.2139/ssrn.3797730.

O'DONOGHUE, R., PADILLA, J. (2020). *The law and economics of article 102 TFEU* (3ª ed.). Bloomsbury Publishing.

Organización para la Cooperación y el Desarrollo Económicos. (2006). *What is Competition on the Merits?*. Disponible en https://www.oecd.org/competition/mergers/37082099.pdf.

PETIT, N. (2021). The Proposed Digital Markets Act (DMA): A Legal and Policy Review. *SSRN* https://ssrn.com/abstract=3843497.

PODSZUN, R., BONGARTZ, P., LANGENSTEIN, S. (2021). Proposals on How to Improve the Digital Markets Act. *SSRN*. Disponible en https://ssrn.com/abstract=3788571. https://dx.doi.org/10.2139/ssrn.3788571.

PODSZUN, R. (2023). *From competition law to Platform Regulation – Regulatory choices for the digital markets act. Economics*, 17(1). doi:10.1515/econ-2022-0037.

PORTUESE, A. (2022). The Digital Markets Act: A Triumph of Regulation Over Innovation. *Information Technology & Innovation foundation*. https://itif.org/publications/2022/08/24/digital-markets-act-a-triumph-of-regulation-over-innovation/.

RAEDTS, E. (2023). *Guidelines vs Guidance: exclusionary abuse Guidelines due by 2025*. Disponible en https://www.stibbe.com/publications-and-insights/guidelines-vs-guidance-exclusionary-abuse-guidelines-due-by-2025.

RIBERA MARTÍNEZ, A. (2023). An inverse analysis of the digital markets act: applying the Ne bis in idem principle to enforcement. *European Competition Journal, 19*(1), 86-115. https://doi.org/10.1080/17441056.2022.215672.

RUIZ PERIS, J. I. (2023). El Reglamento de mercados digitales (Reglamento (UE) 2022/1925) y la acción de las Autoridades nacionales de competencia (ANCs) de los Estados miembros. *Revista de Derecho de la Competencia y la Distribución, 33*, 37 páginas.

SCHWEITZER, H (2021). The art to make gatekeeper positions contestable and the challenge to know what is fair: A discussion of the Digital Market Act Proposal. *SSRN*. https://ssrn.com/abstract=3837341.

Stigler Center for the Study of the Economy and the State (2019). *Stigler Committee on Digital Platforms. Final Report.*

TIROLE, J (2018). *La economía del bien común.* Debolsillo.

VAN DE GRONDEN, J., Rusu, C. (2021). *Competition Law in the EU. Principles, substance, enforcement*. Cheltenham y Northampton: Elgar.

VAN DEN BOOM, J. (2023). What does the Digital Markets Act harmonize? – Exploring interactions between the DMA and national competition laws. *European Competition Journal*, 19(1), 57-85.

VILÀ COSTA, B. (2022). The new Digital Markets Act and Services Market Act and its Relevance on EU Legal Harmonization: A Methodological, Holistic Introductory Approach. *Evrigenis Yearkook of International and European Law (EvrYIEL), 4*, 209-219.

WITT, A. (2023). The Digital Markets Act – Regulating the Wild West. *Common Market Law Review, 60*, 625-666.

WU, T. (2018). *The curse of bigness: Antitrust in the new gilded age*. Columbia Global Reports, New York.

II. Empresa y actividad

BENEFICIOS FISCALES POR LA REALIZACIÓN DE ACTIVIDADES DE I+D+i PARA LAS PERSONAS FÍSICAS

Zuley Fernández Caballero
Profesora lectora de Derecho Financiero y Tributario
Universidad Autónoma de Barcelona

ABSTRACT:
Public aid to boost research, development, and technological innovation (R&D&I) activities is structured through fiscal and parafiscal instruments. Spain has implemented various tax measures for several years that benefit the performance of such activities. In this study, we analyze the current tax incentives for conducting research, development, and technological innovation activities and their effectiveness in encouraging individuals to engage in these activities.

Keywords: R&D&I activities, tax benefits, direct taxation.

Palabras clave: actividades I+D+i, beneficios fiscales, imposición directa.

SUMARIO:

exentas; 3. Instrumento para el impulso de actividades I+D+I alternativo al fiscal; 4. Consideraciones finales.

1. INTRODUCCIÓN

"Las políticas de ciencia, tecnología e innovación constituyen un elemento de primordial importancia en el desarrollo de las sociedades modernas ya que existe una relación entre la capacidad de generación de conocimiento y de innovar de un país y su competitividad y desarrollo económico y social"[1].

En este contexto, los sistemas de incentivos a la investigación, el desarrollo y la innovación tecnológica (I+D+i) se materializan a través de instrumentos fiscales y parafiscales. España tiene implementado desde hace varios años diferentes medidas tributarias que benefician la realización de actividades de I+D+i. Las ventajas fiscales que tienen una mayor connotación en nuestro ordenamiento tributario se encuentran en la imposición directa, concretamente, en el Impuesto de Sociedades (IS). En efecto, la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades (LIS) reconoce un régimen preferente para las actividades de investigación, desarrollo e innovación tecnológica. Por medio de esta norma se configuran beneficios tributarios por la realización de actividades de I+D+i que comprenden tanto a la base imponible como a la cuota tributaria[2].

De esta forma nos encontramos con un grupo de medidas que afecta directamente la determinación de la base imponible al estar formado por un conjunto de deducciones sobre aquella. Nos referimos a la libertad de amortización de los elementos del inmovilizado material e intangible en la parte que se hallen afectos a las actividades de investigación y desarrollo del artículo 12.3 b) de la LIS, a los gastos de investigación y desarrollo activados como inmovilizado intangible, excluidas las amortizaciones de los elementos que disfruten de libertad

1. QUIRÓS GÓMEZ, J. (2021:3). "Incentivos fiscales a la investigación, desarrollo e innovación tecnológica: los informes motivados", *Quincena Fiscal*, núm. 21. Disponible en: https://acortar.link/pT6FBW. Consultado 03/04/2024.

2. "*En el ámbito de la Unión Europea, se puede observar que los incentivos fiscales que están ligados a este tipo de actividades consisten en reducciones en la base imponible o bien en deducciones en la cuota, si bien se constata una tendencia a suprimir estas últimas en la mayoría de los países de la Unión Europea. También se percibe que, en ocasiones, se permite una amortización acelerada, mientras que, en otros casos, los países establecen medidas para el fomento de la contratación de investigadores altamente cualificados o bien algún tipo de incentivo para la inversión de horas de trabajo en actividades de I+D+I. Asimismo, existen otras fórmulas complementarias, como las deducciones por donativos para financiar estas actividades, la exención de las becas de investigación o los tratamientos especiales para las transferencias de tecnología entre sociedades de un mismo grupo*". DELGADO GARCÍA, A. M.; OLIVER CUELLO, R. (2008:59). "Nuevas tendencias en la política de fomento de las actividades de investigación, desarrollo e innovación tecnológica", *Crónica Tributaria,* núm. 128.

de amortización que podrán amortizarse libremente (artículo 12.3 c) de la LIS) y a la reducción de las rentas positivas procedentes de la cesión del derecho de uso o de explotación de patentes, modelos de utilidad, certificados complementarios de protección de medicamentos y de productos fitosanitarios, dibujos y modelos legalmente protegidos, que deriven de actividades de I+D+i prevista en el artículo 23 de la LIS. Por otro lado, el artículo 35 de la LIS regula una deducción en la cuota íntegra por la realización de actividades de I+D+i.

En principio, estos beneficios fiscales están pensados para ser aplicados por los sujetos pasivos del IS, principalmente, el mundo empresarial, sin embargo, las personas físicas también podrán ejercitar su derecho a aplicar las deducciones sobre la base y la cuota cuando se trate de contribuyentes del Impuesto sobre la Renta de las Personas Físicas (IRPF) que realicen actividades económicas. Y esto es así porque la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio dispone en su artículo 28 que el rendimiento neto de las actividades económicas realizadas por las personas físicas o las entidades a las que se refiere el artículo 35.4 de la Ley General Tributaria (LGT) se determinará aplicando las normas del IS y más adelante, en el artículo 68 apartado 2 de la misma ley establece que los contribuyentes que ejerzan actividades económicas les serán de aplicación los incentivos y estímulos a la inversión empresarial establecidos en el IS con igualdad de porcentajes y límites de deducción. Asimismo, el legislador exime de tributar en concepto de IRPF, si se cumplen con determinados requisitos: las becas públicas, las becas concedidas por las entidades sin fines lucrativos y las becas concedidas por las fundaciones bancarias percibidas para cursar estudios reglados, tanto en España como en el extranjero, en todos los niveles y grados del sistema educativo.

En este ámbito, se aprecia otro instrumento alternativo a los beneficios fiscales con el que se pretende también incentivar la realización de actividades de I+D+i, consistente en una bonificación sobre la cuota empresarial a la Seguridad Social por contingencias comunes de las empresas que contraten de manera indefinida a personal para el desempeño de actividades de investigación y desarrollo e innovación tecnológica. Esta medida se recoge en el Real Decreto 475/2014, de 13 de junio, sobre bonificaciones en la cotización a la Seguridad Social del personal investigado y es incompatible con las ventajas fiscales que acabamos de mencionar, excepto para aquellas entidades que dispongan del sello de "PYME Innovadora".

En definitiva, nos encontramos ante un conjunto potente de ayudas públicas para dar impulso a las actividades de investigación, desarrollo e innovación tecnológica que pueden ser aplicadas por cualquier persona que realice actividades económicas, pero que no está exento de polémica. Lo que se demuestra con la dificultad para identificar cuándo estamos frente a una actividad de investigación y desarrollo o una actividad de innovación tecnológica. Y es que a pesar de que la ley parece clara en relación con estas definiciones (asunto nada baladí si como veremos más adelante no les afectan los mismos beneficios y en aquellos

casos en que sí se puede aplicar iguales medidas los porcentajes de deducción son notoriamente diferentes según de qué actividad se trate), ciertas acepciones contenidas en la norma han creado indefinición jurídica, donde se utilizan en algunos casos conceptos jurídicos indeterminados. A lo que debemos adicionar que el legislador ha puesto a disposición de los contribuyentes ciertos instrumentos como el Informe Motivado que determinan si los esfuerzos técnicos y/o científicos de estos obligados se pueden calificar de I+D, iT o, quedan excluidos de estas definiciones, vinculante para la Administración tributaria, aunque como constataremos en el transcurso del trabajo se ha producido un cambio de criterio por parte del Tribunal, alejándose la jurisprudencia de la postura seguida hasta hace poco respecto a dichos informes.

A su vez, cuando se trate del contribuyente, persona física del IRPF con derecho a aplicar estos incentivos fiscales, el ejercicio de aquél estará condicionado a la determinación de la base imponible a través del método directo normal, que requiere la realización de un mayor número de gestiones y costes, no obstante, disponer estos sujetos de otras vías de cálculo del beneficio empresarial que implican un menor coste de gestión, principalmente, para aquellos pequeños empresarios individuales, aludimos a la estimación objetiva y la estimación directa simplificada.

Por lo cual, el presente estudio tiene como finalidad analizar los actuales beneficios fiscales que incentivan las actividades de investigación, desarrollo e innovación tecnológica y la suficiencia de éstos para promover que las personas físicas lleven a cabo dichas actividades.

2. VENTAJAS FISCALES A LA I+D+i

El actual régimen de beneficios tributarios a la I+D+i está constituido, principalmente, por ventajas fiscales aplicables en el Impuesto sobre Sociedades y también en el Impuesto sobre Renta de las Personas Físicas. Se trata de un régimen que está pensado, básicamente, para las empresas y que a pesar de las ventajas que supone para aquéllas presenta "*una elevada complejidad en su aplicación, que ha llevado a diseñar mecanismos de consultas vinculantes que otorguen mayor seguridad jurídica a las empresas con el fin de evitar que las ayudas públicas sean opciones desechadas por las empresas y se fomente, por tanto, la discriminación entre ellas*"[3].

3. BELDA, I. (2023:3). "Metaverso y NFT, nuevos retos tecnológicos en la imposición indirecta e internacional", *Revista de Internet, Derecho y Política,* núm. 37. Disponible en https://acortar.link/ANodQS. Consultado 14/03/2024.

2.1. Concepto de I+D+i

Una de las mayores dificultades que presenta nuestro sistema tributario en relación con los beneficios fiscales por la realización de actividades de I+D+i es la definición de investigación, desarrollo e innovación[4]. Actualmente, el artículo 35.1 a) de la LIS determina que la investigación es la "*indagación original planificada que persiga descubrir nuevos conocimientos y una superior comprensión en el ámbito científico y tecnológico, y desarrollo a la aplicación de los resultados de la investigación o de cualquier otro tipo de conocimiento científico para la fabricación de nuevos materiales o productos o para el diseño de nuevos procesos o sistemas de producción, así como para la mejora tecnológica sustancial de materiales, productos, procesos o sistemas preexistentes.*

Se considerará también actividad de investigación y desarrollo la materialización de los nuevos productos o procesos en un plano, esquema o diseño, así como la creación de un primer prototipo no comercializable y los proyectos de demostración inicial o proyectos piloto, siempre que éstos no puedan convertirse o utilizarse para aplicaciones industriales o para su explotación comercial.

Asimismo, se considerará actividad de investigación y desarrollo el diseño y elaboración del muestrario para el lanzamiento de nuevos productos. A estos efectos, se entenderá como lanzamiento de un nuevo producto su introducción en el mercado y como nuevo producto, aquel cuya novedad sea esencial y no meramente formal o accidental.

También se considerará actividad de investigación y desarrollo la creación, combinación y configuración de software avanzado, mediante nuevos teoremas y algoritmos o sistemas operativos, lenguajes, interfaces y aplicaciones destinados a la elaboración de productos, procesos o servicios nuevos o mejorados sustancialmente. Se asimilará a este concepto el software destinado a facilitar el acceso a los servicios de la sociedad de la información a las personas con discapacidad, cuando se realice sin fin de lucro. No se incluyen las actividades habituales o rutinarias relacionadas con el mantenimiento del software o sus actualizaciones menores"[5].

---

4. En este punto son importantes los manuales metodológicos elaborados por la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Estos manuales de la OCDE son considerados como indicadores de la ciencia y tecnología, comprenden diversos estudios relativos a la investigación y desarrollo (Manual de Frascati, de 2002) y la innovación tecnológica (Manual de Oslo, de 1997). De igual forma, debe tenerse en consideración las previsiones contenidas en el Derecho de la Unión Europea, como las que incorporaba el Tratado de las Comunidades Europeas, cuyos preceptos regulaban las actividades comunitarias en materia de innovación y desarrollo tecnológico, fijando los objetivos a conseguir y estableciendo normas a cumplir para su realización. Véase, GIL GARCÍA, E. (2018:1-31). "La seguridad jurídica en la aplicación de los incentivos a la I+D+i.", *Quincena Fiscal*, núm. 17, parte Estudios. Disponible en https://acortar.link/fGzUPa. Consultado 16/01/2024.

5. Sobre la evolución histórica de estos conceptos véase RIVAS SÁNCHEZ, C. (2007:41-55). "Los incentivos fiscales a la innovación en el Impuesto sobre Sociedades español", *Revista de Contabilidad y Tributación*, núm. 39. Disponible en: https://acortar.link/ZmByut. Consultado 18/03/2024 y FABRA VALLS, M., FALCHI P. (2017:1-56). "Los incentivos fiscales para el fomento de la innovación empresa-

Por su parte, el concepto de innovación tecnológica es similar al de desarrollo, aunque el legislador regula una lista cerrada de desembolsos que dan derecho a la deducción a este tipo de actividades. En este sentido, se establece que la innovación tecnológica es "*la actividad cuyo resultado sea un avance tecnológico en la obtención de nuevos productos o procesos de producción o mejoras sustanciales de los ya existentes. Se considerarán nuevos aquellos productos o procesos cuyas características o aplicaciones, desde el punto de vista tecnológico, difieran sustancialmente de las existentes con anterioridad.*

Esta actividad incluirá la materialización de los nuevos productos o procesos en un plano, esquema o diseño, la creación de un primer prototipo no comercializable, los proyectos de demostración inicial o proyectos piloto, incluidos los relacionados con la animación y los videojuegos y los muestrarios textiles, de la industria del calzado, del curtido, de la marroquinería, del juguete, del mueble y de la madera, siempre que no puedan convertirse o utilizarse para aplicaciones industriales o para su explotación comercial" (artículo 35. 2 a) LIS).

Y continúa el precepto destacando que los únicos gastos que podrán ser incluidos en la base de la deducción serán los que se deriven por actividades de innovación, concretamente:

— *"Actividades de diagnóstico tecnológico tendentes a la identificación, la definición y la orientación de soluciones tecnológicas avanzadas, con independencia de los resultados en que culminen".*
— *"Diseño industrial e ingeniería de procesos de producción, que incluirán la concepción y la elaboración de los planos, dibujos y soportes destinados a definir los elementos descriptivos, especificaciones técnicas y características de funcionamiento necesarios para la fabricación, prueba, instalación y utilización de un producto, así como la elaboración de muestrarios textiles, de la industria del calzado, del curtido, de la marroquinería, del juguete, del mueble y de la madera".*
— *"Adquisición de tecnología avanzada en forma de patentes, licencias, «know-how» y diseños. No darán derecho a la deducción las cantidades satisfechas a personas o entidades vinculadas al contribuyente. La base correspondiente a este concepto no podrá superar la cuantía de 1 millón de euros".*
— *"Obtención del certificado de cumplimiento de las normas de aseguramiento de la calidad de la serie ISO 9000, GMP o similares, sin incluir aquellos gastos correspondientes a la implantación de dichas normas*".

---

rial en España e Italia", *Revista Quincena Fiscal*, núm. 9, parte estudio. Disponible en: https://acortar.link/6ovcCt. Consultado 24/02/2024. TSJ Islas Canarias, Santa Cruz de Tenerife (Sala de lo Contencioso-Administrativo), sentencia núm. 82/2002 de 28 enero (JT 2002\1157), TS (Sala de lo Contencioso-Administrativo, Sección2ª), sentencia de 9 febrero 2016. RJ 2016\1894.

De las definiciones transcritas se "*puede deducir que el legislador está pensando fundamentalmente en el ejercicio de las mismas en el marco de una actividad empresarial de tipo industrial, aunque no cabe descartar su aplicación en cualquier ámbito económico. Otra precisión que debe hacerse es que la ley no exige el éxito o la existencia de algún tipo de resultado satisfactorio de las actividades de I+D+I para que las mismas puedan ser objeto de un tratamiento fiscal favorable*"[6].

En este orden, existe unidad de criterios por parte de los autores de que resulta complejo precisar qué se entiende por actividad de I+D o por el contrario de innovación tecnológica. Para ello, destacan dos cuestiones relevantes:

— Desvincular la actividad de I+D de la consecución de un resultado, frente a la innovación, que hace referencia, precisamente, a aquél.
— La necesidad de que la actividad de ïT se produzca en el ámbito tecnológico del proceso o producto.

De igual forma, se reconocen otras dos características para las actividades de I+D:

— "*Por un lado, exigen una organización y una voluntad o intención dirigida a la obtención de una innovación, lo que excluye los descubrimientos y mejoras casuales.*
— *De otro, pretenden incentivar una actividad investigadora y no se exige, en consecuencia, que tengan un resultado satisfactorio. Ahora bien, estas actividades, para disfrutar de la deducción, deben concretarse en proyectos concretos, sean sus resultados o no satisfactorios. En definitiva, la actividad debe ir dirigida a conseguir una novedad*"[7].

Siguiendo con los criterios expuestos por la doctrina científica, las actividades de investigación son "*aquellas en las que no se aprecie componente alguno que persiga descubrir nuevos conocimientos y una comprensión superior en el ámbito científico y tecnológico*". Tampoco serán consideradas como actividades de investigación y desarrollo la que no tengan "*elementos que den lugar a un producto sustancialmente nuevo, siendo solamente lo que se hace por las entidades meras adaptaciones de productos ya existentes en el mercado a las nuevas condiciones de dicho mercado*". En la medida "*en que el desarrollo constituya,*

6. DELGADO GARCÍA, A. M.; OLIVER CUELLO, R. (2008:60). "Nuevas tendencias en la política de fomento de las actividades de investigación…", *op. cit*. De igual forma, NIETO MONTERO, J. J. (2000:117 y ss.): "Régimen fiscal de la creación e inversión en nuevas tecnologías", *Derecho Tributario e informática*, Tirant Lo Blanch, Valencia. Véase también TEAC resolución de 8 enero 2015 (JT 2019\398).

7. BELDA, I. (2023:3). "Metaverso y NFT, nuevos retos tecnológicos…" *op. cit*. Disponible en https://acortar.link/ANodQS. Consultado 14/03/2024. Para más información: MAGRANER MORENO, F. J. (2006:8-15): "Aspectos relevantes para la calificación de actividades y determinación de la base en las deducciones de I+D e IT", *Tribuna Fiscal*, Ciss, núm. 188, 2006.

como fin último, un nuevo producto o la mejora tecnológica sustancial de un producto existente, tal actividad podrá calificarse como desarrollo a efectos de la aplicación de la deducción de I+D"[8].

Por ende, "*se pude concluir que la investigación se caracteriza por operar en un plano abstracto, desvinculado del proceso industrial, en el que se persigue descubrir nuevos conocimientos, mientras que el desarrollo aplica estos resultados a los procesos productivos. La distinción entre las distintas fases de la investigación, por consiguiente, carece de virtualidad a los efectos de la deducción en la cuota (…), al ofrecerse un régimen común a las actividades de investigación y desarrollo*"[9]. Por lo que se desprenden varias consecuencias, a partir de esta posición científica.

— La primera: que las actividades de investigación y desarrollo destacan por su "*originalidad y novedad en relación con los conocimientos, estado tecnológico, procesos o productos existentes en el mercado, plasmada en un plano teórico en el supuesto de la investigación (nuevos conocimientos y una superior comprensión en el ámbito científico o tecnológico), en el producto en que se concrete el desarrollo (nuevos materiales, productos, procesos o sistemas de productos), o en los nuevos teoremas y algoritmos utilizados en el desarrollo de sistemas operativos y lenguajes nuevos*", quedando fuera las simples adaptaciones o esfuerzos rutinarios para la mejora de los procesos o productos.
— La segunda, que las actividades de investigación y desarrollo no tienen carácter productivo. "*La investigación y el desarrollo se producen en un momento previo al proceso productivo y el límite a partir del cual ya no pueden considerarse gastos de investigación y desarrollo (…) que se podrá incluir la materialización de los nuevos productos en un plano, esquema o diseño, así como la creación de un primer prototipo no comercializable*".
— La tercera consecuencia está relacionada con el hecho de que estas actividades de I+D tienen un carácter planificado ya que se requiere "*una identificación por proyectos en los que se recogerán los objetivos perseguidos, una previsión de los resultados, las actuaciones a realizar, así como un presupuesto de los costes en que se incurrirá en su ejecución*".
— En cuarto lugar, cabe destacar que es intrascendente el resultado al que se llegue, "*en el sentido de que se podrá incurrir en gastos relativos a estas actividades con independencia de que, finalmente y a causa de los resultados obtenidos, el resultado se incorpore o no al proceso productivo*".

---

8. DELGADO GARCÍA, A. M.; OLIVER CUELLO, R. (2008:62). "Nuevas tendencias en la política de fomento de las actividades de investigación…", *op. cit.*

9. BELDA, I. (2023:4). "A vueltas con las deducciones por innovación tecnológica y el software en el Impuesto sobre Sociedades", *Quincena Fiscal*, núm. 7, parte Estudios. Disponible en: https://acortar.link/6xS3pW. Consultado 15/03/2024. También FABRA VALLS, M. (2003:1-22): "Deducción por actividades de I+D+I: principales aspectos de su régimen jurídico", *Jurisprudencia Tributaria*, núm. 11.

— "*Por último, el concepto de innovación tecnológica comprende aquellas actividades de transferencia de tecnología (diagnóstico tecnológico y adquisición de tecnología avanzada) cuyo grado de novedad en relación con el estado de ciencia o de la técnica existente no permite considerarlas como investigación y desarrollo, aunque incorporen novedades respecto a los productos o procesos existentes en relación con la situación de partida de la propia empresa. Y, también, otras como la incorporación de nuevos diseños industriales o procesos de producción o la certificación de sistemas de calidad, con las que la empresa realiza un esfuerzo de adaptación y mejora en un contexto cambiante y competitivo*"[10].

De la misma forma, la Administración tributaria también se ha referido a la distinción entre actividades de desarrollo e investigación y actividades de innovación tecnológica, a través de su contestación a las consultas dirigidas a la Dirección General de Tributos (DGT) y las resoluciones del Tribunal Económico Administrativo Central (TEAC). Respecto a la interpretación que hace la Administración de qué se entiende por actividades de I+D, destacan la contestación a dos consultas a la DGT: una del día 26 de diciembre de 2000 (V0107-00) y la otra del 27 de febrero de 2001 (V0010-01). En el caso de la primera consulta de 26 de diciembre de 2000, Hacienda determina que no es actividad de I+D aquella que corresponda a la elaboración de normativa sobre homologación y certificación de componentes y vehículos completos. Estas actividades, según la Administración tributaria no significan la incorporación de nuevas tecnologías, la adquisición de nuevos conocimientos en el ámbito científico o técnico, la creación de productos novedosos, la inclusión de procesos desconocidos, ni tampoco que mejoren los ya existentes.

Siguiendo con esta doctrina administrativa y de manera parecida a la interpretación anterior, en la contestación a la Consulta Vinculante del 27 de febrero de 2001 la DGT no entendió que se trataba de actividades de investigación y desarrollo la adaptación de un sistema de entorno industrial ya existente en un sector para su utilización en otro distinto con usuarios también diferentes. Y en esta misma línea de interpretación, en relación con el software avanzado, Hacienda considera que lo que hace la entidad es adicionar un desarrollo propio a unas tecnologías preexistentes que se adquieren de terceros para obtener un producto informático con nuevas prestaciones y posibilidades de unos programas, sin necesidad de acudir a su compra en el mercado donde ya existen.

Para identificar los criterios que utiliza la Administración a la hora de precisar qué se considera por innovación tecnológica, debemos remitirnos a las consultas vinculante de 20 de abril de 2005 (V0656-05), consulta vinculante de 11 de octubre de 2005 (V2052-05) y consulta vinculante del 16 de enero de 2008 (V0076-08), entre otras. En las contestaciones a dichas consultas se refuerza la

10. BELDA, I. (2023:3). "Metaverso y NFT, nuevos retos tecnológicos…" *op. cit*. Disponible en https://acortar.link/ANodQS. Consultado 14/03/2024.

idea de la necesidad ineludible de que exista una "*novedad científica o tecnológica significativa en los nuevos productos, procesos o materiales buscados o conseguidos, ya que la norma descarta que tal circunstancia se produzca, por ejemplo, cuando estemos ante «esfuerzos rutinarios para mejorar la calidad de productos o procesos o ante «modificaciones estéticas o menores de productos ya existentes para diferenciarlos de otros similares*"[11].

De esta doctrina administrativa que acabamos de comentar se distinguen algunas ideas delimitadoras de la innovación tecnológica:

— Novedad o mejora sustancial: "*el producto o proceso obtenido ha de ser nuevo o incorporar una mejora sustancial. La novedad no ha de ser meramente formal o accesoria, sino que supone la existencia de un cambio esencial, una modificación de alguna de las características básicas e intrínsecas del producto o proceso, que atribuyen una nueva naturaleza al elemento modificado*"[12].
— La novedad tiene que originarse dentro del ámbito tecnológico del proceso o producto.
— No es necesario que se consiga un nuevo producto o proceso que hasta ese momento no estaba en el mercado, sino el desarrollo de un nuevo.

Por su parte, el TEAC en la Resolución de 3 de junio de 2005, determina que la investigación y el desarrollo son conceptos jurídicos indeterminados que pueden dar lugar a valoraciones subjetivas diferentes porque no siempre resulta sencillo identificar si se trata o no de una mejora tecnológica sustancial o si son realmente simples esfuerzos rutinarios para mejorar la calidad de materiales, productos, procesos o sistemas. Este órgano es del criterio de que en el ámbito tecnológico los avances que se producen, en contadas ocasiones, son efectivamente novedosos, por lo cual para saber si estamos en presencia de una novedad, mejora sustancial o esfuerzo rutinario de mejora será imprescindible que se estudie y aprecie todos los elementos contenidos en la norma[13].

Asimismo, el apartado 3 del artículo 35 de la LIS incorpora una delimitación negativa de las actividades que no pueden ser consideradas ni de investigación, ni de desarrollo, ni de innovación tecnológicas. Dispone este precepto que no se consideran actividades de I+D+i:

— *"Las actividades que no impliquen una novedad científica o tecnológica significativa. En particular, los esfuerzos rutinarios para mejorar la calidad de productos o procesos, la adaptación de un producto o proceso de*

11. Para más información: DGT, consulta vinculante núm. V1841/12 de 20 septiembre (JT 2012\1193), DGT, consulta vinculante núm. V0054/02 de 17 septiembre (JUR 2003\24367).

12. BELDA, I. (2023:3). "Metaverso y NFT, nuevos retos tecnológicos…" *op. cit*. Disponible en https://acortar.link/ANodQS. Consultado 14/03/2024.

13. También del TEAC, resolución de 21 diciembre 2006 (JT 2007\498); TEAC, resolución de 19 enero 2001 (JT 2001\188).

producción ya existente a los requisitos específicos impuestos por un cliente, los cambios periódicos o de temporada, excepto los muestrarios textiles y de la industria del calzado, del curtido, de la marroquinería, del juguete, del mueble y de la madera, así como las modificaciones estéticas o menores de productos ya existentes para diferenciarlos de otros similares".

— *"Las actividades de producción industrial y provisión de servicios o de distribución de bienes y servicios. En particular, la planificación de la actividad productiva: la preparación y el inicio de la producción, incluyendo el reglaje de herramientas (…); la incorporación o modificación de instalaciones, máquinas, equipos y sistemas para la producción que no estén afectados a actividades calificadas como de investigación y desarrollo o de innovación; la solución de problemas técnicos de procesos productivos interrumpidos; el control de calidad y la normalización de productos y procesos; la prospección en materia de ciencias sociales y los estudios de mercado; el establecimiento de redes o instalaciones para la comercialización; el adiestramiento y la formación del personal relacionada con dichas actividades".*

— *"La exploración, sondeo o prospección de minerales e hidrocarburos".*

Por último, debemos mencionar que el cuarto apartado del artículo 35 de la LIS permite que los contribuyentes aporten un informe motivado "*emitido por el Ministerio de Economía y Competitividad, o por un organismo adscrito a éste, relativo al cumplimiento de los requisitos científicos y tecnológicos exigidos*" (…) "*para calificar las actividades del contribuyente como investigación y desarrollo, o*" (…) "*para calificarlas como innovación tecnológica*". (…)[14] "*Dicho informe tendrá carácter vinculante para la Administración tributaria exclusivamente en relación con la calificación de las actividades*". El carácter vinculante de este informe, básicamente, en lo que respecta a la clasificación como innovación tecnológica del desarrollo del software era entendido por la jurisprudencia en términos amplios y prevalecía la calificación que contenían estos informes motivados[15]. Sin embargo, recientemente se ha producido un cambio interpretativo de la Audiencia Nacional que se pronuncia a favor del TEAC que no reconoce el carácter vinculante de la calificación como iT desarrollo del software que admitían los informes motivados de los contribuyentes afectados[16].

---

14. TSJ de Madrid, Sentencia de fecha 10 de julio de 2013 (JUR 2013, 261193). ALONSO ANTÓN, C. (2016: 1-3). "Deducción en el IS por actividades de investigación y desarrollo. Alcance del informe de la Administración", *Revista Aranzadi Doctrinal*, núm. 8, parte Jurisprudencia. Disponible en https://acortar.link/2qAm5q. Consultado 30/01/2024.

15. Sobre el carácter vinculante de dichos informes motivados, entre otras: sentencia SAN 2459/2021, del 12 de mayo del 2021; sentencia SAN 3099/2021, del 2 de junio del 2021; sentencia SAN 3172/2021, del 1 de julio del 2021; sentencia SAN 3177/2021, del 7 de julio del 2021.

16. Sentencia SAN 5529/2022, del 23 de noviembre del 2022, sentencia SAN 5530/2022, de la misma fecha, sentencia SAN 5537/2022, del 9 de diciembre del 2022, sentencia SAN 5731/2022, del 14 de noviembre del 2022 y sentencia SAN 5866/2022, del 30 de noviembre del 2022. El cambio de criterio interpretativo de la Audiencia Nacional referente a la calificación como innovación tecnológica del

2.2. Beneficios fiscales por actividades I+D+i en el Impuesto de Sociedades

Ya señalábamos al inicio de este estudio que es en el IS y en el IRPF (por la remisión que hace este tributo al primer impuesto) donde se prevén los beneficios fiscales más destacados dentro del ordenamiento tributario español relativos a las actividades de I+D+i. En este orden, las normas del IS, respecto a dichas actividades, afectan fundamentalmente a los ajustes al resultado contable en la configuración de la base imponible en relación con las amortizaciones y a la deducción de la cuota del impuesto[17].

2.2.1. Libertad de amortización de activos afectos a actividades de I+D

El primero de los beneficios fiscales por actividades de I+D+i que analizaremos se vincula a la libertad de amortización, a través de la cual se permite al inversor elegir el momento en que haya de registrarse la depreciación fiscal, sin necesidad de que tenga que acogerse a las reglas generales de amortización máxima de los activos. De esta forma, los contribuyentes pueden acelerar las dotaciones a la amortización por encima de los porcentajes máximos determinados para cada activo. Este beneficio *"supone anticipar en el tiempo gastos fiscales; aunque al final se terminará amortizando lo mismo: el valor del activo. De este modo, no se reduciría en un sentido estricto el impuesto pagado; únicamente se lograría su diferimiento*"[18].

La primera apreciación que debemos hacer respecto a la libertad de amortización es que la misma no se aplica a las actividades clasificadas como innovación tecnológica[19]. El artículo 12.3 b) de la LIS regula la libertad de amortización de los elementos del inmovilizado material e intangible, en la parte que se hallen afectos a las actividades de investigación y desarrollo. No obstante, el

---

desarrollo del software se basa en un informe emitido por el Equipo de Apoyo Informático de la Delegación Central de Grandes Contribuyentes. Sobre este cambio de postura jurisprudencial remítase a: BELDA, I. (2023:1-16). "A vueltas con las deducciones por innovación tecnológica y el software en el Impuesto sobre Sociedades", *Quincena Fiscal*, núm.7. Disponible en https://acortar.link/Y3hsLQ, consultado 30/05/2024.

17. MARTÍNEZ-CARRASCO PIGNATELLI, J. M. (2015:1-22). "Deducciones en la cuota tributaria del Impuesto sobre Sociedades", *Quincena Fiscal, núm.* 21/2015. Disponible en: https://acortar.link/mTnfct. Consultado 03/02/2024.

18. RIVAS, S. C., (2007:76). "Los incentivos fiscales a la innovación en el Impuesto sobre Sociedades español: historia y actualidad", *Revista de Contabilidad y Tributación,* Centro de Estudios Financiero, núm. 39. Disponible en: https://acortar.link/ZmByut. Consultado: 05/04/2024.

19. Entiende la doctrina que, en las actividades de investigación y desarrollo, la amortización tiene, a su vez, una finalidad extrafiscal. Por todos, NIETO MONTERO, J. J. (2000:130). "Régimen fiscal de la creación., *op., cit*. RIVAS SÁNCHEZ, C. y ORDÓÑEZ DE HARO, C. (2004: 35 y ss.), "Régimen tributario de las actividades de investigación y desarrollo e innovación tecnológica en el Impuesto sobre Sociedades", *Revista Técnica Tributaria*, núm. 66.

precepto no aclara cuál es el período de tiempo de la afectación del bien. "*En este sentido, es posible entender que los elementos del inmovilizado material e intangible deberían permanecer afectos hasta que se cumpla su finalidad específica en las actividades de investigación y desarrollo, en concordancia con lo que determina el artículo 35.1 c) de la LIS*"[20].

La excepción a este régimen especial de libertad de amortización la encontramos en los edificios que quedan excluidos del mismo y que podrán amortizarse de forma lineal durante un período de 10 años, aunque sigue constituyendo un trato fiscal ventajoso para estos inmuebles "*hay que tener en cuenta que, según las tablas oficiales de amortización, los edificios industriales tienen un coeficiente máximo del 3% y los edificios administrativos y de viviendas un 2%; porcentajes que se ven incrementados hasta el 10% en el caso de afectarse estos activos a la I+D*"[21].

En cualquier caso, estas normas sobre libertad de amortización que afectan a las actividades de I+D, solo se van a aplicar en el ámbito fiscal, ya que desde la perspectiva contable la amortización se hará en función de la vida útil del bien de que se trate. Por ello, a efectos fiscales, dependiendo de la amortización que se realice será necesario hacer los ajustes fiscales en la base imponible. "*De manera que, en los años en que se decida aplicar una amortización fiscal superior a la dotación contable, se tendrá que realizar el correspondiente ajuste negativo al resultado contable. Esta diferencia negativa revertirá en los ejercicios posteriores, a través del ajuste positivo al resultado contable, que se producirá como consecuencia de la mayor cuantía de la amortización contable con respecto a la fiscal. Lo cual sucederá siempre que el inmovilizado permanezca en el patrimonio hasta el fin de su vida útil. Si se transmite el bien, la diferencia negativa que surgió en su día se regularizará en el período en que se enajene el inmovilizado por la diferencia entre el resultado de la operación desde el punto de vista contable y fiscal*"[22].

---

20. QUIRÓS GÓMEZ, J. (2021:9-10). "Incentivos fiscales a la investigación…", *op. cit*., Disponible en: https://acortar.link/pT6FBW. Consultado 03/04/2024. "*Para poder disfrutar de la deducción el inmovilizado material e inmaterial tiene que estar afecto exclusivamente a actividades de I+D. Del mismo modo, se debe tener en cuenta que esta deducción está condicionada a que la inversión permanezca en el patrimonio del sujeto pasivo hasta que cumpla su finalidad específica en la actividad de I+D, a menos que su vida útil fuese menor según las tablas oficiales de amortización*". GIL GARCÍA, E. (2018:1-31). "La seguridad jurídica en la aplicación …" *op. cit.,* Disponible en https://acortar.link/fGzUPa. Consultado 16/01/2024. De manera muy parecida: DGT, consulta núm. 2055/04 de 13 diciembre (JUR 2005\43566).

21. RIVAS, S. C., (2007:78). "Los incentivos fiscales a la innovación en el Impuesto sobre Sociedades español: historia y actualidad", *op. cit*., Disponible en: https://acortar.link/ZmByut. Consultado: 05/04/2024.

22. DELGADO GARCÍA, A. M.; OLIVER CUELLO, R. (2008:65). "Nuevas tendencias en la política de fomento de las actividades de investigación…", *op. cit*.

2.2.2. Libertad de amortización de los gastos de I+D activados

La libertad de armonización de los gastos de I+D activados parte de la premisa de que la deducción de los gastos realizados por una entidad contribuyente del IS conlleva dos exigencias: su contabilización conforme a las normas del Plan General de Contabilidad y su admisibilidad por la LIS a la hora de establecer los ajustes sobre el resultado contable para la determinación de la base imponible de dicho impuesto.

De manera general, todos los gastos contabilizados serán deducibles, con algunas excepciones recogidas en la LIS y en las otras disposiciones sobre ajustes contenidas en la propia norma tributaria (que no incluyen los gastos I+D, por lo que pueden ser deducibles). No obstante, los gastos de investigación y desarrollo tienen rasgos que les separan de otras figuras afines. En este orden, el Plan General de Contabilidad contempla su activación al cierre del ejercicio como inmovilizado intangible, siempre que se dividan por proyectos individualizados y especificados para que puedan ser distribuido en el tiempo, además deben existir indicios racionales de su éxito técnico y de la rentabilidad de los proyectos.

Los gastos de investigación y desarrollo activados como inmovilizado intangible, excluidas las amortizaciones de los elementos que disfruten de libertad de amortización podrán amortizarse libremente (artículo 12.3 c) de la LIS). De esta forma, el legislador descarta de este beneficio a "*las amortizaciones de los elementos que disfruten de libertad de amortización, teniendo su origen en que entre los gastos activados se recoge la amortización del inmovilizado afecto directamente al proyecto de I+D y éstos ya gozan de libertad de amortización*" con lo que acabamos de comentar en el apartado anterior (artículo 12.3 b) de la LIS), "*lo que provocaría duplicar el beneficio*"[23].

Para que los gastos de investigación y desarrollo formen parte del inmovilizado inmaterial y, en consecuencia, puedan amortizarse, tendrán que producirse una serie de condiciones:

— Existencia de un proyecto específico e individualizado para cada actividad de investigación y desarrollo.
— La asignación, imputación y distribución temporal de los costes de cada proyecto debe estar claramente establecidas.
— En todo momento deben existir motivos fundados de éxito técnico en la realización del proyecto de investigación y desarrollo, tanto para el caso en el que la empresa tenga la intención de su explotación directa como para el de la venta a un tercero del resultado del proyecto una vez concluido, si existe mercado.

23. QUIRÓS GÓMEZ, J. (2021:9-10). "Incentivos fiscales a la investigación…", *op. cit.*, Disponible en: https://acortar.link/pT6FBW. Consultado 03/04/2024.

En definitiva, que exista:

— Una rentabilidad económica-comercial del proyecto asegurada.
— Una financiación de los distintos proyectos de investigación y desarrollo que permita completar la realización de éstos.
— Una individualización específica de los proyectos y su coste claramente establecido para que pueda ser distribuido en el tiempo.
— Una serie de motivos fundados de éxito técnico y de la rentabilidad económico comercial del proyecto o proyectos de lo que se trate.

El cumplimiento de estos requisitos permitirá considerar los gastos en investigación y desarrollo como inmovilizado inmaterial, amortizándose contablemente lo más breve posible siempre dentro del plazo de 5 años desde la conclusión del proyecto de investigación y desarrollo. Por el contrario, el incumplimiento de aquellas exigencias provocará la consideración de los gastos de investigación y desarrollo como gastos del ejercicio en que se realicen[24].

En resumen, los gastos en investigación y desarrollo serán deducibles, ya sea como gastos normales del ejercicio o como amortizaciones (en aquellos casos que fueran considerados como inmovilizado intangible). A lo que debemos incluir la libertad de amortización que hacíamos referencia en el apartado anterior, así como las deducciones en cuota que examinamos a continuación. Lo que nos lleva afirmar que el beneficio fiscal es doble, pues sirven tanto para reducir la base imponible como para minorar la cuota tributaria.

2.2.3. Reducción de rentas procedentes de activos intangibles

El artículo 23 de la LIS recoge una reducción aplicable en la base imponible del tributo y que afecta tanto a las actividades de desarrollo e investigación como a las actividades de innovación tecnológicas. En efecto, las rentas positivas procedentes de la cesión del derecho de uso o de explotación de patentes, modelos de utilidad, certificados complementarios de protección de medicamentos y de productos fitosanitarios, dibujos y modelos legalmente protegidos, que deriven de actividades de I+D+i, tendrán derecho a la reducción de la base imponible resultante de multiplicar el 60% de los ingresos integrados, por el resultado de un coeficiente[25] que se calcula en base a gastos de creación, adquisición y subcontratación. "*Beneficiando a aquellos contribuyentes que acrediten haber*

24. Al permitirse libertad de amortización de los "gastos de investigación y desarrollo, es evidente que los beneficios tributarios para las PYME que inciden en la amortización poco van a influir en ese elemento del inmovilizado inmaterial, en cuanto el máximo beneficio tributario en lo que amortización se refiere viene ya establecido en el régimen general". ECHEVERRÍA ECHEVERRÍA, Gaspar (2005:178-179) Beneficios tributarios para la PYME en el Impuesto sobre Sociedades, Editorial Universitario, Granada.

25. En ningún caso se incluirán en dicho coeficiente gastos financieros, amortizaciones de inmuebles u otros gastos no relacionados directamente con la creación del activo.

desarrollado directamente una actividad inventora respecto a aquellos que se limitan a encargar o comprar a terceros, en España o en el extranjero, el fruto de dicha actividad"[26].

Esta reducción de la base también resultará de aplicación a las rentas positivas procedentes de la transmisión de los activos intangibles referidos en el mismo, cuando dicha transmisión se realice entre entidades que no tengan la condición de vinculadas.

También entiende el legislador que se trata de rentas positivas susceptibles de reducción:

— Los ingresos procedentes de la cesión del derecho de uso o de explotación de los activos y las rentas positivas procedentes de su transmisión, que superen la suma de los gastos incurridos por la entidad directamente relacionados con la creación de los activos que no hubieran sido incorporados al valor de los activos.
— Las cantidades deducidas por aplicación del artículo 12.2 de la LIS en relación con los activos.
— Los gastos directamente relacionados con los activos, que se hubieran integrado en la base imponible.

En cualquier caso, para poder aplicar la reducción será necesario que se cumplan con los requisitos que aparecen en el apartado 3 del artículo 23 LIS. Estos son:

— *"Que el cesionario utilice los derechos de uso o de explotación en el desarrollo de una actividad económica y que los resultados de esa utilización no se materialicen en la entrega de bienes o prestación de servicios por el cesionario que generen gastos fiscalmente deducibles en la entidad cedente, siempre que, en este último caso, dicha entidad esté vinculada con el cesionario".*
— *"Que el cesionario no resida en un país o territorio de nula tributación o calificado como paraíso fiscal, salvo que esté situado en un Estado miembro de la Unión Europea y el contribuyente acredite que la operativa responde a motivos económicos válidos y que realice actividades económicas".*
— *"Cuando un mismo contrato de cesión incluya prestaciones accesorias de bienes o servicios deberá diferenciarse en dicho contrato la contraprestación correspondiente a los mismos".*
— *"Que la entidad disponga de los registros contables necesarios para poder determinar cada uno de los ingresos y de los gastos directos (…) correspondientes a los activos objeto de cesión".*

26. BELDA, I. (2023:2). "Metaverso y NFT, nuevos retos tecnológicos…" *op. cit*. Disponible en https://acortar.link/ANodQS. Consultado 14/03/2024.

De la misma manera, el precepto delimita las rentas que no darán derecho a la reducción, que serán aquellas procedentes de la cesión del derecho de uso o de explotación o de la transmisión de:

— Marcas.
— Obras literarias, artísticas o científicas, incluidas las películas cinematográficas.
— Derechos personales susceptibles de cesión, como los derechos de imagen.
— Programas informáticos distintos al software avanzado registrado que derive de actividades de investigación y desarrollo.
— Equipos industriales, comerciales o científicos.
— Planos.
— Fórmulas o procedimientos secretos.
— Derechos sobre informaciones relativas a experiencias industriales, comerciales o científicas.

Finalmente, el contribuyente antes de aplicar la reducción podrá solicitar a la Administración tributaria la adopción de dos acuerdos previos: uno de valoración en relación con los ingresos procedentes de la cesión de los activos y de los gastos asociados, así como de las rentas generadas en la transmisión. Y otro acuerdo de calificación de los activos como pertenecientes a alguna de las categorías anteriormente señaladas y de valoración en relación con los ingresos procedentes de la cesión de éstos y de los gastos asociados, así como de las rentas generadas en la transmisión. En este segundo caso, la resolución del acuerdo requerirá informe vinculante emitido por la DGT, en relación con la calificación de los activos. A su vez, la Administración tributaria podrá solicitar opinión no vinculante al respecto, al Ministerio de Economía, Industria y Competitividad.

2.2.4. Deducción en la cuota por la realización de actividades I+D+i[27]

Uno de los beneficios fiscales más atrayentes para aquellos contribuyentes que realicen actividades de I+D+i es la deducción en la cuota íntegra que regu-

27. Hasta el 1 de enero de 2011, estuvo vigente la deducción para el fomento de las tecnologías de la información y de la comunicación. Se trataba de una deducción de la cuota del IS que fue introducida por el RDL 3/2000, de 23 de junio, de Medidas fiscales urgentes de estímulo al ahorro familiar y a las PYMES. Esta medida estuvo pensada para apoyar a las Empresas de Reducida Dimensión (ERD) en sus iniciativas de innovación e internacionalización con el fin de mejorar su competitividad y lograr la supervivencia en un entorno de globalización en constante cambio. El importe de la deducción se derivaba de aplicar al importe total de los gastos e inversiones un porcentaje del 15 por ciento. Gastos e inversiones relativos con la presencia en Internet que incluía la adquisición de equipos, con software y periféricos asociados, para el desarrollo y publicación de páginas y portales web; la realización de trabajos, internos o contratados a terceros, para el diseño y desarrollo de páginas y

la el artículo 35 de la LIS. Al igual que sucedía con la reducción en la base por rentas positivas procedentes de la cesión del derecho de uso o de explotación de patentes, modelos de utilidad, certificados complementarios de protección de medicamentos y de productos fitosanitarios, dibujos y modelos legalmente protegidos, que deriven de actividades de I+D+i, esta ventaja fiscal afecta tanto a las actividades de I+D como a las actividades iT[28].

En el caso de las primeras, actividades de I+D, la base de la deducción estará constituida por el importe de los gastos de investigación y desarrollo y, en su caso, por las inversiones en elementos de inmovilizado material e intangible excluidos los edificios y terrenos. *"Se considerarán gastos de investigación y desarrollo los realizados por el contribuyente, incluidas las amortizaciones de los bienes afectos a las citadas actividades, en cuanto estén directamente relacionados con dichas actividades y se apliquen efectivamente a la realización de éstas, constando específicamente individualizados por proyectos"* (artículo 35.1 b LIS).

La realización de las actividades de investigación y desarrollo dará derecho a practicar una deducción de la cuota íntegra del 25 por 100 de los gastos efectuados en el período impositivo. En el caso de que los gastos efectuados en la realización de actividades de I+D en dicho período impositivo sean mayores que la media de los efectuados en los 2 años anteriores se aplicará el 25 por ciento hasta dicha media, y el 42 por ciento sobre el exceso respecto de ésta. También el legislador prevé una deducción adicional del 17 por ciento del importe de los gastos de personal de la entidad correspondientes a investigadores cualificados adscritos en exclusiva a actividades de investigación y desarrollo[29].

Por su parte, el porcentaje de la deducción será de un 8 por ciento por las inversiones en elementos de inmovilizado material e intangible, excluidos los edificios y terrenos, siempre que estén afectos exclusivamente a las actividades

---

portales web; la instalación e implantación de dichos sistemas y la formación del personal de la empresa para su uso. Además de otros gastos e inversiones relacionados con el comercio electrónico, su implantación a través de Internet con las adecuadas garantías de seguridad y confidencialidad de las transacciones.

28. Sobre este beneficio fiscal: AN (Sala de lo Contencioso-Administrativo, Sección2ª), sentencia de 30 julio 2020 (JUR 2020\303889), TSJ Madrid (Sala de lo Contencioso-Administrativo, Sección5ª), sentencia núm. 573/2019 de 12 junio (JUR 2019\306325); TSJ Madrid (Sala de lo Contencioso-Administrativo, Sección5ª), sentencia núm. 559/2019 de 5 junio. JUR 2019\215653, TS (Sala de lo Contencioso-Administrativo, Sección2ª), sentencia de 21 noviembre 2013 (RJ 2014\470).

29. "*La DGT también se ha pronunciado con respecto a lo que considera investigador cualificado adscrito en exclusiva a actividades de I+D en su consulta vinculante V0059-01 del 10 de julio de 2001. En ella reconoce como investigador cualificado a aquel profesional poseedor de título de nivel universitario, que trabaja en la concepción o creación de nuevos conocimientos, productos, procesos, métodos y sistemas y en la gestión de los respectivos proyectos. Por ello, no tendrían esta consideración aquellos técnicos y personal asimilado que participan en la actividad de I+D ejecutando tareas bajo la supervisión de investigadores, así como el personal de apoyo y el personal administrativo".* BELDA, I. (2023:5). "Metaverso y NFT, nuevos retos tecnológicos…" *op. cit.* Disponible en https://acortar.link/ANodQS. Consultado 14/03/2024. Véase en este sentido, DGT, consulta vinculante núm. V1833/05 de 20 septiembre (JT 2005\1294).

de investigación y desarrollo. A su vez, los elementos en que se materialice la inversión deberán permanecer en el patrimonio del sujeto pasivo, salvo pérdidas justificadas, hasta que cumplan su finalidad específica en las actividades de investigación y desarrollo, excepto que su vida útil conforme al método de amortización que se aplique fuese inferior.

En relación con la deducción por actividades de innovación tecnológica (art. 35.2 TRLIS), los únicos gastos corrientes de iT susceptibles de beneficiarse del crédito fiscal regulado en el precepto son:

— Las actividades de diagnóstico tecnológico tendentes a la identificación, la definición y la orientación de soluciones tecnológicas avanzadas, con independencia de los resultados en que culminen.
— El diseño industrial e ingeniería de procesos de producción que incluirán la concepción y la elaboración de los planos, dibujos y soportes destinados a definir los elementos descriptivos, especificaciones técnicas y características de funcionamiento necesarios para la fabricación, prueba, instalación y utilización de un producto, así como la elaboración de muestrarios textiles, de la industria del calzado, del curtido, de la marroquinería, del juguete, del mueble y de la madera.
— La adquisición de tecnología avanzada en forma de patentes, licencias, know-how y diseños.
— La obtención del certificado de cumplimiento de las normas de aseguramiento de la calidad de la serie ISO 9000 o similares.

El porcentaje de deducción por actividades de iT es del 12 por ciento de los gastos incurridos en el periodo impositivo por este concepto.

Hay que tener en cuenta, a su vez, una serie de normas comunes a las deducciones por actividades de I+D e innovación tecnológica, como que:

— La deducción se minorará en el importe de las subvenciones recibidas para el fomento de las actividades de I+D+i e imputables como ingreso en el período impositivo.
— Los gastos de investigación, desarrollo e innovación que se incluyan en la base de la deducción deben corresponder a actividades efectuadas en España o en cualquier Estado miembro de la Unión Europea o del Espacio Económico Europeo[30].
— Tendrán la consideración de gastos de investigación, desarrollo e innovación las cantidades pagadas para la realización de dichas actividades en España o en cualquier Estado miembro de la Unión Europea o del Espa-

30. Se adapta la norma interna a la Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 13 de marzo de 2008. Al respecto remítase también a TEAC, resolución de 26 abril 2012 (JT 2012\593).

cio Económico Europeo, por encargo del contribuyente, individualmente o en colaboración con otras entidades[31].

— Los sujetos pasivos podrán aportar informe motivado emitido por el por el Ministerio de Economía y Competitividad, o por un organismo adscrito a éste, relativo al cumplimiento de los requisitos científicos y tecnológicos exigidos en el artículo 35 LIS para calificar las actividades como investigación y desarrollo o innovación tecnológica. Dicho informe tendrá carácter vinculante para la Administración.
— El contribuyente podrá presentar consultas sobre la interpretación y aplicación del derecho a la deducción sobre la cuota íntegra del IS, cuya contestación tendrá carácter vinculante para la Administración tributaria.
— El contribuyente podrá solicitar a la Administración tributaria la adopción de acuerdos previos de valoración de los gastos e inversiones correspondientes a proyectos de investigación y desarrollo o de innovación tecnológica.

Llegados a este punto, podemos concretar respecto a la deducción en la cuota por actividades de I+D+i que:

— La deducción en la cuota es compatible con las demás ventajas fiscales que hemos visto hasta el momento y representan para los contribuyentes una doble ventaja fiscal.
— Existe una gran diferencia entre la cuantía de los porcentajes aplicables y el sistema empleado para determinar el importe de la deducción por actividades de innovación frente a la deducción por I+D. "*Es más, esta es una de las razones principales por las que resulta tan importante la diferenciación entre ambos tipos de actividades*". (…)
— "*El sistema seguido por nuestra legislación deja de dar un trato más favorable a los incrementos de gasto con respecto a los periodos anteriores que a los esfuerzos continuados años tras año. Es decir, que todo se reduce a aplicar un porcentaje sobre el volumen de gastos de un periodo, sin atender a los desembolsos registrados en años anteriores. De este modo el sistema de innovación parece renunciar a las supuestas ventajas que llevaron en su momento a optar por un sistema mixto en el caso de la I+D*"[32].

31. CALVO VÉRGEZ, J. (2010:1-7) "La incidencia del lugar de realización en la aplicación de la deducción en concepto de I+D+i dentro del Impuesto sobre Sociedades a la luz de la reciente jurisprudencia del Tribunal de Justicia de la Unión Europea", *Revista Aranzadi Unión Europea*, núm. 11, 2010 parte Crónica. Disponible en https://acortar.link/ilw4p5. Consultado 20/04/2024.

32. BELDA, I. (2023:9). "A vueltas con las deducciones por innovación…" *op. cit*. Disponible en: https://acortar.link/6xS3pW. Consultado 15/03/2024.

2.3. Incentivos fiscales por actividades I+D+i en el Impuesto sobre la Renta de las Personas Físicas

2.3.1. Rendimientos de actividades económicas de personas físicas

Uno de los impuestos que mayor relevancia fiscal tienen dentro de nuestro ordenamiento, lo es sin duda el IRPF, cuyo hecho imponible estará constituido, entre otras modalidades, por los rendimientos de las actividades económicas obtenidos por el contribuyente. Lo primero que debemos subrayar, y que se vincula al objeto de estudio de este trabajo, es que el artículo 28 de la LIRPF establece que el rendimiento neto de las actividades económicas realizadas por las personas físicas o las entidades a las que se refiere el artículo 35.4 de la LGT se determinará aplicando las normas del IS. De la misma forma, el artículo 68 apartado 2 de la LIRPF dispone que los contribuyentes que ejerzan actividades económicas les serán de aplicación los incentivos y estímulos a la inversión empresarial establecidos en el IS con igualdad de porcentajes y límites de deducción[33]. En definitiva, que para la cuantificación de los rendimientos de las actividades económicas, se podrán deducir los gastos de I+D+i en la base imponible, como gastos del ejercicio o por su activación y posterior amortización como inmovilizado intangible y también, serán de aplicación para las personas físicas que realicen actividades económicas, las mismas deducciones reguladas en la LIS (artículo 35 a 39), según la remisión del artículo 68.2 LIRP, concretamente la deducción sobre la cuota íntegra por la realización de actividades de I+D+i.

Antes de continuar, nos parece oportuno hacer una serie de precisiones en relación con el cálculo de los rendimientos por actividades económicas. En este orden, debemos incidir en el hecho de que existen varios métodos para determinar el rendimiento neto que ha de introducirse en la base imponible general del IRPF. El método más exacto para determinar la verdadera capacidad económica del contribuyente es el de estimación directa. Sin embargo, la utilización de este método requerirá, por parte del contribuyente, la realización de un mayor número de gestiones (contabilidad ajustada al Código de Comercio, realización de ajustes extracontables adecuados para determinar la capacidad gravable, entre otros), aunque el legislador proporciona otras vías de cálculo del beneficio empresarial a efectos tributarios que implican un menor coste de gestión para aquellos pequeños empresarios individuales, nos referimos a la estimación objetiva y la estimación directa simplificada.

Cabe recordar que algunos sectores regulados por la normativa tributaria pueden determinar su base de forma objetiva (atendiendo a una serie de elementos como son: trabajadores, potencia eléctrica consumida, etc.) a través de los cuales se calculará el rendimiento de actividades económicas por aquellos signos externos de capacidad económica, salvo que se renuncie a éste o que el ordenamiento jurídico excluya expresamente de la estimación objetiva de la

33. Excepto aquellas que reconoce el artículo 39 apartados 2 y 3 de la LIS.

base. En el caso de que la actividad económica no esté contemplada entre los sectores para los que la norma prevé el régimen de estimación objetiva o bien cuando lo determine, el empresario renuncie a dicha estimación o éste haya sido excluido de aquella estimación objetiva, se calculará el rendimiento de la actividad económica por el régimen de estimación directa simplificada. Igualmente, si el contribuyente que está sujeto al régimen de estimación directa simplificada, renuncia o resulta excluido de este último régimen, entonces, deberá determinar el rendimiento de su actividad económica por el régimen de estimación directa normal.

Teniendo en cuenta lo comentado hasta el momento, y tomando en consideración la remisión que hace la LIRPF en sus artículos 26 y 68 podemos firmar que en la determinación de la base imponible serán deducibles los gastos de I+D+i que prevé el artículo 12 y el artículo 23 de la LIS y la deducción en la cuota íntegra que contempla la misma ley en su artículo 35, siempre y cuando se determinen los rendimientos de las actividades económicas a través de la estimación directa normal.

Ahora bien, la aplicación de aquellas deducciones, tanto en la base como la cuota, por la realización de actividades económicas, difícilmente, se podrán aplicar cuando se calculen los rendimientos por el método de estimación directa simplificada o por el método de estimación objetiva. En el caso de la estimación directa simplificada, si bien es cierto que la determinación de la base imponible y el inmovilizado intangible sigue las mismas reglas de amortización que en la estimación directa normal, tiene como peculiaridad la simplificación de las tablas de amortización aplicables al inmovilizado material. "*En este caso, el inmovilizado material afecto a actividades de I+D sólo puede amortizarse linealmente conforme a la tabla simplificada que se apruebe por el Ministerio de Economía y Hacienda"*[34]. Lo que significa que, si el sujeto pasivo desea acogerse a la libertad de amortización, deberá renunciar a la estimación directa simplificada y optar por la normal.

En lo que respecta al método de estimación objetiva el artículo 68. 2 c) de la LIRPF regula que *"los contribuyentes por este Impuesto que ejerzan actividades económicas y determinen su rendimiento neto por el método de estimación objetiva sólo les serán de aplicación los incentivos a que se refiere este apartado 2 cuando así se establezca reglamentariamente teniendo en cuenta las características y obligaciones formales del citado método"*[35].

Esta disposición es acorde con las características que atañen a la estimación objetiva "*dado que las normas de cálculo del rendimiento neto parten de la aplicación de signos, índices y módulos objetivos*", (…) y *"no cabe tener en cuenta los gastos específicos que se realizan en actividades de I+D+I, ni es posible su activación ni la amortización libre. Por lo tanto, en este ámbito no existe ningún*

34. DELGADO GARCÍA, A. M.; OLIVER CUELLO, R. (2008:70). "Nuevas tendencias en la política de fomento de las actividades de investigación…", *op. cit.*

35. Dicha regulación todavía no se ha producido.

beneficio tributario en la determinación de la base imponible que tenga en cuenta las actividades de I+D+I"[36]. Por ende, al igual que sucede con la estimación directa simplificada, si el contribuyente desea aplicar los beneficios tributarios previstos para las actividades de I+D+i, deberá renunciar a este régimen y optar por la estimación directa normal.

2.3.2. Rendimientos de actividades económicas de entidades en régimen de atribución de rentas

La persona física es el contribuyente del impuesto, sin embargo, la LIRPF también se aplica a determinadas personas jurídicas, concretamente, las sociedades civiles (salvo que se trate de sociedades agrarias de transformación en cuyo caso están sometidas al IS) herencias yacentes, comunidades de bienes y demás entidades a que se refiere el artículo 35.4 de la LGT. En estos últimos casos se aplica el régimen de atribución de rentas establecido en el artículo 8.3 de la LIRPF, el que dispone que las "*rentas correspondientes a las mismas se atribuirán a los socios, herederos, comuneros o partícipes, respectivamente*".

Como acabamos de indicar en el apartado anterior, aunque los beneficios tributarios por la realización de actividades de I+D+i vienen recogidos en la LIS, también se podrán aplicar a los contribuyentes del IRPF que determine el rendimiento de sus actividades económicas mediante estimación directa normal, gracias a la remisión expresa que hace la LIRPF a la LIS. En definitiva, dentro las rentas sujetas a gravamen en el IRPF se encuentran los rendimientos de actividades económicas. En estos rendimientos, los beneficios tributarios contemplados en los preceptos de la LIS incidirán en el cálculo del rendimiento neto de tales actividades económicas siempre que para calcular dicho rendimiento se atienda al régimen de estimación directa normal. Ello implica que las ventajas fiscales que reconoce el IS por I+D+i serán aplicables de forma indirecta a los sujetos pasivos del IRPF, ya sean profesionales o empresarios, siempre que los mismos apliquen el método de estimación directa normal.

En el régimen de atribución de rentas, las entidades desarrollan fiscalmente la actividad productora de los rendimientos, por lo que la determinación del rendimiento neto derivado de la actividad empresarial se realizará por la entidad sobre la base de sus datos contables o registrales y atendiendo al régimen de determinación del rendimiento neto al que se halle acogida. Posteriormente, dichas rentas se distribuyen a cada uno de los miembros que conforman la entidad para entrar a formar parte de su propia renta como persona física. Las rentas atribuidas tienen la naturaleza derivada de la fuente de donde procedan. Esta regulación da lugar también a que las entidades en régimen de atribución de

36. DELGADO GARCÍA, A. M.; OLIVER CUELLO, R. (2008:71). "Nuevas tendencias en la política de fomento de las actividades de investigación…", *op. cit.*

rentas les puedan ser de aplicación los beneficios tributarios establecidos en el IS, siempre que determine su renta a través del régimen de estimación directa[37].

2.3.3. Becas de investigación exentas

El último de los beneficios fiscales al que haremos referencia y que afectan o pudieran afectar a las actividades de I+D+i que se encuentran en la LIRPF son las becas de investigación exentas de tributar en concepto de ese impuesto. El artículo 7 j) de dicha norma prevé que estarán exentas:

— *"Las becas públicas, las becas concedidas por las entidades sin fines lucrativos a las que sea de aplicación el régimen especial regulado en el Título II de la Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo, y las becas concedidas por las fundaciones bancarias reguladas en el Título II de la Ley 26/2013, de 27 de diciembre, de cajas de ahorros y fundaciones bancarias en el desarrollo de su actividad de obra social, percibidas para cursar estudios reglados, tanto en España como en el extranjero, en todos los niveles y grados del sistema educativo, en los términos que reglamentariamente se establezcan".*
(…)
— *"Las becas públicas y las concedidas por las entidades sin fines lucrativos y fundaciones bancarias mencionadas anteriormente para investigación en el ámbito descrito por el Real Decreto 63/2006, de 27 de enero, por el que se aprueba el Estatuto del personal investigador en formación, así como las otorgadas por aquellas con fines de investigación a los funcionarios y demás personal al servicio de las Administraciones públicas y al personal docente e investigador de las universidades".*

En relación con aquellas disposiciones, el Real Decreto 439/2007, de 30 de marzo, por el que se aprueba el Reglamento del Impuesto sobre la Renta de las Personas Físicas y se modifica el Reglamento de Planes y Fondos de Pensiones, aprobado por Real Decreto 304/2004, de 20 de febrero, en su artículo 2 regula que estarán exentas las becas públicas percibidas para cursar estudios reglados cuando "*la concesión se ajuste a los principios de mérito y capacidad, generalidad y no discriminación en las condiciones de acceso y publicidad de la convocatoria. En ningún caso estarán exentas las ayudas para el estudio concedidas por un Ente Público en las que los destinatarios sean exclusiva o fundamental-*

37. Para determinar el resultado de las actividades económicas realizadas a través de entidades en atribución de rentas, el importe neto de la cifra de negocio tendrá en cuenta exclusivamente el conjunto de actividades económicas ejercidas por dichas entidades, sin computar las rentas de origen o rentas individuales de los socios, comuneros, partícipes. Ello pone de relieve de que a pesar de que se trate de entidades sin personalidad jurídica, constituye una economía autónoma.

mente sus trabajadores o sus cónyuges o parientes, en línea directa o colateral, consanguínea o por afinidad, hasta el tercer grado inclusive, de los mismos".

En el caso de las becas para estudios que sean otorgadas por entidades sin fines lucrativos a las que les sea de aplicación el régimen especial regulado en el título II de la Ley 49/2002, de 23 de diciembre, de régimen fiscal de las entidades sin fines lucrativos y de los incentivos fiscales al mecenazgo, o por fundaciones bancarias reguladas en el título II de la Ley 26/2013, de 27 de diciembre, de cajas de ahorros y fundaciones bancarias en el desarrollo de su actividad de obra social, estarán exentas siempre y cuando cumplan con los siguientes requisitos:

— *"Que los destinatarios sean colectividades genéricas de personas, sin que pueda establecerse limitación alguna respecto de los mismos por razones ajenas a la propia naturaleza de los estudios a realizar y las actividades propias de su objeto o finalidad estatutaria".*
— *"Que el anuncio de la Convocatoria se publique en el Boletín Oficial del Estado o de la comunidad autónoma y, bien en un periódico de gran circulación nacional, bien en la página web de la entidad".*
— *"Que la adjudicación se lleve a cabo en régimen de concurrencia competitiva".*

Asimismo, no tendrán que tributar en concepto de IRPF las becas para investigación en el ámbito descrito por el Real Decreto 63/2006, de 27 de enero, por el que se aprueba el Estatuto del personal investigador en formación, "*siempre y cuando el programa de ayudas a la investigación haya sido reconocido e inscrito en el Registro general de programas de ayudas a la investigación*" (…). "*En ningún caso tendrán la consideración de beca las cantidades satisfechas en el marco de un contrato laboral*".

De igual forma, las bases de la convocatoria deberán disponer como requisito o mérito y de manera expresa que los destinatarios sean funcionarios, personal al servicio de las Administraciones Públicas y personal docente e investigador de las Universidades. También deberán ajustarse a los requisitos que acabamos de mencionar las becas convocadas por entidades sin fines lucrativos a las que sea de aplicación el régimen especial regulado en el título II de la Ley 49/2002 o por fundaciones bancarias reguladas en el título II de la Ley 26/2013 en el desarrollo de su actividad de obra social.

Asimismo, el precepto citado prevé que el "*importe de la beca exento para cursar estudios reglados alcanzará los costes de matrícula, o cantidades satisfechas por un concepto equivalente para poder cursar tales estudios, y de seguro de accidentes corporales y asistencia sanitaria del que sea beneficiario el becario y, en su caso, el cónyuge e hijo del becario siempre que no posean cobertura de la Seguridad Social, así como una dotación económica máxima, con carácter general, de 6.000 euros anuales*". Sin embargo, podrá elevarse de los 6.000 euros hasta los 18.000 euros anuales "*cuando la dotación económica tenga por objeto compensar gastos de transporte y alojamiento para la realización de estudios reglados del sistema educativo, hasta el nivel de máster incluido o equivalente.*

Cuando se trate de estudios en el extranjero dicho importe ascenderá a 21.000 euros anuales". Por su parte, si se trata de estudios de doctorado la dotación económica exenta será de 21.000 euros o 24. 600 euros anuales, em el caso de este último monto cuando los estudios se realicen en el extranjero.

> "En el supuesto de becas para investigación gozará de exención la dotación económica derivada del programa de ayuda del que sea beneficiario el contribuyente".

Por último, las becas que se concedan para la realización de estudios de doctorado y para investigación el importe exento estará constituido, además por:

— *"Las ayudas complementarias que tengan por objeto compensar los gastos de locomoción, manutención y estancia derivados de la asistencia a foros y reuniones científicas".*
— *"La realización de estancias temporales en universidades y centros de investigación distintos a los de su adscripción para completar, en ambos casos, la formación investigadora del becario".*

3. INSTRUMENTO PARA EL IMPULSO DE ACTIVIDADES I+D+i ALTERNATIVO AL FISCAL

Puede leerse en el preámbulo de la LIRPF que *"la deducción por actividades de investigación y desarrollo e innovación tecnológica, cuya aplicación se mantiene otros cinco años, conservando esta deducción la estructura actual si bien se reducen los porcentajes de deducción en la misma proporción en que se minoran los tipos de gravamen, al objeto de que las empresas puedan adaptar sus políticas de inversión al nuevo marco de ayudas públicas de impulso a estas actividades, dado que se introduce un nuevo instrumento, alternativo al fiscal, incentivador de estas mismas actividades, consistente en una bonificación de las cotizaciones a la Seguridad Social a favor del personal investigador".*

En efecto, el Real Decreto 475/2014, de 13 de junio, sobre bonificaciones en la cotización a la Seguridad Social del personal investigado[38], regula en su artículo 2 que:

— *"La contratación indefinida, por empresas dedicadas a actividades de investigación y desarrollo e innovación tecnológica, entendiendo como*

38. Anteriormente, Real Decreto 278/2007, de 23 de febrero, desarrolla este régimen de bonificaciones en la cotización a la Seguridad Social respecto del personal investigador. Sobre este instrumento introducido en el Real Decreto 278/2007 en el preámbulo de esta norma se dispone que "*este nuevo incentivo a la investigación ha demostrado un buen funcionamiento en otros países de la Unión Europea en que ya se está aplicando y, además, presenta otras ventajas frente al incentivo de naturaleza tributaria, ya que tiene un efecto más directo y favorece la realización de la actividad y la contratación de trabajadores en España*".

tales las actividades descritas respectivamente en el artículo 34.1.a) y 35.2.a) de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades, de personal para la realización con carácter exclusivo y por la totalidad de su tiempo de trabajo dará lugar, durante un máximo de tres años, a una bonificación del 40 por 100 sobre la cuota empresarial a la seguridad social por contingencias comunes. La contratación de personas investigadoras jóvenes, entendiendo por tales aquellas que sean menores de 30 años, y la contratación de mujeres investigadoras dará, respectivamente, derecho a una bonificación adicional de un 5 por 100, siendo estas acumulables, en su caso, entre sí".

— *"Con relación a la exclusividad y al cómputo de la totalidad del tiempo de trabajo, se admitirá que hasta un 15 por ciento del tiempo dedicado a tareas de formación, docencia, divulgación o similares, compute como dedicación exclusiva a actividades de I+D o iT"*[39].

Por su parte, el artículo 6 del citado Real Decreto 475/2014 se refiere a la compatibilidad de estas bonificaciones a la Seguridad Social respecto del personal investigador y la deducción en las cuotas tributarias del Impuesto de Sociedades. En tal sentido, estipula el precepto que:

— "*La bonificación en la cotización (…) será plenamente compatible con la aplicación del régimen de deducción por actividades de investigación y desarrollo e innovación tecnológica establecida en el artículo 35"* de la LIS *"únicamente para las pequeñas y medianas empresas (en adelante, PYMES) intensivas en I+D+i reconocidas como tal mediante el sello oficial de «PYME innovadora» y que por ello figuren en el Registro que, a tal efecto, gestionará el Ministerio de Economía y Competitividad".*

Asimismo, se entenderá que una entidad tiene la consideración de PYME intensiva en I+D+i cuando reúna alguno de los siguientes requisitos[40]:

— *"Cuando haya recibido financiación pública en los últimos tres años, sin haber sufrido revocación por incorrecta o insuficiente ejecución de la actividad financiada, a través de:*
  - *Convocatorias públicas en el marco del VI Plan Nacional de Investigación Científica, Desarrollo e Innovación Tecnológica o del Plan Estatal de Investigación Científica y Técnica y de Innovación.*
  - *Ayudas para la realización de proyectos de I+D+i, del Centro para el Desarrollo Tecnológico Industrial.*

39. *"Se considerarán actividades de I+D e iT las definidas como tales en el artículo 35 de la Ley 27/2014, de 27 de noviembre, del Impuesto sobre Sociedades"* (artículo 2.3 Real Decreto 475/2014).

40. Definición contenida en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo, sobre la definición de microempresas, pequeñas y medianas empresas.

  - *3.º Convocatorias del 7.º Programa Marco de I+D+i o del Programa Horizonte 2020, de la Unión Europea".*
- — *"Cuando haya demostrado su carácter innovador, mediante su propia actividad:*
  - *Por disponer de una patente propia en explotación en un período no superior a cinco años anterior al ejercicio del derecho de bonificación.*
  - *Por haber obtenido, en los tres años anteriores al ejercicio del derecho de bonificación, un informe motivado vinculante positivo a efectos de aplicación de la deducción a la que se refiere el artículo 35"* de la LIS.
- — *"Cuando haya demostrado su capacidad de innovación, mediante alguna de las siguientes certificaciones oficiales reconocidas por el Ministerio de Economía y Competitividad":*
  - Joven Empresa Innovadora, según la Especificación AENOR EA0043.
  - Pequeña o microempresa innovadora, según la Especificación AENOR EA0047.
  - Certificación conforme a la norma UNE 166.002 "Sistemas de gestión de la I+D+i".

El resto de las empresas o entidades que no tengan la condición de PYMES Innovadoras podrán aplicar la bonificación en la cuota empresarial a la Seguridad Social junto con la deducción en la cuota íntegra del IS siempre que no se trate del mismo investigador. En estos casos, el legislador permite a las empresas optar por aplicar la bonificación en la cotización a la Seguridad Social respecto del personal investigador o la deducción por los costes de dicho personal en los proyectos en los que participe y en los que realice actividades de I+D+i. *"Será compatible por una misma empresa y en un mismo proyecto, la aplicación de bonificaciones sobre investigadores junto con la de deducciones por otros investigadores por los que la empresa, en ese caso, desee deducirse".*

Por último, la Agencia Estatal de Administración Tributaria (AEAT), en el ejercicio de sus facultades de control en materia de deducciones fiscales, comprobará el cumplimiento de la condición de «PYME Innovadora» para que las empresas o entidades puedan aplicar los beneficios fiscales por realización de actividades de investigación, desarrollo e innovación tecnológica.

De todo lo anterior debemos destacar que esta medida incentivadora para actividades de I+D+i se concreta en una:

— Bonificación equivale al 40 por ciento de las cotizaciones por contingencias comunes a cargo del empresario.
— Bonificación incompatible con la aplicación del régimen de deducción por actividades de investigación y desarrollo e innovación tecnológica

que regula el artículo 35 de la LIS[41]. Excepto cuando se trate de una empresa que tenga la condición del PYME Innovadora[42].

— Se tiene derecho a la aplicación de la bonificación en los casos de contratos de carácter indefinido, así como en los supuestos de contratación temporal.

4. CONSIDERACIONES FINALES

Primera: No existe una acepción legal de actividades de I+D+i, para ello es necesario remitirse a la LIS que regula un concepto limitado y que, junto con la interpretación restringida por parte de la Administración, confieren poca certeza al obligado tributario en cuanto a la obtención y cuantía de los beneficios fiscales.

Segunda: Los principales incentivos fiscales a la I+D+i se encuentran regulados en la imposición directa y se conforman, principalmente, por deducciones aplicables en la base imponible y en la cuota íntegra del IS y el IRPF, en el caso de este último tributo, solo serán aplicables si se determinan los rendimientos de las actividades económicas por el método de estimación directa normal.

Tercera: No se justifica la diferencia de trato fiscal entre actividades I+D e iT cuyos porcentajes de aplicación en la deducción de la cuota íntegra varían considerablemente según se trate de un tipo u otro.

Cuarta: La incompatibilidad de la bonificación en la cotización de la Seguridad Social con la deducción en la cuota íntegra resuelta incongruente si se tiene en cuenta que en el caso de la segunda afecta a toda la actividad económica.

Quinta: Las personas físicas que desarrollen actividades I+D+i no podrán aplicar de manera conjunta la deducción en la cuota íntegra y la bonificación a la Seguridad Social únicamente permitido a las PYMES innovadoras, lo que se traduce en un trato desigual por razón de organización social.

BIBLIOGRAFÍA

ALONSO ANTÓN, C. (2016). "Deducción en el IS por actividades de investigación y desarrollo. Alcance del informe de la Administración", *Revista Aranzadi Doctrinal*, núm. 8, parte Jurisprudencia. https://acortar.link/2qAm5q:1-3.

BELDA, I. (2023). "Metaverso y NFT, nuevos retos tecnológicos en la imposición indirecta e internacional", *Revista de Internet, Derecho y Política,* núm.37. https://acortar.link/ANodQS: 1-12.

41. *Vid. supra*., 2.2.4. "Deducción en la cuota por la realización de actividades I+D+i".

42. La Orden ECC/1087/2015, de 5 de junio, regula la obtención del sello de "Pyme innovadora" y el funcionamiento del Registro de la Pequeña y Mediana Empresa Innovadora. Sobre los requisitos para obtener el sello de PYME Innovadora véase: https://www.ciencia.gob.es/InfoGeneralPortal/documento/47c073ee-ee3b-4c27-9c8d-496dd03a1c26.

— (2023). "A vueltas con las deducciones por innovación tecnológica y el software en el Impuesto sobre Sociedades", *Quincena Fiscal*, núm. 7, parte Estudios. Disponible en: https://acortar.link/6xS3pW. Consultado 15/03/2024: 1-16.

CALVO VÉRGEZ, J. (2010) "La incidencia del lugar de realización en la aplicación de la deducción en concepto de I+D+i dentro del Impuesto sobre Sociedades a la luz de la reciente jurisprudencia del Tribunal de Justicia de la Unión Europea", *Revista Aranzadi Unión Europea*, núm. 11, 2010 parte Crónica. Disponible en https://acortar.link/ilw4p5: 1-7.

Comité de Personas Expertas (2022). *Libro Blanco sobre la Reforma Tributaria*. Madrid: Ministerio de Hacienda y Función Pública. https://acortar.link/hj9kzU.

DELGADO GARCÍA, A. M.; OLIVER CUELLO, R. (2008). "Nuevas tendencias en la política de fomento de las actividades de investigación, desarrollo e innovación tecnológica", *Crónica Tributaria,* núm. 128:1-24. 57-80.

ECHEVERRÍA ECHEVERRÍA, G. (2005). *Beneficios tributarios para la PYME en el Impuesto sobre Sociedades,* Granada, Editorial Universitario:178-179.

FABRA VALLS, M.(2003). "Deducción por actividades de I+D+I: principales aspectos de su régimen jurídico", *Jurisprudencia Tributaria*, núm. 11. https://acortar.link/oHzMdt: 1-22.

FABRA VALLS, M., FALCHI P. (2017). "Los incentivos fiscales para el fomento de la innovación empresarial en España e Italia", *Revista Quincena Fiscal*, núm. 9, parte estudio. https://acortar.link/6ovcCt.:1-56.

GIL GARCÍA, E. (2018). "La seguridad jurídica en la aplicación de los incentivos a la I+D+i.", *Quincena Fiscal*, núm. 17, parte Estudios. https://acortar.link/fGzUPa:1-31.

MAGRANER MORENO, F. J. (2006). "Aspectos relevantes para la calificación de actividades y determinación de la base en las deducciones de I+D e IT", *Tribuna Fiscal*, Ciss, núm. 188:8-15.

MARTÍNEZ-CARRASCO PIGNATELLI, J. M. (2015). "Deducciones en la cuota tributaria del Impuesto sobre Sociedades", *Quincena Fiscal, núm.* 21/2015. https://acortar.link/mTnfct:1-22.

NIETO MONTERO, J. J. (2000). "Régimen fiscal de la creación e inversión en nuevas tecnologías", *Derecho Tributario e informática*, Tirant Lo Blanch, Valencia: 117-130.

QUIRÓS GÓMEZ, J. (2021). "Incentivos fiscales a la investigación, desarrollo e innovación tecnológica: los informes motivados", *Quincena Fiscal*, núm. 21. https://acortar.link/pT6FBW: 1-21.

RIVAS, S. C., (2007). "Los incentivos fiscales a la innovación en el Impuesto sobre Sociedades español: historia y actualidad", *Revista de Contabilidad y Tributación,* Centro de Estudios Financiero, núm. 39. https://acortar.link/ZmByut: 29-86.

RIVAS SÁNCHEZ, C. y ORDÓÑEZ DE HARO, C. (2004). "Régimen tributario de las actividades de investigación y desarrollo e innovación tecnológica en el Impuesto sobre Sociedades", *Revista Técnica Tributaria*, núm. 66: 35 y ss.

III. Empresa y Administración tributaria

PERFILES DE RIESGO FISCAL CREADOS POR INTELIGENCIA ARTIFICIAL

Miguel Ángel Sánchez Huete
Profesor titular de Derecho financiero y tributario
Universitat Autònoma de Barcelona

ABSTRACT:
The purpose of this chapter is to analyse the risk profiles used by the tax administration where AI seems to be very present. The questions addressed start by defining what a tax risk profile is and what its functions and main legal effects are. Delimiting the idea of a profile and its operability requires differentiating the two moments that integrate it: its creation and the decision made about it. The creation of a risk profile involves defining the risk prevention model from which it starts and indicating who is responsible for carrying it out. The administrative decision made about the profile must respect specific legal guarantees, and here the basic questions are where they are regulated and what they consist of. The normal intervention of AI in both processes requires that the guarantees and precautions be in accordance with the uniqueness that such technologies integrate, and here the regulatory absences are notable.

Keywords: tax fraud, artificial intelligence, automated decision, tax risk.

Palabras clave: fraude tributario, inteligencia artificial, decisión automatizada, riesgo fiscal.

SUMARIO:

FICIAL. 2.1.El riesgo del perfilado mediante IA. 2.2.El riesgo al uso de la IA por la Administración tributaria. 3. PERFILES DE RIESGO COMO DECISION AUTOMATIZADA. 3.1. La prohibición de decisiones automatizadas. 3.1.El Reglamento de IA y el ámbito tributario. 4. CONCLUSIONES.

Las Administraciones tributarias están utilizando cada vez más la Inteligencia Artificial (en adelante IA) en sus tareas de aplicación de los tributos. Según la OCDE efectúan un uso creciente por su capacidad para manejar grandes conjuntos de datos, por su potencialidad a la hora de gestionar los recursos público, y por su eficiencia en la detección de riesgos que afectan a la recaudación (OCDE, 2022). En este contexto la Administración tributaria española resulta una de las más avanzadas en el empleo de medios y sistemas informáticos para el control del cumplimiento fiscal.

La IA aparece muy presente en las tareas de prevención y represión del fraude pues permite organizar, cruzar, modelizar y clasificar automáticamente la información disponible para delimitar áreas de riesgo y detectar incumplimientos. Sistemas como ZÚJAR, TESEO, INEX, INTER, DÉDALO, PROMETEO o GENIO permiten tratar la información de manera automatizada para detectar inconsistencias[1]. Y aquí la importancia de los perfiles de riesgo fiscal resulta evidente para hallar patrones de incumplimiento y desarrollar estrategias que permitan prevenir las conductas lesivas. Pues la IA permite, sobre la base de múltiples criterios, el realizar cálculos rápidos y eficientes que permiten predicciones más fiables.

Pero realmente ¿qué sabemos de los perfiles de riesgo tributario? ¿cuál es el régimen jurídico que pauta dichos usos? De ahí que el objeto del presente capitulo sea el análisis de los perfiles de riesgo empleados por la Administración tributaria en donde la IA está muy presente. Los interrogantes que se abordan parten de delimitar qué es un perfil de riesgo tributario y cuáles son sus funciones y principales efectos jurídicos. Para llevar a cabo tal propósito es preciso delimitar la idea de perfil diferenciando los dos momentos que lo integran: su creación y la decisión que sobre el mismo se toma. Son momentos diversos que requieren de un tratamiento diferencial. De un lado, la creación de un perfil de riesgo supone acotar el modelo de prevención del riesgo de que se parte delimitando los comportamientos que lo integran. De otro lado, las decisiones administrativas que se toman sobre el perfil han de respetar garantías jurídicas, y aquí los interrogantes básicos es dónde se regulan y en qué consisten.

1. Ver programas y aplicaciones usados por la Agencian Estatal de la Administración Tributaria en Res 825/2019, 13 de febrero del Consejo de Transparencia y Buen Gobierno.

1. LOS PERFILES DE RIESGO FISCAL

El perfil de riesgo fiscal requiere acotar algunas ideas previas que, más que conformar un concepto cerrado y definido, permita introducirnos en aspectos relacionados con su función y efectos jurídicos.

1.1. Ideas previas

Acercarnos a la idea de perfil de riesgo fiscal exige aproximarnos separadamente a cada uno de los conceptos que integran su mención para una mejor comprensión conjunta.

Perfil, es una expresión que se asocia a la idea de contorno, o de postura que solo deja ver una de las mitades del cuerpo, a decir del diccionario[2]. Se trata así del conocimiento de un conjunto de rasgos peculiares que permiten caracterizar a alguien o a algo. Ahora bien, el perfil es conocimiento —ya sea personal o negocial— parcial e intuido. Es un saber imperfecto. Con él se delimita una serie de aspectos o características que normalmente acompañan a identificar una realidad, no la identifican en sí misma. Tal carácter apunta ya los eventuales efectos asociados a tal figura: el perfil no permite identificar con plenitud una realidad, de ahí que no pueda constituir la prueba de su existencia.

Connotar al perfil como de riesgo supone añadir a la anterior idea el poner en peligro, la posibilidad de lesionar derechos o interés legítimos de terceros. Evidencia así la función de prevención que posee; el perfil de riesgo acota comportamientos de peligro probable o posible con el fin de evitar un daño.

Adicionar a la anterior idea de riesgo el carácter fiscal genera no pocas dudas. Riesgo fiscal, y sin perjuicio de lo que señalaremos, exige concretar la proximidad de la lesión a que apunta. El riesgo fiscal no puede ser inespecífico ni indiscriminado. Es preciso delimitar cuál es el daño que se ha de evitar, pues existen conductas diversas que pueden ser lícitas e ilícitas (incumplimiento, conflicto en la aplicación de la norma tributaria, evasión) y que precisan tratos diferenciados.

En el ordenamiento español no existe una definición de perfil, y mucho menos de los perfiles de riesgo fiscal utilizando IA. Ahora bien, en la medida que para la creación de estos se utilizan procedimientos automatizados, resulta de interés la definición efectuada por el Reglamento (UE) 2016/679 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 (en adelante Reglamento General de Datos). En tal regulación habla de perfil como una forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, si-

2. Diccionario de la Real Academia Española, consultado en web https://dle.rae.es/perfil?m=form

tuación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos (art. 4.4.). Tal concepto alude a que han de cumplir tres requisitos: el resultar una forma automatizada de tratamiento, el efectuarse sobre datos de carácter personal, y el suponer una evaluación de aspectos relativos a la persona física.

A los anteriores requisitos se ha de remarcar su finalidad de predecir el comportamiento de la persona. En las Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679 se afirma que "La elaboración de perfiles es un procedimiento que puede implicar una serie de deducciones estadísticas. Suele usarse para hacer predicciones sobre personas, utilizando datos de distintas fuentes para inferir algo sobre un individuo, sobre la base de las cualidades de otros que parecen similares estadísticamente." En el proceso de elaboración de perfiles suelen existir tres fases distintas: la recogida de datos; el análisis automatizado para identificar correlaciones, y la aplicación de la correlación a una persona para identificar características de comportamientos presentes o futuros (Grupo de trabajo, 2017).

Ahora bien, la definición del Reglamento General de Datos es a los únicos efectos de la aplicación de dicha norma. No pretende ser omnicomprensiva para aprehender el fenómeno, sino útil para aplicar dicho Reglamento. Dicho carácter se aprecia no sólo de la dicción del precepto sino por el hecho de que el perfil se asocia exclusivamente a la persona física y no a la jurídica. No obstante, es un concepto indiciario valido para aprehender las características y elementos que integra, en el bien entendido que precisa de una visión que incluya la realidad de las personas jurídicas, una contextualización a la realidad tributaria, y el uso administrativo el mismo. Desde esta perspectiva podríamos acotar la idea de perfil de riesgo fiscal como el tratamiento automatizado llevado a cabo por la Administración tributaria de datos personales con transcendencia tributaria que permiten evaluar aspectos asociados a su comportamiento tributario a fin de analizar y predecir aspectos asociados, principalmente, a su rendimiento, situación económica, relaciones o comportamiento en la media que pueda suponer un peligro para la recaudación.

Pero el perfil es algo más que un conjunto de características que delimitan de forma indiciaria la identidad de una persona. Sobre el perfil se toman decisiones y ésta es una dimensión diversa, si bien normalmente asociada, que precisa garantías específicas. Así pues, operar sobre los perfiles demanda dos tipos de procesos; exige un proceso inductivo para crear dichos perfiles, y un proceso deductivo en su aplicación.

El proceso inductivo se lleva a cabo a la hora de crear patrones de conductas peligrosas, tipologías de lo que se entiende por tal. Se parte de analizar conductas, tendencias y modelos para llegar a configurar el perfil. A la hora de su aplicación se efectúa un proceso deductivo en donde se conjugan los criterios que conforman el patrón con la realidad concreta a considerar, en último extremo con la conducta del ciudadano.

Ambos procesos comportan tareas complejas al entrañar decisiones previas que han de ser conocidas para poder ser controladas. Son dos momentos sepa-

rables, pero necesariamente consecutivos, pues la creación de perfiles sólo se explica para su aplicación a la realidad concreta e individual. La importancia de diferenciar estos dos momentos radica en que el régimen jurídico aplicable es diferente. En uno, la Administración tiene que velar por la corrección técnica de la determinación que supone. En este sentido ha de responder a las cuestiones de quien aprueba el aplicativo informático, el rango de la norma que lo efectúa, y de qué manera se contemplan los controles. El segundo, supone concretar una aplicación individualizada, entraña una decisión que, si se efectúa de forma automatizada y respecto de personas físicas, está sujeta a concretas garantías.

Pero antes de proceder a tales análisis, objeto principal de estas páginas, resulta oportuno acotar los diversos usos y funciones asociadas a los perfiles de riesgo en el ámbito tributario.

1.2. Funciones

La OCDE ubica las funciones atribuidas al perfilado dentro de los procesos informáticos de análisis de datos. El análisis de datos, continua esta entidad, implica la detección, interpretación y comunicación de patrones significativos en los datos. Este campo abarca desde la inteligencia de negocio hasta el análisis de Big Data y de redes. En el contexto de la administración tributaria el análisis de datos se utiliza para diversas finalidades prácticas, como la elaboración de informes, la modelización de riesgos, el análisis predictivo y prescriptivo, y otras variantes que permiten obtener información valiosa.

Atendiendo a lo anterior las tareas de perfilado se encontrarían dentro del análisis de datos que afectaría principalmente al ámbito del cumplimiento. En este contexto los procesos de análisis parten de considerar los datos como un activo vital a explotar, y no como mero subproducto de los procesos tributarios. Ello precisa de un uso de datos de alta calidad para lo cual se requiere una inversión en personal y tecnología (OCDE, 2023).

Y en el ordenamiento español ¿para qué se utilizan los perfiles? Los perfiles de riesgo, en la línea de lo señalado, poseen dos claras funciones. La primera, ayudar a descubrir actos lesivos y, la segunda, previene la realización de futuras lesiones. Son facetas diversas, en una se mira al pasado, y en la otra se mira al futuro, si bien con los hechos del pasado.

De un lado, se busca el descubrimiento de las ocultaciones e incumplimientos tributarios en los ámbitos de riesgo acotados. Con el perfil de riesgo se pretende detectar una irregularidad ya originada. En esta función, y desde una perspectiva de los derechos y garantías aplicables, se pone de relieve un posible derecho a conocer los perfiles y saber qué efectos posee en aras de ejercer una defensa adecuada, así como a corregir usos arbitrarios que pudieran efectuarse.

De otro lado, con los perfiles de riesgo se busca el prevenir la realización futura de comportamientos lesivos. En el empleo de técnicas de IA las funciones de prevención de riesgos resultan casi connaturales, y acostumbran a referirse a ellas como tareas "predictivas". Esta designación no resulta adecuada al sentido

y función jurídica atribuido a los perfiles; con éstos no se sabe que va a suceder de manera determinista. No se predice que acaecerá una realidad, sino se estima como probable[3]. El perfil fruto de aplicar la IA no predice el futuro, no dice que tenga que ser, sino que es una mera probabilidad. Este análisis de previsión utiliza los datos históricos, información estadística, también pueden entrenarse con nuevos datos fruto de aprendizaje posterior, pero se trata de información no necesariamente individualizada referida al sujeto que se aplica.

Junto a los anteriores análisis de probabilidad existen los análisis prescriptivos que pretende provocar las acciones de la ciudadanía[4]. Se trata de cómo influir en los acontecimientos para que ocurran de manera más beneficiosa para el interés en cuestión, en nuestro caso, el cumplimiento normativo. Ambas dimensiones de análisis, aun siendo diferenciadas, suponen estrategias de planificación, de anticipación a los riesgos y de diseño de estrategias para evitarlos. Poseen una cierta lógica secuencial si bien difieren en su objeto. Mientras que el análisis predictivo se interroga sobre la probabilidad de los eventos, la prescriptiva estudia las acciones más acertadas considerando los eventos futuros perfilados.

Estos análisis prescriptivos se asocian a políticas preventivas que pretenden corregir antes de que se origine el comportamiento no deseado, cualquiera que este sea, ya se inscriba en retraso, incumplimiento, o incumplimiento infractor. Trata así de prevenir: a) errores —conocer erróneamente—, b)olvidos —desconocer—, c)avisos de que la Administración conoce, d)apercibimientos leves sobre la conducta seguida[5]. En la actualidad aparece muy presente en algunas

3. A este respecto predecir, según el diccionario de la Real Academia de la Lengua alude a "anunciar por revelación, conocimiento fundado, intuición o conjetura algo que ha de suceder". Diccionario de la Real Academia Española, consultado en web https://dle.rae.es/predecir?m=form

4. Bajo la designación de behavioural insights la Agencia tributaria española afirma su utilización destacando su aplicación en el área de Gestión Tributaria, en el ámbito del Impuesto sobre la Renta de las Personas Físicas (IRPF), avisando a aquellos contribuyentes que, cuando modifican algunos datos fiscales relativos a los rendimientos del trabajo suministrados en su declaración de Renta, pueden cometer errores en la presentación. También en las áreas de Gestión, Inspección, Recaudación y Aduanas se analizan las posibilidades de una mejora y simplificación del literal de los documentos que se emiten con más frecuencia, de manera que éstos sean más comprensibles y sencillos para sus destinatarios. Ver https://shre.ink/DO26

5. Son frecuentes los denominados acicates o nutges en su terminología inglesa. Se trata de incentivos, guías de comportamiento, facilitadores de diverso tipo sin que implique el uso de coacción, sanción. ni estímulo fiscal al uso relacionado con políticas de fomento. Supone un estímulo, un "empujar suavemente" un "golpecito" a fin de avisar o amonestar suavemente al otro. Con ello se trata de incrementar el grado de cumplimiento voluntario animando a ello de manera expresa, frecuentemente mediante cartas o remitiendo avisos. Ver a este respecto Dictamen del Comité Económico y Social Europeo sobre «Integrar los nudges en las políticas europeas» (Dictamen de iniciativa) (2017/C 075/05) Ponente: Thierry Libaert, También ver número monográfico de la revista Gestión y análisis de políticas públicas sobre los nudges y el diseño conductual de políticas públicas de marzo de 2021 y Cabrales, 2021. También Moreu, 2018.

iniciativas de la Administración tributaria como las cartas-recordatorio o el programa "Le llamamos"[6].

1.3. Efectos jurídicos

Los perfiles de riesgo tributario efectuados sobre la base de pronósticos y previsiones no son novedosos en sí, lo que resulta novedoso es la precisión que permite el uso de la IA por la ingente información que gestiona. En tal contexto, y valorando los intereses concurrentes, más que una negación rotunda a su aplicación, a su admisibilidad, la cuestión radica en ¿qué efectos poseen dichas previsiones? ¿qué consecuencias jurídicas se originan? Y también de forma correlativa ¿con qué garantías jurídicas se cuenta?

En un primer análisis la eficacia jurídica de un perfil de riesgo no puede ser constitutiva de una realidad que nunca fue. No resulta prueba, ni directa ni indirecta de los hechos que no han tenido lugar. Pero ¿puede ser indicio?

En relación con los efectos jurídicos cabe plantear tres consideraciones generales:

En primer lugar, el abuso de los perfiles puede llevar a establecer prejuicios y estigmas respecto de concretos grupos sociales abocando a una "sociedad etiquetada", en donde se predetermine comportamientos sobre la base de otros previos, propios o ajenos. También el etiquetado sistemático e ilógico de colectivos, por ejemplo, los empresarios autónomos, o las sociedades inmobiliarias, cuando supone una consideración negativa puede conllevar alterar el principio general que presume la buena fe.

En segundo lugar, hay que considerar que los perfiles de riesgo poseen peculiaridades que los hacen falibles. De un lado, parten en buena medida de datos que han sucedido lo que lleva aparejado la problemática de ¿hasta cuándo nos vemos afectados por el pasado? Ya que pueden suponer unos antecedentes indelebles. Imaginemos sobre todo los datos que provengan de delitos y sanciones impuestas; la inclusión de tal valoración a la hora de configurar perfiles de riesgo puede constituir una pervivencia de antecedentes punitivos, o una especie de sanción basada en una peligrosidad indeleble. Nuevamente dichas valoraciones negativas pondrían en tela de juicio el principio de buena fe imperante en el ordenamiento jurídico[7].

De otro lado, no todos los datos usados son relevantes ni todas las fuentes de información poseen la misma fiabilidad. Los datos que sirven para la aplicación de los tributos han de poseer la transcendencia tributaria necesaria y, además, han de ser obtenidos de forma lícita con las garantías legales para ser es-

6. Ver https://sede.agenciatributaria.gob.es/Sede/ayuda/consultas-informaticas/renta-ayuda-tecnica/cita-previa-renta.html

7. De manera más dubitativa a la que sustentamos se posiciona Martín al hablar de los sesgos en relación con los datos (Martín, 2022).

grimidos en contra del interesado. En este sentido la eficacia jurídica del perfil de riesgo viene asociado a su trasparecía y a las posibilidades de verificar los datos sobre los que opera. En la medida que tales datos se consideran generalmente reservados, como indicaremos, la eficacia predicable de tal instrumento ha de ser reducida.

En tercer lugar, los perfiles difícilmente pueden predeterminar efectos jurídicos individualizados porque no conocen la realidad concreta, sino la genérica y, normalmente, estadística conformada con una pluralidad de comportamientos. El riesgo asignado no depende exclusivamente de la concreta conducta de aquel a quien se aplica, por lo que no puede decidirse sobre una cuestión individualizada considerando el comportamiento de otros.

En definitiva, el perfil supone un juicio genérico no susceptible de constituir la prueba de una situación individualizada o su decisión. Pues los riesgos que acotan el perfil se delimitan también por las conductas de otros, no sólo de aquel a quien se le aplica, y no podemos responder por actos ajenos.

El perfil de riesgo no puede decidir directa o indirectamente un procedimiento, pero tal aspecto no le niega eficacia jurídica como indicio, necesitando ser corroborado por otros elementos de prueba. El indicio resulta una prueba que posee una cierta indeterminación en las circunstancias, por lo que puede considerarse una prueba abierta (Pastor, 2003). En su ideación acostumbra a relacionarse con sospechas y conjeturas[8]. Ahora bien, en todo caso, los indicios requieren una apariencia de verosimilitud y razonabilidad, además de que sean plurales y concordantes para ser tenidos en cuenta[9].

El perfil de riesgo es un indicio relevante a la hora de determinar el inicio de procedimientos de inspección, desplegando unas consecuencias importantes dado los deberes de colaboración e información que tal procedimiento conlleva[10]. En tal sentido el perfil de riesgo si bien no destruye la presunción de

8. A este respecto la STS 01-12-1989 con cita de la STS 499/2003 de 04 de abril diferencia entre sospecha conjetura e indicio. La sospecha, que consistiría en la aprehensión o imaginación de una cosa por conjeturas fundadas en apariencias o visos de verdad. La conjetura, que sería el juicio que, con ciertas probabilidades de acierto, se forman de las cosas o acaecimientos por las señales que se ven u observan y, finalmente, el indicio, que es la acción o señal que da a conocer lo oculto, en virtud de las circunstancias, que concurren en un hecho, dándole carácter de verosimilitud.

9. La sentencia de la Sala Segunda del Tribunal Supremo de 16-07-2002 (RG 3507/2000) y la sentencia del Tribunal Supremo de 08-05-2003 (RG 708/2002) en relación con los requisitos aluden a: 1. Los indicios han de estar acreditados por prueba directa, con lo que se trata de evitar los riesgos inherentes a la admisión de una concatenación de indicios que aumentaría los riesgos en la valoración. 2. Los indicios tienen que estar sometidos a una constante verificación, que debe afectar tanto a la acreditación del indicio como a su capacidad deductiva. 3. Los indicios tienen que ser plurales e independientes o siendo único que posea una singular potencia. 4. Los indicios deben ser concordantes entre sí, de manera que converjan en la conclusión. 5. Esa conclusión debe ser inmediata, sin que sea admisible que el hecho consecuencia pueda llegar a través de varias deducciones o cadena de silogismos.

10. A este respecto cabe tener presente que el aparecer incluido o no en las directrices del Plan de control tributario no le otorga al contribuyente un derecho subjetivo a no ser inspeccionado, así la Sentencia del Tribunal Superior de Justicia de Cataluña de 31/03/2023 (Numroj: STSJ CAT 1874:2023).

buena fe como principio, sí que lo pone en tela de juicio en esta concreta aplicación por los intereses concurrentes.

La función administrativa de prevención del riesgo fiscal aparece fundamentada en el deber de contribuir y supone una injerencia en la esfera del particular que no subvierte el principio de buena fe. La necesidad de soportar la carga derivada de la acción pública no puede alterar las reglas sobre la carga probatoria o quebrantar tal principio general de trato. El deber constitucional de contribuir conlleva una obligación de pago, pero también de colaboración cuya exigencia no supone presumir la mala fe.

En todo caso se han de mesurar los efectos y consecuencias asociados a las decisiones jurídicas basadas en tales perfiles. Sin duda, el restringir la posibilidad de intervención y control en los datos y algoritmos que conforman los perfiles de riesgo utilizados por la Administración está en relación inversa al valor y eficacia jurídica que tales instrumentos han de poseer. Los menores controles y posibilidades de intervención y fiscalización de los datos y algoritmos usados en la IA —como sucede en la actualidad— implican menores posibilidades de afectación en la esfera jurídica de la ciudadanía. Es esta, sin duda, una decisión del legislador a la hora de permitir un mayor acceso a la información utilizada y a la participación de su selección y control que posee una correlación concreta en su aplicación en el procedimiento tributario y su consideración probatoria genérica.

2. CREACIÓN DE PATRONES DE RIESGO MEDIANTE IA

La creación de perfiles de riesgo es a su vez una actividad que entraña peligros; peligros por las incertidumbres asociadas al uso de la técnica de IA, y por los laxos controles exigibles a tal actividad cuando se lleva a cabo por la Administración tributaria.

2.1. El riesgo de perfilado mediante IA

La creación de perfiles de riesgo es una actividad en donde la IA posee un acomodo natural por la capacidad de gestionar una gran masa de datos para analizar patrones y tendencias[11]. Son miradas que tienen en consideración eventos normalmente ya acaecidos pues el patrón alude a la repetición de datos, mientras que la tendencia conlleva una dirección de los datos a lo largo del tiempo, que puede ser ascendente, o descendente.

11. Los procesos de automatización, también la elaboración de perfiles de esta forma, aparecen muy poco regulados dando lugar a resultados no siempre justos y notablemente invasivos (Politou y otros, 2019).

En el anterior contexto es preciso conocer las fuentes de los datos empleados. Han de ser fuentes legales y han de aportar datos fidedignos y fiables. La legalidad de los datos deriva de que su origen sea lícito, no pueden haberse obtenido violando derechos, por ejemplo, a través de comunicaciones privadas o en entradas en espacios protegidos sin la correspondiente autorización. También estos datos han de poseer la suficiente trascendencia tributaria, pues la Administración únicamente puede utilizar aquellos que posean tal cualidad, prescindiendo de aquellos que son únicamente privados, o fruto de violentar normas relativas a su secreto. También, no todas las fuentes de información poseen el mismo valor, pues acudir a las redes sociales no conlleva tantas garantías de veracidad como la información obtenida de registros oficiales o públicos.

Si el origen y las fuentes de los datos son importantes no menos relevante resulta evitar los sesgos cuando se utiliza la IA. Los sesgos en el marco de las técnicas de IA ponen de relieve la tendencia sistemática, ya sea por los datos empleados o por el algoritmo, de dar lugar a resultados perjudiciales que acostumbran a perpetuar situaciones de inequidades en relación con ciertos grupos o individuos. Los sesgos en la IA se pueden clasificar de diversas formas, pero puede hablarse de tres grandes categorías; el sesgo preexistente, el técnico y el emergente. El sesgo preexistente se origina en datos históricos o sociales que reflejan prejuicios humanos. El técnico surge de limitaciones técnicas o decisiones de diseño en la creación de algoritmos. Y, por último, el sesgo emergente se desarrolla a medida que la IA interactúa con los usuarios y aprende de nuevos datos que pueden ser sesgados[12].

Los sesgos suponen prejuicios y patrones sociales inequitativos que pueden afectar a derechos reconocidos como la igualdad, la no discriminación o la protección de datos personales, y que los sistemas de IA pueden amplificar. Ello puede ocurrir por que los datos de entrenamiento contienen prejuicios históricos o sociales de los que la IA puede aprender y perpetuar estos sesgos. Desde una perspectiva cuantitativa también pueden existir realidades deformadas por el exceso de datos (sobrerrepresentada) o bien con deficiencias (infrarrepresentada). También desde una perspectiva cualitativa es preciso adecuar los datos a la realidad de su aplicación. No pueden utilizarse datos que permitan análisis particulares o propios de otros contextos o realidades. Tampoco es posible la trasposición de datos de un ámbito jurídico a otro, piénsese en el carácter reservado que poseen los datos tributarios art. 94 de la LGT.

Los algoritmos también pueden ser diseñados, intencional o inadvertidamente, de una manera que favorezca o desfavorezca a ciertos grupos. Con relación

12. Los sesgos pueden aparecer en los datos empleados, en los algoritmos, también pueden ser contextuales cuando atienden al momento de aplicación aludiendo a los sesgos culturales, geográficos y temporales. La clasificación de los sesgos resulta plural así se hablan de sesgos de interacción. que originan prejuicios respecto de los individuos, sesgos latentes, que establecen una correlación inadecuada, sesgos de selección, que resultan de datos no representativos. Navas alude a tres de ellas de forma no exhaustiva: a)Derivados del diseño del sistema. b)Derivados del entrenamiento del sistema. c)Derivados de las aplicaciones y usos del sistema. (Navas, 2017).

al algoritmo se ha de considerar que su operatividad, entrenamiento y aprendizaje se basa en acontecimientos del pasado, que no siempre acaecen de la misma forma en el futuro. También pueden contener lagunas, o mostrarse ciegos a otras realidades. La IA no puede incrementar las brechas de trato desigual por los sesgos, prejuicios, lagunas o deficiencias que contenga.

Precisamente en el Reglamento de Inteligencia Artificial de la UE de 13 de junio de 2024 (en adelante Reglamento de IA)[13] en su Considerando 67 se habla de que la utilización de datos de alta calidad resulta básica para que los sistemas de IA de alto riesgo funcionen de forma segura y no se conviertan en fuente de discriminación. Los conjuntos de datos para la formación, la validación y las pruebas, incluidas las etiquetas —se nos indica— que deben ser: pertinentes, suficientemente representativos y, en la medida de lo posible, libres de errores y completos en vista de la finalidad prevista del sistema. También deben tener las propiedades estadísticas adecuadas y deben tener en cuenta, en la medida en que lo exija su finalidad prevista, los rasgos, características o elementos propios del entorno geográfico, contextual, conductual o funcional específico en el que se pretende utilizar el sistema de IA. En esta línea afirma que se debe prestar especial atención a la mitigación de posibles sesgos en los conjuntos de datos, que puedan afectar a los derechos fundamentales o dar lugar a discriminaciones prohibidas por el Derecho de la Unión. Así se alude a ejemplos de sesgos cuando son inherentes a los conjuntos de datos subyacentes, especialmente cuando se utilizan datos históricos, o generarse cuando los sistemas se aplican en entornos del mundo real. Los sesgos alteran el buen funcionamiento de los sistemas de IA pues aumentan de forma gradual tendiendo a "perpetuar y amplificar la discriminación existente, en particular para las personas pertenecientes a determinados grupos vulnerables, incluidos los grupos raciales o étnicos".

Para verificar la legalidad y calidad de la información que se gestiona, así como la inexistencia de sesgos que den lugar a un mal funcionamiento, es preciso una mayor información, una mayor transparencia[14]. De ahí la necesidad de preveer de manera expresa el derecho a conocer que existen perfiles de riesgo que dan lugar a decisiones que nos afectan y que son elaborados por IA. La información y el derecho a conocer devienen aspectos básicos para poder impugnar y poder ejercer el derecho a la tutela judicial efectiva.

---

13. Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 –2021/0106(COD).

14. Así Martín habla de "incluir, en primer lugar, una referencia al conjunto del proceso decisional en el que se inserta el modelo algorítmico, con expresa mención a su función dentro del mismo, así como al grado y forma de supervisión de los resultados; en segundo lugar, una descripción detallada del propio modelo algorítmico, abarcando el tipo de técnica empleada y los datos de entrenamiento utilizados; y, en tercer lugar, una explicación de la racionalidad de los algoritmos que permita la realización de evaluaciones de su impacto en relación con los principios de igualdad y no discriminación". (Martín, 2022). Ver también Rodríguez, 2021.

De manera específica, y con relación al algoritmo empleado, existe el riesgo de su falta de explicabilidad al ignorar las razones que llevan a un concreto resultado; tal ignorancia afecta sin duda al deber de motivar, y este a que la tutela judicial sea efectiva. ¿Cómo podemos saber el acierto de la decisión si no tenemos los argumentos y motivos para reconstruir el proceso seguido? ¿Como saber si los derechos y libertades se han respetado, si la solución es proporcional, si ignoramos y no sabemos? No se trata de conocer todo el proceso de razonamiento, pero sí de los aspectos esenciales y determinantes de la decisión. Hemos de asegurar que no existen circunstancias personales y sociales sobre las que se establecen diferencias como el sexo, género, edad, raza, origen pues tales diferencias pueden suponer vulneración del principio de igualdad y no discriminación.

La Agencia tributaria en su Plan Estratégico 2024-2027 plantea el estado de la cuestión del uso de la IA y su proyección de futuro. La Agencia tributaria afirma que no usa la IA, entendida como sistemas capaces de funcionar con ciertos niveles de autonomía para alcanzar determinados objetivos, generar información en forma de predicciones, recomendaciones o decisiones a partir de datos y aplicando para ello estrategias de aprendizaje automático o estrategias basadas en la lógica y el conocimiento. Delimitación en ningún caso baladí pues la IA dista de ser una y uniforme; es plural y diversa. La complejidad en la IA, como indica la Agencia Española de Protección de Datos, deriva de converger plurales formas operativas: mediante redes neuronales, sistemas basados en reglas, lógica borrosa, aprendizaje automático, sistemas expertos, sistemas adaptativos, algoritmos genéticos, sistemas multiagente, etc. (AEDP, 2020). Por consiguiente, no toda inteligencia artificial requiere unas mismas cautelas, de ahí la necesidad de conocer la concreta técnica que se usa, y si la Administración aparece autorizada para el empleo de una u otra. Pues, en todo caso, ha de ser una técnica verificable y controlable.

La Agencia, se nos dice, que hace uso de tecnologías analíticas en el tratamiento masivo de datos que funcionan sobre la base de reglas fijadas por humanos y que no emplean capacidades predictivas o generativas de la IA[15]. Ahora bien ¿cómo sabemos que la Administración usa esas u otras tecnologías en la selección de los obligados?

Las amplias posibilidades de uso por parte de la Administración tributaria de medios informáticos, incluida la IA, aparece reconocida en el art. 96 de la LGT. Tal amplitud y discrecionalidad, en el uso de los medios tecnológicos aplicados, se amplifica en el caso de su utilización por la inspección al asociarlo a su carácter reservado; y ante tal estado de cosas ¿cómo controlar, si no se sabe la tecnología empleada?

15. "la Agencia Tributaria hace uso de distintos tipos de tecnologías de tipo analítico, como puedan ser el tratamiento masivo de datos (ampliamente conocido como Big Data), el análisis de redes o grafos, o los sistemas de análisis de riesgos. Estos sistemas funcionan en base a reglas fijadas por humanos, de manera que no hacen uso de las capacidades predictivas o generativas propias de los sistemas de inteligencia artificial". pág. 57.

2.2. EL RIESGO AL USO DE LA IA POR LA ADMINISTRACIÓN

El anterior planteamiento nos introduce en la otra variable de riesgo a considerar: la falta de control de la actuación administrativa en el uso de esta tecnología.

2.2.1. El control en los medios informativos y sistemas de selección

El uso de la tecnología en la selección de los obligados aparece avalado en el art. 170.7 del Real Decreto1065/2007, de 27 de julio. Dicho precepto afirma el carácter reservado en relación con cualquier medio de selección de los obligados objeto de actuación inspectora. En este sentido la elaboración de perfiles se presenta como una actividad asociada a la planificación tributaria de la Administración y por ello reservada en la línea del art. 116 LGT.

El carácter reservado según el art. 170.7 del Real Decreto1065/2007 se asocia a diversos instrumentos, comienza refiriendo a planes de inspección, los medios informáticos de tratamiento de información, y acaba por indicar cualquiera: "los demás sistemas de selección". La anterior es una relación genérica inapropiada para el derecho de acceso a la información pública generalmente afirmado, cuya excepción se pretende de interpretación estricta, e incluso, restrictiva. El derecho de acceso a la información pública se configura como una posición de atribución subjetiva general que únicamente se ve excepcionada por concretas causas legales del art. 14 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Es un derecho esencial para promover la transparencia de las instituciones públicas y para fomentar la participación ciudadana en la toma de decisiones[16]. En este sentido las específicas previsiones de la LGT sobre confidencialidad de los datos tributarios no desplazan ni hacen inaplicable el régimen de acceso que se diseña en la Ley 19/2013[17].

La amplia habilitación legal en el ámbito de la inspección parte de que el conocimiento de los medios informáticos de tratamiento de la información, y de los criterios de selección por la ciudadanía, pueden perjudicar la recaudación y la lucha contra el fraude. Esta perspectiva conlleva que no se pueda controlar su aplicación, generando un claro riesgo a la arbitrariedad administrativa. Esto nos lleva a que el conocimiento de las tecnologías empleadas por la Administra-

16. Ver doctrina contenida en Res 825/2019, de 13 de febrero de 2020 del Consejo de Transparencia y Buen Gobierno.

17. Ver la STS 3071/2022, de 18/07/2022, Nº de Recurso: 2024/2021 afirma su aplicación razonando que "[…] no se contiene en la Ley General Tributaria un régimen completo y autónomo de acceso a la información, y sí un principio o regla general de reserva de los datos con relevancia tributaria como garantía del derecho fundamental a la intimidad de los ciudadanos (art 18 CE). Por ende, las específicas previsiones de la LGT sobre confidencialidad de los datos tributarios no desplazan ni hacen inaplicable el régimen de acceso que se diseña en la Ley 19/2013, de Transparencia y Buen Gobierno (Disposición Adicional Primera)."

ción —no ya los criterios de selección— resulta una información graciable que nos facilita la propia entidad. Y la cuestión resulta ¿perjudica a la recaudación y a la acción administrativa el establecer cualquier control y regulación jurídica sobre la tecnología que emplea? Sin duda, no, pues existen muchos puntos intermedios sujetos a control y muchos los controles —externos o internos— pensables que no perjudican la función de prevención. También y, sobre todo, no pueden ignorarse los principios básicos que han de ser conjugados: la interdicción de la arbitrariedad (art. 9.3 de la CE) y la aplicación reglada de los tributos (art. 6 de la LGT).

En este marco el uso de la IA por la Administración tributaria supone un incremento de los riesgos para la ciudadanía por la capacidad de impacto que posee esta tecnología y la opacidad que la rodea. De ahí la necesidad de reconocer derechos y garantías expresas que hagan posible el control y mejore su funcionamiento sin que perjudique a las políticas de prevención de fraude. Pues no se sabe cómo se seleccionan las variables con mayor capacidad predictiva, cómo se seleccionan los datos de entrenamiento o cómo se selecciona el modelo que supone usar diversos algoritmos. Sin duda son precisos procesos más transparentes en donde la existencia de auditorías y controles externos resulte básica. Las auditorias han de ser capaces de evaluar aspectos tanto tecnológicos como jurídicos sobre la adecuación de los datos y el respeto a los derechos concurrentes. No se trata tanto de conocer los concretos perfiles de riesgo sino de controlar el proceso de gestión de los datos y del algoritmo empleado.

En todo caso los perfiles de riesgo elaborados, dado la opacidad con la que hasta la fecha operan y la falta de contraste concreto sobre la fiabilidad de sus fuentes, carecerán de eficacia probatoria. Su aportación en el procedimiento tributario no podrá ser tenida en cuenta si no se acompaña de otros elementos de prueba suficientes, plurales y concordantes, dado la falta de transparecía y audiencia con la que se opera.

2.2.2. Inexistencia de un modelo de prevención de fraude

El anterior es un claro riesgo administrativo vinculado a la opacidad y falta de control, pero también existe otro derivado de la inexistencia de un modelo de riesgo contra el fraude. No existe regulación expresa alguna que paute el riesgo a prevenir y, en consonancia al mismo, poder establecer las medidas proporcionales.

La operativa que supone crear patrones de conductas peligrosas, perfiles, demanda determinar los riesgos a prevenir. Y lo que sea riesgo no resulta un concepto fácil de delimitar pues el ordenamiento tributario no indica a la Administración cuáles son tales patrones normativos y, sobre todo, no todos los riesgos han de ser protegidos y prevenidos de igual forma.

Como riesgo fiscal no puede considerarse el riesgo para la recaudación, pues identificaría el peligro sólo por el resultado sin atender a las conductas de diversa entidad que pueden concurrir. En tal sentido resulta que cualquier conducta ilícita o lícita, incluso la derivada de error de la propia Administración, o de

una interpretación divergente a la administrativa sería considerada de riesgo tributario e imputada a quien no ingresa. El riesgo tributario ha de asociarse a la lesión del deber de contribuir, pero tal parámetro, siendo correcto, no despeja todas las incógnitas pues las conductas de peligro son muy plurales.

Las conductas de riesgo para el deber de contribuir pueden poseer diverso grado de ilicitud, e incluso resulta plenamente lícitas, por lo que es preciso acotar el comportamiento de referencia para que las medidas asignadas resulten proporcionales a la entidad de los efectos asociados. Así el riesgo tributario puede aludir a la evasión (fraude tributario en sentido estricto), a la elusión ilícita (fraude de ley o conflicto en la aplicación de la norma tributaria) a la elusión lícita (economía de opción) o al incumplimiento tributario (ausencia de ingreso). Diversos son los riesgos tributarios porque diversas son las conductas peligrosas. Saber cuáles han de ser prevenidos y arbitrar medidas adecuadas, diferenciadas y proporcionales, es un reto huérfano de regulación normativa. Y ante la ausencia de un modelo claro de prevención del riesgo fiscal ¿cómo pueden llevarse a cabo políticas de prevención coherentes? El modelo que no puede dejarse al albur de los Planes de Inspección de cada año o de resoluciones internas o a expresiones ambiguas que no hacen más que enmascarar la falta de control y precisión de un aspecto tan necesitado de él.

Sobre el modelo de prevención del fraude fiscal se ha de puntualizar que ni la Administración tributaria realiza con exclusividad tal función, ni las normas tributarias poseen únicamente tal cometido. Ahora bien, ello no quiere decir que no exista una preocupación y una organización, tanto institucional como normativa, que atienda a tales fines. La ausencia de una especialidad de la función preventiva del fraude hace que el modelo sea difuso, al incluirse en normativas que atienden simultáneamente a diversos fines.

Desde la perspectiva institucional, la Administración tributaria no posee órganos específicos y autónomos que atienda a tal finalidad, es más, en sus funciones no se singularizan las de prevención del fraude. Pero ello no implica que, a través de la exigencia de la información y colaboración, se lleven a cabo dicha función. En tal sentido, y por la amplitud de las funciones tributarias atribuidas será la inspección tributaria quien normalmente lleve a cabo tales tareas preventivas; de manera particularizada, a través de la obtención de información y colaboración relacionada con la aplicación de los tributos. Sin perjuicio que dentro de los cometidos propios de los órganos de gestión y recaudación se puedan exigir concretas actuaciones de información y colaboración.

El modelo normativo de prevención del riesgo tributario lo podemos calificar de difuso e inespecífico sobre la base de los siguientes argumentos:

En primer lugar, se atribuye a una Administración no especializada el desarrollo de tal función. Pues comparte dicha función con las de comprobación, investigación y recaudación del tributo, así como de imposición de sanciones.

En segundo lugar, se basa en un régimen de vinculaciones jurídicas plurifuncional. Existe un conjunto intenso y extenso de obligaciones de información y colaboración que pretenden, principalmente, la aplicación del tributo y, adicionalmente, la prevención de las conductas lesivas.

En tercer lugar, existen diversos e inespecíficos procedimientos tributarios que permiten aplicar las normas preventivas. Así resulta que los procedimientos de aplicación de los tributos no son singulares para cumplir la función preventiva.

En cuanto lugar, se efectúa una regulación conjunta y no singularizada de la función preventiva. El régimen preventivo en el ámbito tributario se regula principalmente en el marco de la LGT, junto a las otras funciones correctivas, aplicativas y sancionadoras de la Administración.

En quinto lugar, los riegos tributarios a prevenir son heterogéneos y diversos. Se previene, en el mismo plano y como si del mismo fenómeno se tratara, al fraude tributario o evasión, al fraude de ley integrado en la elusión, y a otras conductas que afectan a la recaudación. Son dos los riesgos, diferentes sus lesiones y diversos también tendrían que ser los medios de prevención. La falta de diferenciación de las medidas que previene uno u otro fraude, o de las que persiguen fines diversos como el recaudatorio, hace que resulte difícil el control y la valoración de su proporcionalidad (Sánchez, 2019).

En definitiva, la prevención en el ámbito tributario se efectúa a través de un modelo no especializado y multifunción en donde ni los mecanismos de prevención son expresos, ni son totalmente coherentes con sus riesgos. Tales discordancias generan, sin duda, graves problemas de proporcionalidad. Esta falta de precisión en la prevención del fraude propende a identificar incumplidores e infractores. En tal planteamiento la orientación normativa y la práctica administrativa apuntan a una idea difusa y amplia de riesgo fiscal que acoge desde la evasión, la elusión —lícita e ilícita— y el incumplimiento en sus múltiples formas. En definitiva, el riesgo fiscal acaba siendo el riesgo para la recaudación.

3. PERFILES DE RIESGO COMO DECISIÓN AUTOMATIZADA

Si duda los perfiles de riesgo se crean para ser aplicados. Este es un segundo momento que da pie a un análisis deductivo para ser llevado a cabo (del perfil abstracto a la aplicación individualizada) en donde los efectos jurídicos de tal decisión cobran una especial significado. Singular importancia posee las garantías jurídicas existentes en el uso de la IA, garantías que se ponen de relieve sobre todo en la normativa europea del Reglamento General de Datos y el Reglamento de Inteligencia Artificial. Si bien cabe observar cómo al escindir la creación del perfil, de la decisión que sobre el mismo se toma, da lugar a plantear la posible intervención de la IA en ambos momentos o solamente en alguno de ellos.

3.1. La prohibición de decisiones automatizadas

Las decisiones tomadas mediante IA sobre la base de perfiles de riesgo —que pueden estar creados o no por IA— aparece especialmente afectado por la regulación de la UE, específicamente el Reglamento General de Datos.

El Reglamento General de Protección de Datos establece en su art. 22 la prohibición general a las decisiones totalmente automatizadas cuando afecten a personas físicas. Se formula el derecho-prohibición de todo interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar[18].

Del mismo destacan varios aspectos; la referencia a decisiones incluye tanto la de los agentes privados como la de las Administraciones, y contempla de manera expresa la elaboración de perfiles[19]. Esta última referencia a la elaboración de perfiles se ha de entender en el sentido de que existe una decisión que resulta la aplicación de estos. Matiz que no deja de ser relevante dado que en su literalidad la garantía que se establece sólo se aplicaría en el momento de creación de los perfiles ("elaboración de perfiles"), aspecto poco coherente con la idea de decisión a la que se asocia la garantía.

Junto al anterior aspecto la garantía establecida se delimita por el hecho de que la decisión sea plenamente automatizada, que afecte a una persona física, posea efectos jurídicos, y que no exista autorización por el Derecho de la Unión o de los Estados miembros para ser dictada. En consecuencia, la delimitación de la anterior garantía se haya excepcionada por la existencia de legislación del Estado o del Derecho de la Unión que, atendiendo a diversas consideraciones, entre ellas las fiscales, establezcan la posibilidad de decidir de forma automatizada en relación con personas físicas, *ex* art. 23. 1, e) del Reglamento UE 2016/679. Tal posibilidad de injerencia se haya condicionado por diversos requisitos; que formalmente se efectúe a través de medidas legislativas, que materialmente la limitación respete en lo esencial los derechos y libertades fundamentales concernidos, y que sea una medida necesaria y proporcionada.

De los anteriores aspectos cabe destacar las siguientes consideraciones relacionadas con el ordenamiento español.

---

18. La posición jurídica que enuncia puede ser entendida como derecho del interesado a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten, o como una prohibición genérica. Ver sobre ámbito, naturaleza y requisitos Armada, 2019. Sobre el Reglamento de protección de datos en general ver Díaz, 2018 y Dopazo, 2018.

19. El Considerando 71 alude a que este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento automatizado de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

La primera, con relación a la decisión y los efectos jurídicos que supone. Se alude a la decisión sobre la base del perfil de riesgo creado, ya se tome ésta de manera directa o indirecta. Nos referimos a decisión indirecta como el contenido determinante para adoptar otra relacionada, resulta la postura adoptada en otro acto diverso pero base fundamental de la decisión. Este aspecto resulta básico para determinar si la inclusión o no en un perfil de riesgo justifica y valida otra decisión que se ha de tomar. El ejemplo sería si la inclusión en un perfil de riesgo tributario puede servir para adoptar y motivar una medida cautelar o la entrada en domicilio. Con relación a la entrada en domicilio la STS 3023/2020, de 1 de octubre, entre otras, afirma la ausencia de motivación cuando se base en informes procedentes de estadísticas, sin especificación suficiente y sin poseer una adecuada transparencia de sus fuentes[20]. Mas explícitamente en su Sentencia de 14/10/2022 (Numroj: STS 3808:2022) afirma que no puede aceptarse "[…] jurídicamente que el mero análisis estadístico o algorítmico sobre medias del sector, no sometido a contraste y no explicado por la Agencia promotora, sea suficiente para justificar una entrada en el domicilio constitucionalmente protegido de un contribuyente, con perfil alto de riesgo […]."

También, y relacionado, resulta el hecho de que los perfiles de riesgo poseen efectos jurídicos, sobre todo como hemos apuntado en el ámbito probatorio. Cabe reiterar que no constituye prueba plena y/o anticipada, ni tan siquiera puede resultar presunción *iuris tantum* que precise ser desvirtuada mediante prueba en contra. No obstante, puede ser considerado como indicio. En este sentido la decisión tributaria de apertura de un procedimiento tributario, concretamente de inspección, sobre la base de un perfil de riesgo genera efectos jurídicos por los deberes asociados al mismo, aunque no prejuzgue el resultado ni constituya prueba válida para la decisión del procedimiento.

La segunda consideración aparece referida a que sea una decisión totalmente automatizada. En el Plan Estratégico de la Agencia 2024-2027 y haciendo un pronóstico de aplicación de IA se indica que "las actuaciones administrativas automatizadas que dicte la Agencia Tributaria no descansarán, en ningún caso, de manera exclusiva en el resultado obtenido de un sistema de IA. En estas situaciones, se garantiza siempre la intervención humana que habrá de supervisar, validar o incluso vetar las opciones que hayan podido ser propuestas por el sistema. En definitiva, todas las decisiones serán adoptadas por personas." La literalidad de lo indicado da pie a pensar que cuando se emplee la IA la intervención humana pueda verse reducida a la mera validación de la decisión de la IA o a una mera supervisión formal de lo que esta decida. La existencia de decisiones mixtas plantea la trascendental cuestión de cuando aplicar las garantías

20. "[…] del cotejo de la situación hipotética, sospechada o derivada de una información meramente fragmentaria, nacida de la proyección de datos genéricos obrantes en documentos o cuadros estadísticos y cuya fiabilidad, a falta de más sólidos elementos de convicción, hemos de poner por fuerza en duda, no es base suficiente para servir de título habilitante a la Administración —para pedir— y al juez —para otorgar— la entrada en el domicilio"

de Reglamento General de Datos, pues en puridad no son decisiones totalmente automatizadas.

En las decisiones automatizadas el reto es sin duda acotar la relevancia de la intervención humana en aquellas que son parcialmente automatizadas o semiautomatizadas. En otros términos, determinar cuál es la influencia del humano y del sistema automatizado en la toma de decisión. En una primera acotación cabe considerar que no toda intervención humana excluye las garantías previstas en el art. 22 del Reglamento. Las Directrices sobre las decisiones individuales automatizadas habla de que la intervención humana ha de ser significativa, no una mera formalidad o un gesto simbólico[21]. Es así posible hablar de decisiones automatizadas cuando la valoración determinante de la decisión descanse en el sistema de inteligencia artificial, aunque formalmente la decisión sea de una persona humana[22]. En todo caso la intervención humana, cuando resulta exigible, no puede resultar una mera apariencia o formalidad.

Los supuestos de decisiones compartidas por el humano y por la IA son situaciones hibridas en donde criterios sobre la aportación relevante[23] en la decisión han de considerarse para delimitar la autoría[24]. Si el juicio de la persona física es el decisivo para la adopción de la solución, aunque intervenga la IA, la decisión no será totalmente automatizada, y *a contrario*. En esta orientación resulta básico el examen de la motivación y justificación de los actos, tanto en el caso de que el parecer humano concuerde como cuando resulte discrepante del ofrecido por la IA.

La tercera consideración alude, como excepción a la garantía, a la posibilidad de que el Derecho de la Unión o el Derecho del Estado miembro autorice las decisiones o perfiles automatizados estableciendo, eso sí, las medidas adecuadas para la salvaguarda de los derechos e intereses del interesado. De forma específica se prevé en el Considerando 71 que se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, "si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, nor-

21. Se indica que el responsable del tratamiento no puede obviar las disposiciones del art. 22 inventándose una participación humana. Dicha participación ha de ser significativa en la decisión, no un mero gesto simbólico. Para poder valorar dicha aportación prevé que dentro de la evaluación de impacto del responsable del tratamiento identifique y registre el grado de participación humana en el proceso de toma de toma de decisiones y en qué punto se produce esta (Directrices, 2017, pág. 23).

22. La STJUE de 7 de diciembre de 2023 asunto C-634/21 aplica las garantías del art. 22 a terceros que procesan los datos, aunque sean responsables formalmente de la toma de decisiones. Ver Contino, 2024.

23. Todolí habla de "intervención humana significativa" (Todolí, 2018).

24. La Carta de Derechos Digitales del Ministerio de Asuntos Económicos y Transformación Digital habla en el XXVIII apartado 6 que será necesaria una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas.

mas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales […]"[25].

El ordenamiento español no establece en la actualidad excepción a la aplicación de la regla del art. 22 del Reglamento General de Datos, pues no basta la formulación genérica de la DA 14 de la LO 3/2018 de 5 de diciembre, al exigirse concretar los derechos concernidos y justificar su necesidad y proporcionalidad. La mención del art.100.2 LGT cuando alude a que tendrá la consideración de resolución la contestación efectuada de forma automatizada por la Administración tributaria no supone una autorización tácita. Pues se requiere una habilitación reglamentaria expresa para determinar los procedimientos tributarios a que resulta de aplicación dicha previsión (Sánchez, 2023).

Llegados a este punto posiblemente subsiste el interrogante de ¿A que vienen todas estas cautelas para los notables beneficios que conlleva el uso de la inteligencia artificial? La respuesta es clara, la norma jurídica demanda procesos aplicativos complejos en donde aprehender la realidad, conocer el Derecho, y explicar el proceso de razonamiento hace imprescindible —hasta la fecha— la inteligencia humana. En este sentido cabe hablar de tres principios/garantías jurídicas estrechamente imbricado en tal proceso[26].

En primer lugar, la sumisión al Derecho. La aplicación del Derecho no supone sólo considerar normas escritas, definidas y concretas, sino todas las fuentes del Derecho, incluidos los principios generales. Cabe recordar que la Administración aparece sometida no sólo a la ley sino al Derecho como afirma el art. 103.1 de la CE. En tal contexto la búsqueda de los principios, su prelación, y la solución de las controversias jurídicas son tareas esencialmente racionales en donde el sentido común y las múltiples inteligencias humanas necesitan estar presentes. El uso de la IA en tales procesos exige probar la posibilidad de su aplicación al autorizar los programas informáticos, y se ha de facilitar el control del *iter* seguido.

En segundo lugar, se ha de garantizar la seguridad jurídica. Se ha de poder prever, conocer y controlar la lógica empleada atendiendo a la complejidad que supone tanto la apreciación de los hechos como la aplicación normativa. El principio de seguridad jurídica supone un valor y principio constitucional recogido en el art. 9 por lo que demanda garantías, en ningún caso soslayables por meras resoluciones administrativas que autorizan la utilización de programas y aplicaciones informáticas.

Y, por último, se ha de asegurar que no existe arbitrariedad. Se ampara dicho principio en la medida que puedan fiscalizarse las razones y fundamentos en que se basa la decisión jurídica. Nuevamente se trata de un principio constitu-

25. Todo ello sin perjuicio de que el Comité Europeo de Protección de Datos establecido por el Reglamento pueda formular orientaciones en este contexto (Considerando 72).

26. Al margen de que la introducción de la tecnología digital y la inteligencia artificial no supone una menor burocracia del sector público y consiguientes menores gastos. También existe el peligro de crear una tecnocracia en donde la lógica del poder instituido, a través de las maquinas, acabe por gobernar la sociedad como apuntaba Weber (Ver Newman y otros, 2022).

cionalizado que se garantiza, principalmente, a través de la posibilidad de su control mediante la motivación. Si no pueden conocerse y fiscalizarse las lógicas de las decisiones tomadas de forma automatizada existe el riesgo de convertir a la máquina en un oráculo de la ley, o la representación de una divinidad laica cuyos designios resultan irrefutables. No se trata saber de manera exhaustiva y detallada como opera la IA y sus procesos internos, pues al ser humano tampoco le podemos fiscalizar dichos procesos neuronales, sino de poder controlar los procesos básicos de decisión. La motivación que puede ser exigible es aquella que resulta determinante de la decisión y permite su control para hacer posible el derecho a la tutela judicial efectiva.

3.2. El reglamento de IA y el ámbito tributario

Averiguar la manera que impacta el Reglamento de Inteligencia Artificial de la UE de 13 de junio de 2024 en las garantías y objeto que tratamos pasa por contextualizar su regulación.

En primer lugar, articula un nuevo ámbito de garantías en el uso de la IA tanto para las empresas como para las Administraciones públicas.

En segundo lugar, su régimen jurídico que no se limita a sectores concretos, es horizontal, lo que supone una notable amplitud regulatoria. Esta heterogeneidad de lo regulado lleva a que su incidencia sea focalizada, pues son muchos los sectores, usos y entornos, y múltiples las decisiones afectadas.

En tercer lugar, es una regulación preventiva que modula los derechos que reconoce en función de los ámbitos de riesgo que acota. Las normas preventivas en materia de IA son necesarias para hacer posible su aplicación al ámbito jurídico, pues de otra manera no se garantizaría la indemnidad de los principios anteriormente enunciados. A este respecto se ha de tener presente que la estructura de una decisión jurídica pasa por tres complejas tareas que distan de ser mecánicas; en primer lugar, la reconstrucción de los hechos que integran el contenido típico de la norma —que tiene que ver con la valoración de la prueba—; en segundo lugar, la motivación legal mínima que supone enjuiciar la validez, la eficacia, o la supremacía de la norma aplicada y, en tercer lugar, la motivación legal concreta que conlleva la calificación jurídica de los hechos y sus concretas consecuencias. Y tales procesos, diversos y complejos, han de ser susceptibles de control. Se ha de poder prever, conocer, y controlar la lógica empleada atendiendo a la complejidad que supone tanto la apreciación de los hechos como la aplicación normativa.

Con tales premisas se observa que el Reglamento de IA posee una especial sensibilidad con relación a los perfiles y su uso para el enjuiciamiento del individuo, si bien lo circunscribe al ámbito penal. Resulta elocuente el Considerando 42 al afirmar que las personas físicas nunca deben ser juzgadas por su comportamiento previsto por la IA basado únicamente en su perfil, "[…] Por lo tanto, deben prohibirse las evaluaciones de riesgo realizadas en relación con personas físicas con el fin de evaluar la probabilidad de que delincan o de predecir la

comisión de una infracción penal real o potencial". Junto a lo anterior resulta que se excluye al ámbito tributario de las garantías asociadas al alto riesgo. En el Considerando 59 se indica que los sistemas de IA destinados a ser utilizados en procedimientos administrativos por las autoridades tributarias y aduaneras no deben clasificarse como sistemas de IA de alto riesgo.

Por consiguiente, el Reglamento sobre IA excluye de la categoría de alto riesgo y de las garantías asociadas a la materia tributaria. Tampoco establece un marco reglado para la actuación administrativa en sus procedimientos tributarios. Todo lo cual supone que las garantías y cautelas en la materia habrán de ser facilitadas por el legislador nacional. Y a este respecto la normativa tributaria nacional resulta parca en garantías a tenor del art. 96 de la LGT pues enfatiza más las posibilidades administrativas que los derechos y garantías del interesado. Así se establece la necesidad, y suficiencia, de que sea la propia administración quien apruebe los programas y aplicaciones que vayan a ser utilizados, y para cuya publicación basta la facilitada por el web —art. 85 del Real Decreto 1065/2007— que en la práctica ha sido la vía para determinar los actos y procedimientos automatizados (Sánchez, 23)[27]. De ahí la necesidad y urgencia en la creación de un marco jurídico que regule el uso de la inteligencia por la Administración tributaria. Es preciso un régimen propio del ámbito tributario que contemple concretos derechos y garantías en los contextos tecnológicos. No sólo hace falta sentido común, que sin duda el funcionario o autoridad administrativa posee —a diferencia de la IA—, sino garantías y controles jurídicos que avalen las opciones necesariamente valorativas que se toman.

4. CONCLUSIONES

Considerando los anteriores análisis caben formular las siguientes conclusiones:

Primera. Los perfiles de riesgo tributario creados por IA suponen un tratamiento automatizado llevado a cabo por la Administración tributaria de datos personales con transcendencia tributaria que permiten evaluar aspectos asociados a su comportamiento tributario a fin de analizar y predecir aspectos relacionados, principalmente, a su rendimiento, situación económica, relaciones o comportamiento en la media que pueda suponer un peligro para la recaudación.

27. Ver las numerosas resoluciones al respecto, la resolución de 23 de febrero de 2015 de la Agencia estatal de administración tributaria por la que se aprueban nuevas aplicaciones informáticas para las actuaciones administrativas automatizadas, la de 27 de abril de 2018 de la Agencia estatal de administración tributaria destacan actuaciones de gestión tributaria del IVA en relación del sistema de Suministro Inmediato de Información, la de 4 de julio de 2019 de la Agencia estatal de administración tributaria se alude a diversas actuaciones que refieren al procedimiento de recaudación y en las que se entremezclan la resolución de cuestiones tramite con otras de mayor calado o la de 13 de julio de 2023 de la dirección general de la agencia estatal de administración tributaria, por la que se aprueban nuevas aplicaciones informáticas para la actuación administrativa automatizada.

Segunda. El uso de los perfiles de riesgo exige poner de relieve los dos momentos que lo integran pues poseen diversas garantías y exigencias jurídicas y que ambos, o alguno de ellos, puede llevarse a cabo mediante IA. De un lado, el perfil resulta un conjunto de características que delimitan de forma indiciaria la identidad de una persona, y que se crea a través de un proceso de generalización o inductivo. De otro lado, sobre el perfil creado se toman decisiones, y ésta es una dimensión diversa que supone un proceso —deductivo— de aplicación a una realidad individualizada.

Tercera. Las determinaciones de un perfil de riesgo tributario difícilmente pueden predeterminar efectos jurídicos individualizados. Los perfiles no plasman una realidad concreta, sino genérica y, normalmente, estadística conformada con una pluralidad de comportamientos. De ahí que el perfil de riesgo no resulta prueba, ni directa ni indirecta de los hechos que han tenido lugar. En consecuencia, el perfil de riesgo no puede decidir directa o indirectamente un procedimiento; ahora bien, ello no le priva de todo efecto jurídico pues puede constituir indicio, necesitando ser corroborado por otros elementos de prueba.

En el mismo sentido las escasas posibilidades de intervención de la ciudadanía en el control de los datos y algoritmos que conforman los perfiles de riesgo utilizados por la Administración están en relación inversa al valor y eficacia jurídica que tales instrumentos han de poseer. La menor fiscalización de datos y algoritmos implican menores posibilidades de afectación en la esfera jurídica individualizada.

Cuarta. La Administración tributaria declara que no usa en la actualidad IA, lo cual no elimina los problemas asociados a los perfiles de riesgos, sino que los evidencia más si cabe. La Agencia nos dice, que hace uso de tecnologías analíticas en el tratamiento masivo de datos que funcionan sobre la base de reglas fijadas por humanos y que no emplean capacidades predictivas o generativas de la IA. Ahora bien ¿cómo sabemos que la Administración usa esas u otras tecnologías en la selección de los obligados? Existen unas amplias y discrecionales posibilidades de uso por parte de la Administración tributaria de medios informáticos, que en el caso de aludir a la inspección se amplifican al asociarlo a su carácter reservado; y ante tal estado de cosas ¿cómo controlarla, si no se sabe la tecnología empleada?

Quinta. La creación de perfiles de riesgo mediante IA ha de procurar el control de la legalidad y fiabilidad de los datos existentes. También han de existir suficientes mecanismos que aseguren la inexistencia de sesgos que pueden conducir a tratos inequitativos. Los sesgos suponen prejuicios y patrones sociales inequitativos que bien pueden afectar a derechos como la igualdad, la no discriminación o a la protección de datos personales, y que los sistemas de IA se pueden amplificar. Para verificar la legalidad y calidad de la información que se gestiona, así como la inexistencia de sesgos que den lugar a un mal funcionamiento es preciso una mayor información, una mayor transparencia. En tal contexto la información y el derecho a conocer devienen aspectos básicos para poder impugnar y poder ejercer el derecho a la tutela.

Sexta. El perfil también se ha de contemplar como decisión automatizada, y de esta manera le resultan aplicable las garantías del Reglamento General de Datos. A este respecto cabe destacar que el Plan Estratégico de la Agencia 2024-2027 prevé un uso futuro de la IA a la hora de tomar decisiones si bien de forma mixta o semiautomatizado. La aplicación del régimen de las decisiones totalmente automatizadas a estas decisiones mixtas pasa porque la intervención humana sea una mera formalidad o su aportación resulte irrelevante. Para ello resulta básico el examen de la motivación y justificación de los actos, tanto en el caso de que el parecer humano concuerde con el de la IA como cuando resulte discrepante.

Séptima. El Reglamento europeo de IA posee un escaso impacto a la hora de regular los perfiles de riesgo creados por la Administración tributaria a través de IA. Tal carencia de relevancia aboca a que el legislador nacional incremente el marco regulatorio estableciendo un régimen jurídico específico con garantías suficientes. Este debería ser un régimen garantista —que considere la protección de los derechos fundamentales concernidos en su aplicación—, preventivo —que atienda a los riesgos que supone—, y reglado, que paute la concreta actuación en el procedimiento tributario acotando lo que puede hacerse y el cómo efectuarlo.

BIBLIOGRAFÍA

AEDP (2020) *Adecuación del RGPD de tratamientos que incorporan inteligencia artificial. Una introducción*. Disponible en https://www.aepd.es/guias/adecuacion-rgpd-ia.pdf.

ARMADA VILLAVERDE, M. y LÓPEZ BUSTABAD, I. (2019) El reglamento general de protección de datos ante el fenómeno del «big data». *Derecho y Nuevas Tecnologías* (51).

CABRALES GOITIA, A. (2021). Mas allá de los nudges: Políticas públicas efectivas basadas en la evidencia de las ciencias del comportamiento. *GAPP*. (25). 38-45. DOI: https://doi.org/10.24965/gapp.i25.10864.

CONTINO HUESO, L. (2024). La primera Sentencia del Tribunal de Justicia de la Unión Europea sobre decisiones automatizadas y sus implicaciones para la protección de datos y el Reglamento de inteligencia artificial. *Diario LALEY*, Ciberderecho. (80).

DÍAZ MARTÍN, C. (2018) El Reglamento General de Protección de Datos, su implementación y la transición para el responsable público. *Revista Aranzadi de Derecho y Nuevas Tecnologías.* (47)

Dictamen del Comité Económico y Social Europeo sobre «Integrar los nudges en las políticas europeas» (Dictamen de iniciativa) (2017/C 075/05) Ponente: Thierry Libaert.

Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. Adoptadas el 3 de octubre de 2017. 17/ES WP251rev.01

DOPAZO FRAGUÍO, P. (2018) La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente. (Novedades del Reglamento General de Protección de Datos). *Revista Española de Derecho Europeo*. 113-148. (68).

Grupo De Trabajo Sobre Protección De Datos Del Artículo 29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679. Adoptadas el 3 de octubre de 2017.

MARTÍN LOPEZ, J. (2022). Inteligencia artificial, sesgos y no discriminación en el ámbito de la inspección tributaria. *Crónica Tributaria*. 51-89. (182). https://doi.org/10.47092/CT.22.1.2

MOREU CARBONELL, E. (2018). Integración de nudges en las políticas ambientales. *Revista Aragonesa de Administración Pública*, (19). 451-485

NAVAS NAVARRO, S. (2017). Derecho e inteligencia artificial desde el diseño. Aproximaciones, en Robert Guillén, S., Castells I Marquès, M., Camacho Clavijo, S., Navas Navarro, S., Mateo Borge, I., Górriz López, C. *Inteligencia artificial. Tecnología Derecho*. Tirant lo Blanch. Valencia.

NEWMAN, J., MINTROM, M. y O'NEILL, D. (2022) Digital technologies, artificial intelligence, and bureaucratic transformation. *Futures*. (136). https://doi.org/10.1016/j.futures.2021.102886

OCDE (2022). *Manual de la OCDE sobre política de competencia en la era digital*. https://www.oecd.org/daf/competition-policy-in-the-digital-age

OCDE (2023). *Apoyo a la digitalización de las Administraciones en los países en desarrollo*. https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/apoyo-a-la-digitalizacion-de-las-administraciones-tributarias-de-los-paises-en-desarrollo.pdf

PASTOR ALCOY, F. (2003) *Prueba de indicios, credibilidad del acusado y presunción de inocencia,* Tirant lo Blanch. Valencia.

POLITOU, E., ALEPIS, E. y PATSAKIS, C. (2019) Profiling tax and financial behaviour with big data under the GDPR. *Computer Law & Security Review*. 35 (3), https://doi.org/10.1016/j.clsr.2019.01.003

PONCE SOLÉ, J. (2019) Inteligencia artificial, derecho administrativo y reserva de humanidad: Algoritmos y procedimiento administrativo debido tecnológico. *RGDA*. (50).

ROBERT GUILLÉN, S., CASTELLS i MARQUÈS, M., CAMACHO CLAVIJO, S., NAVAS NAVARRO, S., MATEO BORGE, I., GÓRRIZ LÓPEZ, C. (2017). *Inteligencia artificial. Tecnología Derecho*. Tirant lo Blanch. Valencia.

ROIG, A. *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*. Bosch Editor. Barcelona. 2020.

RODRIGUEZ PEÑA, N. (2021). Libertad: "Big data e inteligencia artificial: una aproximación a los desafíos éticos y jurídicos de su implementación en las administraciones tributarias. *Ius et Sciencia*. 7. (1) 64-84.

SÁNCHEZ HUETE, M. Á. (2023). La contestación automatizada de los procedimientos tributarios". *REDF.* (198).

SÁNCHEZ HUETE, M. Á. (2019). *Tributación, fraude y blanqueo de capitales. Entre la prevención y la represión*. Marcial Pons. Madrid.

TODOLÍ SIGNES, A. (2018) La gobernanza colectiva de la protección de datos en las relaciones laborales: big data, creación de perfiles, decisiones empresariales automatizadas y los derechos colectivos. *Revista de Derecho Social*, (84) 69-88.

III. Empresa y Administración tributaria

REFLEXIONES SOBRE BIENES INTANGIBLES BASADOS EN CONJUNTOS ESTRUCTURADOS DE DATOS O CRIPTOACTIVOS Y LA APLICACIÓN DE LOS TRIBUTOS

José Antonio Fernández Amor
Catedrático de Derecho Financiero y Tributario
Universidad Autónoma de Barcelona

ABSTRACT:
Technology has enabled the transition from data as the foundation of knowledge to creating structured and unique sets of these elements that can be used as assets in economic transactions. From that moment, they are of interest to tax law as taxable objects, as they represent economic capacity. However, it is not only in the realm of tax levy regulations that they must be considered, but also in the field of the organization of application procedures. This work is an approach to these intangible movable assets from that perspective, addressing aspects such as the requirements to obtain information about the novel asset, its function as a guarantee of the tax obligation, its valuation, the evidence of its circumstances, or the extinction of the tax debt with its delivery.

Keywords: data, tax information, tax application, crypto-assets.

Palabras clave: datos, información tributaria, aplicación de tributos, criptoactivos

1. INTRODUCCIÓN

Según la definición del Diccionario de la Real Academia de la Lengua, el significado de la palabra dato es *"Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho."*. Así mismo, ofrece otra acepción relacionada con la informática *"Información dispuesta de manera adecuada para su tratamiento por una computadora"*. En ambas acepciones se trata de información, de piezas de conocimiento, de elementos con los que obtener un resultado que sirve, de alguna forma, para aumentar el entendimiento en diversidad de temas.

Las tecnologías para el procesamiento de la información han hecho que esta perspectiva del dato como pieza de cognición evolucione. Si bien siempre ha habido un consenso en las ideas de que la información es poder y que la información tiene un valor crematístico, en la actualidad se ofrece otra perspectiva. Los datos se pueden organizar en estructuras singulares no duplicables y, lo que es más importante a los efectos de estas líneas, ser el soporte de bienes a los que otorgar un valor económico[1].

Esto se hace posible porque, en síntesis, estas formas estructuradas de datos que ya no son solo información para fundamentar razones, sino también soporte de bienes intercambiables, se transfirieren por medio de Internet de un nodo

1. Los hechos que se apuntan discurren paralelos a la evolución que muestra Internet desde su creación. En su seno se diferencia una Web 1.0 identificable con la web que ofrece información para leer por el usuario. Sigue la Web. 2.0 que es un paso más en tanto que el usuario lee lo que ofrece la red y, además, participa escribiendo y creando contenido. A continuación, aparece la Web 3.0 o web semántica basada en estructurar la información en la red de forma que se puedan interconectar páginas web y ofrecer una mayor personalización al usuario en el uso de la información de la red que, además, se descentraliza en varios nodos. Finalmente (aunque quizá no la última versión), se empieza a distinguir una Web 4.0 basada en introducir en la red cualquier cosa interconectándola con otras, ofreciendo experiencias inmersivas al usuario más allá de la pantalla de un ordenador. Para estas líneas se destaca, de todas ellas, la Web 3.0 en la que se enmarca la posibilidad de estructurar información mediante tecnologías como el *Blockchain* o los registros descentralizados de manera que constituya una pieza, objeto intangible o elemento valorable económicamente que los usuarios pueden intercambiar en sus transacciones en la red.

a otro, sin duplicar, perder o devaluar su estructura de conjunto de signos ordenado. De esa transmisión, además, queda constancia pública para los usuarios que participan en el programa sobre el que se construye el efecto intercambiable ya que ha de ser anotada en diversos nodos para que sea validada y aceptada por ellos, conste como realizada y no pueda ser copiada. A ella no han de acceder, además, terceros ajenos a dicha transmisión para lo que se añaden capas de seguridad encriptando las transacciones. Finalmente, se puede añadir la anonimización de los participantes en las operaciones que se lleven a cabo aumentando la privacidad de sus actuaciones. Sumariamente comentadas, todas estas características que rodean a la información convertida en datos causan que pasen a ser bienes intangibles con interés económico capaces de representar bienes, derechos tradicionales o tener un valor intrínseco. Asimismo, esta diferenciación de una novedosa manifestación de la información es merecedora de una nueva denominación: los conjuntos estructurados de datos se identificarán con el término criptoactivos[2].

Dado el salto desde la información al bien valorable económicamente, bien se asume la idea de que los datos estructurados pueden formar parte de los elementos que componen el patrimonio de los sujetos quienes ejercerán sobre ellos facultades dominicales[3]. Yendo un poco más allá en estas reflexiones, estos bienes muebles intangibles, desde el momento en que son representativos de capacidad económica al ser valorables, tienen características a considerar desde el punto de vista tributario. Vistos según sus características y naturaleza —pues pueden ser desde una acción hasta una moneda, pasando por una representación artística— tendrán un tratamiento fiscal determinado —gravando su plusvalía, su transmisión, su titularidad etc…— o, cuanto menos, deberán ser atendidas seguras consecuencias tributarias.

Pero una lectura completa del fenómeno tributario no se agota en la labor de clasificar un bien, calificar un hecho y determinar una consecuencia tributaria a modo de gravamen. También se caracteriza por el ejercicio de facultades y funciones administrativas disciplinadas, como no puede ser de otra manera, por el ordenamiento. En este sentido, la cuestión que se plantea en la presente aportación es indagar cómo se acogen a los definidos criptoactivos en diversas parcelas de la aplicación tributaria.

Siguiendo la intención apuntada, las líneas que siguen tratan, en primer lugar, de aproximarse a la regulación relacionada con los criptoactivos que refuerza las capacidades de investigación tributaria, objetivo vinculado a la inspec-

2. Concepto que se normaliza normativamente pues se recoge en el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos.

3. En este sentido, puede traerse aquí el pronunciamiento del ICAC en su Consulta nº 120/2019, de 31 de diciembre. Partiendo de las consideraciones del Banco Central Europeo sobre las criptomonedas, entendiéndolas como medio de intercambio de bienes, pero no como moneda de curso legal, el organismo considera que pueden ser concebidas en el Balance de Situación como 'existencias' o 'inmovilizado intangible' según sea el caso.

ción tributaria. Concretando, se trata de presentar cómo ha evolucionado la regulación de la potestad administrativa de obtención de información sobre estos nuevos elementos. En segundo lugar, se examinan extremos de la posibilidad de aceptar este bien en alguna de sus manifestaciones como garantía de la deuda tributaria y, ligado con esto, cómo se ha de gestionar la determinación de su valoración o cuestiones en torno a la prueba sobre este elemento. Finalmente, la exposición centra la atención sobre la viabilidad del nuevo bien para la extinción de la deuda tributaria con consideraciones desde el procedimiento de apremio. Cerrará las diferentes reflexiones ofrecidas una recopilación de conclusiones.

2. EL CONJUNTO ESTRUCTURADO DE DATOS Y LA INSPECCIÓN TRIBUTARIA: LA OBTENCIÓN DE INFORMACIÓN

Los conjuntos estructurados de datos, como se ha comentado, tienen entre sus diversas características la de la anonimidad de sus titulares de manera que los gestionan en la red sin que sea necesaria su identificación real o la de la encriptación que impide la intervención de terceros. En este sentido, pueden ser loables las iniciativas que permitan mayor libertad de acción a los individuos a través de proporcionarles espacios reservados, privados y no intervenidos[4]. Pero la anonimidad, la privacidad y el espacio reservado pueden desembocar en la idea de secretismo de las acciones emprendidas. Amparándose en esto, quedan fuera de alcance y control ajeno a los interesados acciones que pueden ser, por supuesto, totalmente lícitas, pero también ilícitas o, siendo más grave, ilegales. El conflicto jurídico está servido pues se ha de trabajar el equilibrio entre la privacidad y espacios de libertad de acción individual con la seguridad para el resto de la sociedad de que lo emprendido es acorde con el orden jurídico vigente[5].

---

4. Sobre todo en el ámbito de las criptomonedas enmarcadas en proyectos privados (para diferenciarlos de los públicos que generan las Central Bank Digital Currency o CBDC o dinero de curso legal en formato de código estructurado) esta característica es uno de sus principales atractivos. La posibilidad de intercambiar valor de forma anónima y reservada a la intervención de terceros encarnados en autoridades financieras fue preconizada, hacia los años 90, por el movimiento Cyberpunk que abogaba por un cambio en las relaciones financieras de manera que se aprovechase la red por los usuarios para hacer transacciones sin control por parte de terceros ajenos a la transacción (vid. Chaum 1983: 199-203).

5. Como recordatorio de esta preocupación se trae aquí la Directiva (UE) 2018/843 de 30 de mayo del Parlamento y del Consejo por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención del sistema Financiero para el blanqueo de capitales o la financiación del terrorismo. Su considerando noveno alude a que *"El anonimato de las monedes virtuales permite su posible uso indebido con fines delictivos"*. Por su parte, CARDOSO indica que *"Los análisis ponen de manifiesto que solo un tercio de los bitcóin ya generados se emplea como medio de intercambio. Dicho de otro modo, en la actualidad se recurre a él, fundamentalmente, con fines de inversión. En este segmento hay que*

Para una mejor comprensión de lo que se afirma, es posible trazar aquí un paralelismo con el secreto bancario que ha sido aprovechado, en ocasiones, para la ocultación de transacciones o riqueza a los ojos de las autoridades[6]. Pues bien, las características citadas podrían ser las piezas con las que construir un parapeto tras el cual esconder actividades a las que adjetivar conforme a su acercamiento o alejamiento al ordenamiento en general y tributario en particular.

Un secreto bancario que, como ya se conoce, ha sido combatido tradicionalmente desde las autoridades, tanto desde un punto de vista doméstico como internacional, con el establecimiento, extensión y refuerzo de los deberes de información de sujetos relacionados con transacciones financieras. Esa línea de acción es la que se ha adoptado también con respecto a aquellos criptoactivos que pudieran beneficiarse, por sus características, de evitar mostrarlos a las autoridades tributarias que han de velar por la justa distribución de las cargas públicas. Estas se encuentran en proceso de reforzar sus capacidades de control incrementando los deberes de información de particulares de manera que conocerán diversos extremos de los nuevos bienes.

Las manifestaciones de criptoactivos, en las que las características que propician el secretismo en la red han sido valoradas por los usuarios, son las de aquellos que se han configurado como monedas de génesis privada. Siendo útiles para la adquisición de bienes o servicios, su dinámica de funcionamiento les ha permitido alejarse de circuitos económicos controlados o intervenidos por autoridades cuyo objetivo es la prevención y represión de comportamientos no ajustados a Derecho.

Para centrar el tema se parte de la base de que las criptomonedas han ocupado la atención de la Inspección tributaria desde ya hace algún tiempo. Su labor de investigación para hacer efectivo un principio de transparencia ante el secretismo mencionado y, por consiguiente, una tributación adecuada, siguiendo el art. 141.c) de la Ley 58/2003, de 17 de diciembre, General Tributaria (en adelante LGT), se ha basado, en la obtención de información sobre esos elementos con justificación en los arts. 93 y 94 de la LGT. Esta idea se confirma si se atiende a la Resolución de 19 de enero de 2021 en el que la Dirección General de la Agencia Estatal de Administración tributaria aprobaba el Plan Anual de Control Tributario y aduanero de ese año. En su apartado III.2.A.4 se indicaba que, ante el auge de los mercados de activos virtuales donde pueden producirse riesgos fiscales, se han de emprender algunas actuaciones como: a) obtención desde diversas fuentes de información sobre operaciones en criptomonedas; b) sistematización y análisis de la información obtenida y c) potenciar la cooperación

---

incluir, como resulta obvio, la posesión de bitcóin como contraprestación por el pago de un "bien o servicio" delictivo; que en este caso no responde a razones especulativas, sino de aprovechamiento del anonimato y la consiguiente dificultad de investigación y persecución policial". CARDOSO (2019: 40).

6. El fenómeno de las criptomonedas plantea considerar la existencia un nuevo paraíso fiscal constituido por el espacio virtual en el que tienen sentido, en el que no hay jurisdicciones que puedan ejercer un poder tributario en forma de control y en el que los sujetos pueden actuar de forma anónima. Véase MARIAN (2013:10)

internacional y la participación en foros internacionales para obtener información.

Esta primera aproximación hacia instrumentos con los que llevar a cabo labores de investigación sobre criptoactivos merece algunas reflexiones. La primera es que se ha de obtener información sobre aspectos como la clase o tipo del bien mueble intangible, quién es su titular, su valor a efectos económicos y las transacciones que se realizan. La segunda es que la normalización de este tipo de bienes en la economía, el aumento de su uso y, en opinión del que escribe, lo voluble de su valoración conllevan el tener que operar con grandes cantidades de datos que habrá que ordenar para que sean útiles. En tercer lugar, es muy elocuente la indicación que se realiza hacia la cooperación internacional en tanto que es un reconocimiento implícito de que los criptoactivos son una realidad que excede el territorio en el que puedan ejercerse las facultades de la autoridad tributaria por lo que ha de acudirse a la cooperación internacional.

Las líneas de actuación sobre el fenómeno que advirtió la autoridad fiscal pasan a ser normas en virtud de la aprobación de la Ley 11/2021, de 9 de julio de medidas de prevención y lucha contra el fraude fiscal. Según su art. 13.26 que modifica la Disposición Adicional 18ª de la LGT, en el marco de los arts. 29 relativo a obligaciones formales y 93 relativo al deber de aportar información, ambos de la LGT, se impone, con una nueva letra d), un nuevo deber formal. Todo obligado tributario (ex. art. 35 LGT) ha de suministrar información con respecto a monedas virtuales situadas en el extranjero cuando sea titular, beneficiario, autorizado o con poder de disposición. Se precisa más el tipo de activo que interesa aludiendo a que ha de estar custodiado por personas o entidades que proporcionen servicios para salvaguardar claves criptográficas privadas en nombre de terceros o para mantener, almacenar y transferir las monedas virtuales.

Con alguna demora, el desarrollo reglamentario de la disposición vino de la mano del Real Decreto 249/2023, de 4 de abril, cuyo art. 3.9, incorpora, entre otros, un art. 42 quater en el Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento de las actuaciones y los procedimientos de gestión e inspección y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos (en adelante RGGIT).

El precepto citado presenta un amplio alcance subjetivo. La ley hace referencia a todo obligado tributario y el reglamento incluye a los establecimientos permanentes en esta categoría lo que parece seguir el apartado 3 del art. 35 de la LGT[7]. Así mismo, relaciona toda una serie de situaciones en las que un sujeto pasa a ser obligado del deber de informar (titular, beneficiario, autorizado o con poder de disposición) a las que añade el concepto de "titular real". Su

7. Esta idea no implica un exceso del reglamento por encomendar a una entidad que tiene más vocación de punto de conexión territorial, el realizar obligaciones formales. El art. 21 del Real Decreto Legislativo 5/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley del Impuesto sobre la Renta de no Residentes ya dispone que es el establecimiento permanente el que ha de presentar la declaración vinculada al tributo.

significado coincide con el previsto en el art. 4.2 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Ese artículo tiene, por un lado, una definición genérica de persona por cuya cuenta se pretenda establecer una relación de negocios o intervenir en cualesquiera operaciones y, por otro lado, unas más específicas relacionando el término con sujetos que controlan personas jurídicas o gestionan entidades como el fideicomiso en diversas variantes (*trust* inglés o *treuhand* alemán). Con todo se prueba que la intención del regulador no es la de ceñir la obligación formal al sujeto que puede ser potencialmente un obligado de prestaciones materiales, sino a todo aquel sujeto que de forma directa o indirecta pueda tener relación con monedas virtuales sitas en el extranjero.

Este sujeto ha de aportar información sobre un bien que tiene interés tributario: la moneda virtual. Adviértase que ni la LGT, ni el RGGIT utilizan el concepto de criptomoneda para identificar el objeto sobre cuyos extremos se ha de declarar, sino el mencionado. Para precisar más su definición, el RGGIT se remite a la ya citada Ley 10/2020 y a su art. 1.5 que define la moneda virtual con cinco características: a) es una representación digital de valor; b) no está emitida ni garantizada por autoridad pública; c) no está asociada necesariamente a moneda fiat; d) legalmente no tiene el carácter de moneda o dinero y e) es aceptada como medio de cambio entre particulares. Con respecto a este efecto se habrá de aportar anualmente la identificación del titular, de cada tipo de moneda virtual que posee y los saldos que pueda tener disponibles a 31 de diciembre expresados en unidades de moneda y valorados en euros. En cualquier caso, la obligación depende de que se superen conjuntamente los 50.000 euros y que, una vez realizada, haya una variación de saldo en años posteriores superior a 20.000 euros. La 'foto fija' de la situación sobre la que informar se realizará en esa fecha y la aportación de datos se llevará a cabo el primer trimestre del año siguiente[8].

La regulación expuesta invita a aportar algunas reflexiones siendo la primera que se limita a las monedas virtuales y no va más allá incluyendo otros criptoactivos.

La consecuencia es que el conocimiento sobre su existencia ha de quedar a expensas de otras obligaciones formales de declarar estos bienes a efectos tributarios (*ad exemplum*, cuando suponen una plusvalía para una persona física en relación con su Impuesto sobre la Renta de las Personas Físicas). Así mismo, no solo se excluye a otros criptoactivos sino también a las CBDC (*Central Bank Digital Currency*), si bien no representan una laguna informativa en tanto que se obtendrían datos desde las entidades emisoras. Esta exclusión se combina con la excepción (art. 42 quater. 5 RGGIT) de determinados sujetos de cumplir esta

8. Véase Orden HFP/886/2023, de 26 de julio, por la que se aprueba el modelo 721 «Declaración informativa sobre monedas virtuales situadas en el extranjero», y se establecen las condiciones y el procedimiento para su presentación.

obligación por razones de estar exentos *ex* art. 9.1 LIS o de figurar el bien convenientemente contabilizado.

La segunda reflexión es alrededor de la idea de valor en euros que ha de ser estimado el cual, debido a la inestabilidad del efecto, se antoja problemático. Según el reglamento, este dato se toma de la cotización que a 31 de diciembre ofrezcan las principales plataformas de negociación o sitios web de seguimiento de precios o, en su defecto, el obligado ha de proporcionar una estimación razonable del valor de mercado de la moneda virtual. La realidad pone a aquél frente al dilema de escoger entre una variedad de plataformas en las que se realizan transacciones con criptomonedas[9]. La cuestión es qué criterio (volumen de negocio, cotizaciones más bajas, medias o altas, cantidad de clientes, etc…) se considera aceptable para que la Administración se conforme con la valoración aportada, pues ¿puede rechazar la valoración por entender que la plataforma no es la adecuada? Pero, además, la capacidad de acción del obligado se cierra con la mención a la 'estimación razonable del valor de mercado' que habrá de justificarse y, por lo tanto, cabría debatirla. No se acaba de entender por qué se deja a la consideración del administrado el factor 'valor' (decisivo por otro lado por cuanto de él depende estimar las cuantías para estar sujeto o no a la obligación) cuando la realidad de las criptomonedas es semejante con la de otros valores como las participaciones en capitales ajenos. No compartirán naturaleza jurídica, pero se parecen en que estas pueden tener cotizaciones diferentes según las condiciones de los mercados en los que estén presentes. Sin embargo, aquí la solución pasa por facilitar por parte del Ministerio de Hacienda, según el art. 15 de la Ley 19/1991, de 6 de junio, del Impuesto sobre el Patrimonio, la cotización media correspondiente al cuarto trimestre del año.

Por último, está determinar un aspecto clave de este deber como es situar la moneda virtual en el extranjero. Este aspecto no deja de ser paradójico pues se trata de ubicar en un espacio físico un bien con sentido en un espacio virtual que prescinde de fronteras. El reglamento es conocedor de esta realidad y utiliza una alternativa. El punto de conexión territorial se determina porque el prestador de servicios no está en España y, por ende, no ha de presentar la declaración que regula la Disposición Adicional 13.6 de la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas (en adelante LIRPF).

Esta previsión traslada la atención a otra obligación de aportar información sobre monedas virtuales que regula ese precepto. Hay que atender a los apartados 6 y 7 de la Disposición Adicional 13 de la LIRPF. Con el deber que regulan se completan las posibilidades de obtención de información en materia de monedas virtuales, poniendo la atención esta vez en los prestadores de servicios

9. La página web https://coinmarketcap.com/ recoge las plataformas centralizadas y descentralizadas en las que pueden encontrarse cotizaciones de criptomonedas. Con fecha de 28 de mayo de 2024 se contrasta la cotización del Bitcoin en la plataforma Binance con 68.082'35 dólares y la plataforma Upbit con 69.695'68 dólares.

residentes. Estos se identifican con personas, entidades o establecimientos permanentes que realicen diversas tareas relacionadas con las monedas virtuales (salvaguarda de claves criptográficas en nombre de terceros, mantenimiento, almacenamiento o transferencia de monedas, servicios de cambio entre monedas u ofertas iniciales de nuevas monedas virtuales). Sobre aquellas han de suministrarse tanto datos relativos a saldos por tipo de moneda y sus titulares, como sobre operaciones que se realicen con las mismas y los sujetos intervinientes.

Con los arts. 39 bis y 39 ter, incorporados en 2023, el RGGIT desarrolla la disposición legislativa descrita[10]. Del primer precepto se deriva que la obligación de informar de los obligados será anual y se prevé el 31 de diciembre como la fecha en la que se fija la situación correspondiente. La información será sobre la identificación de los que disponen de los saldos de los que, a su vez, habrán de especificarse tipo de moneda, número y su valoración en euros. Sobre esta cuestión, la norma sigue la misma pauta que se ha descrito para el art. 42quater.3 RGGIT por lo que pueden traerse aquí los comentarios realizados.

El segundo artículo impone el deber anual de informar a los sujetos (también personas y entidades residentes o establecimientos permanentes en España) que prestan servicios para operar con monedas virtuales (cambios entre monedas, intermediación, salvaguarda de claves, etc…) excluyendo a los que se limiten a una tarea de asesoramiento, de puesta en contacto entre partes interesadas o atención de órdenes de cobro y pago. La información ha de identificar a los sujetos que intervienen en la operación, el tipo de operación, la fecha, el tipo y número de unidades de la moneda virtual utilizada, su valor y gastos y comisiones asociados a la operación. El apartado 3 concreta la obligación para las entidades que realizan ofertas iniciales que completarán una declaración informativa anual sobre las entregas que efectúen de la moneda ofrecida a cambio de otras monedas virtuales o dinero fiat, siendo sustituidos en la obligación si la oferta inicial la efectúa una entidad que presta servicios de intermediación.

El art. 39ter.2, tercer párrafo, RGGIT precisa que si existe contraprestación y el sujeto obligado a proporcionar información se relaciona con ella —lo que va desde satisfacerla o percibirla hasta el simple conocimiento de su existencia— ha de especificar si consiste en moneda fiduciaria, otra moneda o activo virtual, en bienes o servicios o una combinación de las anteriores. La norma, en este caso, muestra expresamente un interés sobre otros criptoactivos diferentes a las monedas virtuales, si bien no aclara qué es lo que se ha de informar (tipo, valor, cantidad, etc…). En este sentido puede cuestionarse si el reglamento no va más allá de lo que exige la ley si se atiene a que la Disposición Adicional 13.7 de la LIRPF, de forma resumida, obliga a informar al prestador de servicios sobre diferentes operaciones que van desde la adquisición a cobros y pagos, pasando

10. Los formularios para hacer efectiva la obligación se han regulado en la Orden HFP/887/2023, de 26 de julio, por la que se aprueban el modelo 172 "Declaración informativa sobre saldos en monedas virtuales" y el modelo 173 "Declaración informativa sobre operaciones con monedas virtuales", y se establecen las condiciones y el procedimiento para su presentación.

por transmisión, cambio o permuta. Sin embargo, el precepto reglamentario alude a informar también sobre la posible contraprestación (moneda fiduciaria, virtual, bienes o servicios) solo por el mero conocimiento de su existencia, lo que no queda claro qué significa exactamente o si dicha circunstancia se da por un conocimiento casual o expreso. En este punto, el reglamento no se ciñe a concretar la obligación de informar sobre aquellas operaciones en las que el prestador de servicios intervenga, sino que el mero hecho de estar al corriente de algo en lo que se es ajeno es causa de la obligación.

Fijando de forma sintética lo dicho hasta ahora, la aplicación de los tributos en relación con las criptomonedas ha causado el refuerzo del deber de informar. Como se ha visto, este se impone para monedas virtuales sitas en el extranjero y para operaciones con estos efectos en las que participan prestadores de servicios residentes. La conclusión inmediata es que se ha dejado al deber genérico de aportar información que pueda relacionarse con cada tributo (*ad exemplum*, la autoliquidación por IRPF) al obligado tributario cuando las monedas virtuales no son gestionadas a través de prestadores de servicios.

Pues bien, ya es conocido que los códigos de datos estructurados que soportan la moneda virtual pueden ser guardados en espacios denominados 'wallet'. Estos pueden estar conectados a Internet y gestionados a través de un prestador de servicios correspondiéndose con el objetivo del descrito deber de declarar. Pero también cabe que el monedero esté en el propio ordenador del usuario, se constituya con un dispositivo externo a modo de *flash drive* o que sea un monedero más tradicional impreso en papel con claves y direcciones con las que disponer de las monedas. Por lo tanto, en estos supuestos en que el usuario controla sus efectos de forma directa cabe preguntarse ¿cuándo están en el extranjero?, ¿quién custodia los saldos? o, si bien puede ser minoritario, ¿qué sucede si el usuario es el que realiza directamente las operaciones con terceros? Reiterando lo dicho, la respuesta es que la Administración, en estos casos, queda a expensas del cumplimiento genérico de informar que pueda tener todo obligado tributario.

El hipotético incumplimiento por su parte impedirá a la Administración tener conocimiento de estos bienes a lo que podrá reaccionar, como se puede suponer, ejerciendo sus funciones comprobadora e investigadora (art. 141 de la LGT). Para ello cuenta con diversas facultades *ex* art. 142 LGT, pudiendo relacionarse con este trabajo la posibilidad de examinar bases de datos informatizadas, programas, registros y archivos informáticos relativos a actividades económicas. Sin embargo, esta vinculación no es del todo clara en tanto las referencias a esos elementos están pensando en medios en los que se registran datos relativos a una actividad económica y no tanto al hecho de que los propios datos, como ocurre en el caso de los criptoactivos, sean elementos patrimoniales gravables. De forma paralela a lo dicho en la Introducción de estas líneas, los medios mencionados se relacionan con datos que son base del conocimiento, pero no con datos que, una vez estructurados, puedan ser considerados bienes muebles intangibles.

Este podría ser un argumento sobre la necesidad de incorporar expresamente a los 'monederos' o 'wallets' entendidos como espacios en los que almacenar criptoactivos que pueda manejar el obligado tributario, al conjunto de elementos a los que puede acceder la Administración en busca de riqueza oculta[11]. Mientras tanto, siguiendo una interpretación acorde con la realidad social del tiempo en que se aplica la norma, se acepta la legitimación de la autoridad tributaria a investigar estos espacios virtuales si se hace una interpretación amplia de la palabra "lugares" que aparece en el apartado 2 del art. 142 LGT desde el momento en que contienen "bienes sujetos a tributación".

La regulación de medidas cautelares que pueda adoptar la Inspección tributaria permite profundizar en lo que se está comentando. El art. 146.1 de la LGT establece, en su segundo párrafo, que cabe la incautación de equipos electrónicos de tratamiento de datos que puedan contener la información de que se trate. Esta formulación genérica permitiría a la Administración llevar a cabo una acción de intervención del 'wallet' que maneja el obligado. El art. 181 del RGGIT indica que el precinto es una de las medidas cautelares que pueden adoptarse, de forma que se ligaría con el correspondiente sello el equipo electrónico para un posterior depósito o incautación.

La Inspección puede proceder, por tanto, de manera que se apropie del elemento informático en el que se registran los criptoactivos. Pero esto es del todo insuficiente si no se accede a los datos que interesan y, en relación con esta acción, se plantean algunas cuestiones. La primera es, si se ha concebido el dispositivo como un 'lugar', ¿se requiere el consentimiento del obligado o un acuerdo de entrada de la autoridad administrativa que reglamentariamente se determine?, dado que los dispositivos son multifuncionales, si los datos que se hallan en él son tanto personales como de interés tributario ¿se ha de hacer honor a algún requisito como consecuencia de la vigencia de un derecho de la persona obligada?

Dando por hecho que no se cuente con el consentimiento del titular, responder afirmativa o negativamente a la primera pregunta pasa, necesariamente, por dar una respuesta a la segunda. El acceso a los dispositivos electrónicos que solo contengan datos que, siguiendo el art. 93 de la LGT, tengan trascendencia tributaria habrá de requerir el acuerdo de entrada citado. En cambio, si se hallan mezclados con aquellos que no tengan esa característica, sino que son de carácter personal, debiera contarse con la legitimidad que otorga la autorización judicial en tanto que se incide de forma clara en el derecho del sujeto a la intimidad personal protegida en el art. 18.1 de nuestra Constitución. Este desarrollo

11. La necesidad de actualización normativa en el ámbito de la Inspección para acoger la investigación sobre contenedores de códigos de datos estructurados sigue evidenciándose en el RGGIT. El art. 173.5 de este texto establece las facultades que tiene el personal inspector entre las que está verificar y analizar sistemas y equipos informáticos mediante los que se lleve a cabo, total o parcialmente, la gestión de la actividad económica. La obtención de datos como información de la actividad del sujeto investigado sigue siendo el factor que legitima la intervención, pero no el hecho de que el dispositivo informático sea depósito de bienes muebles intangibles.

evidencia otra necesidad de actualización o adaptación a una nueva realidad que demanda regulación, ampliando los supuestos del art. 113 de la LGT dedicado a fijar los extremos de la entrada en un espacio como es el domicilio en el que se desarrolla el derecho fundamental enunciado[12]. Se trata de extender la efectividad de los principios de finalidad justificada (regulación de la situación del obligado y determinación de la existencia de criptoactivos en el dispositivo), necesidad (no ha podido ser obtenida la información necesaria por ningún otro medio) y proporcionalidad (la incautación del dispositivo supone únicamente el volcado de información con trascendencia tributaria) hacia nuevos espacios en los que un sujeto puede almacenar tanto datos de carácter personal sin trascendencia tributaria como, facilitado por la tecnología, conjuntos estructurados de datos que funcionan como bienes muebles intangibles.

Las precauciones que estas líneas defienden que habría que adoptar ante un dispositivo de almacenamiento han de considerarse ante una variante posible. Lógicamente, en el art. 113 de la LGT el legislador no está pensando en los dispositivos electrónicos a la hora de obtener la información que contienen sino, más bien, en un concepto tradicional de domicilio. En este sentido, la Administración tributaria puede obtener la autorización de entrada, adoptar medidas cautelares y precintar los dispositivos electrónicos, pero ¿es extensible la autorización judicial obtenida a los dispositivos electrónicos que se hallen en su interior? Obviamente, no cabe duda de que sí con el consentimiento del obligado tributario, pero ¿qué ha de suceder si este no se produce? Es más, si no es así, ¿puede sancionarse el comportamiento tipificándolo como infracción por resistencia y obstrucción, excusa o negativa a las actuaciones de la Administración tributaria siguiendo el art. 203 de la LGT?

Puede ser una respuesta el considerar que una vez incautado el bien dentro del domicilio y tras un registro del espacio que supone en virtud de autorización judicial, el equipo informático puede ser fuente de información a la que acceder inmediatamente. A todo ello cabría añadir que, dado que estamos ante el desa-

12. Sobre esta cuestión la STS 1207/2023 de 29 de septiembre (ECLI:ES:TS:2023:3978) proyecta alguna luz. De ella se deriva la tesis de que es trasladable la protección del domicilio mediante autorización judicial ante la entrada de la Inspección al dispositivo informático en la medida en que, sin previo conocimiento de su contenido, pudiera tener datos personales sin trascendencia tributaria. Se ha de reiterar, en este sentido, que ante la circunstancia de diferente calidad de los datos, distinguiendo entre personales y económicos, insiste en que la Administración, sin mediar consentimiento, solo pueda obtener aquellos en los que pueda basarse la determinación de la situación tributaria del obligado. Sobre la misma cuestión ha de citarse también la STS 549/2024 de 4 de abril (ECLI: ECLI:ES:TS:2024:1876) en la que hay un paralelismo del problema analizado, pero con cajas de seguridad. En este caso, el juzgador entiende que no se requiere la obtención previa de autorización judicial para su apertura, si bien se han de controlar *ex post* el cumplimiento de principios de proporcionalidad, idoneidad y necesidad. Sin embargo, en el Fundamento Jurídico Sexto, número 11, el tribunal marca diferencia por lo que hace a dispositivos electrónicos que cumplen funciones de almacenaje en tanto que *"(…) plantean ya cuestiones relacionadas con los derechos fundamentales ligados al llamado entorno digital o, en su caso y por servir de comunicación, plantean ya la sujeción a la garantía del artículo 18.3 de la Constitución"*.

rrollo de un procedimiento aplicativo de tributos, que no sancionador, no se requieren mayores precisiones pues lo admite la flexibilidad de los derechos fundamentales que puedan estar en juego —los del art. 18.2 de la CE encarnado en inviolabilidad del domicilio— ante un deber de contribuir.

Sin embargo, a poco que se levante la vista del ordenamiento tributario se observa que el legislador evoluciona en el sentido de que no es implícito en el permiso judicial a entrar en el domicilio el acceso a la información de los dispositivos electrónicos que en él se hallen. La Ley de Enjuiciamiento Criminal acoge en su seno medidas entorno a la incautación y obtención de información desde dispositivos electrónicos. Los arts. 588 sexies a) a 588 sexies c) de esa norma prevén la necesidad de autorización judicial para el acceso a la información que contengan los dispositivos electrónicos. Esta ha de ser individualizada para el caso de que se prevea, con la entrada en el domicilio, la aprehensión de dispositivos de almacenamiento masivo o cuando el dispositivo sea incautado fuera de aquel.

La cuestión inmediata es si la legislación dirigida hacia la actuación policial en su tarea de investigación criminal se puede trasladar *pari passu* a la tarea de investigación que para la regularización de la situación tributaria realiza la Inspección. La diferencia del objetivo de ambos procesos podría justificar la actual situación de necesaria precisión en el primer ámbito y de mayor laxitud para situación similar en el segundo. Sin embargo, el aspecto afectado en ambos casos es el mismo: el conjunto de derechos del art. 18 de la CE que confluyen en el dispositivo informático. El carácter inquisitivo del proceder de la autoridad pública en ambos casos es de la misma entidad, pues se pretende obtener información sobre la que basar un proceder y resolución y su finalidad no habría de considerarse como un condicionante a exigir más o menos precauciones a la hora de proteger derechos considerados fundamentales.

La legislación tributaria, en comparación, no es tan completa y requiere de una precisión que ha sido afrontada por otras áreas del Derecho como es la ley procesal criminal. La carencia normativa no se justifica por una calidad no punitiva del procedimiento de investigación tributario que pueda desarrollarse flexibilizando derechos fundamentales como los apuntados o su síntesis en un derecho del obligado tributario a un entorno digital seguro. Un derecho de nueva generación que sintetiza domicilio, datos personales, intimidad o secreto de las comunicaciones en tanto que en un dispositivo informático como una memoria USB, un portátil o la propia nube pueden almacenarse desde datos personales hasta información sobre comunicaciones e, incluso —con la novedad de los criptoactivos— bienes[13]. En definitiva, un derecho a contar con un espa-

13. Hay que aclarar que esta tesis no es un llamamiento a la idea de que la normativa procesal criminal sea supletoria en el ámbito tributario siguiendo un art. 7.2 de la LGT. En este precepto se completan las fuentes del Derecho tributario con la supletoriedad de las disposiciones generales del derecho administrativo y los preceptos del derecho común. No abarcan estas dicciones a la ley procesal criminal lo que, junto a un principio de *lex specialis*, obstaculizaría aplicar sus precauciones al ámbito tributario.

cio virtual seguro en el que la persona pueda desarrollarse sin injerencias no legitimadas de acuerdo con el ordenamiento jurídico. Con esta referencia, habría de hacerse extensible la exigencia de conveniente autorización judicial al acceso de los datos que contenga un dispositivo electrónico[14] y, a raíz de ello, afrontar una reforma de la normativa tributaria.

Resumiendo lo hasta ahora dicho, se observa que hay iniciativas normativas en relación con los criptoactivos, cuando de obtener información sobre criptomonedas se trata. Conseguirla se basa en reforzar los deberes de información de sujetos y plataformas[15]. Sin embargo, se advierten insuficiencias en dos puntos[16]. Por un lado, la falta de ambición en el objeto de información en tanto que se concentra legalmente en las criptomonedas y no hace mención expresa a criptoactivos. Por otro lado, la obtención de información se basa en la intervención de intermediarios o en el propio obligado, pero no abarca de forma precisa la situación que puede darse en la que los bienes están contenidos en un dispositivo informático con la potencial afección de derechos fundamentales.

Hasta aquí se ha comentado que la tributación por criptoactivos demanda la proporción de información y que la actual regulación para obtenerla avanza pero precisa de adaptaciones. Ahora se pone la atención en cómo la normativa

14. Esta autorización habrá de ser solicitada a los Juzgados de lo Contencioso-administrativo siguiendo el art. 8.6 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

15. Las primeras declaraciones de contribuyentes han de ser presentadas, por lo que hace a monedas virtuales en el extranjero entre el 1 de enero y el 31 de marzo de 2024 siguiendo la Orden Ministerial HFP/886/2023 de 26 de julio que aprueba el modelo 721. Durante el mes de enero habían de presentarse los modelos 172 y 173 sobre saldos en monedas virtuales y operaciones con monedas virtuales según Orden Ministerial HFP/887/2023 de 26 de julio.

16. El fenómeno de los criptoactivos no se concentra solo en el hecho de situar e identificar fuentes de información o ejercer facultades de una manera más o menos restrictiva cuando los dispositivos se sitúan en el territorio nacional. La naturaleza de esos bienes intangibles tiene un elemento esencial que la caracteriza como es la ausencia de un espacio físico y tradicional para su ubicación. Su carácter intangible tiene sentido en un espacio en el que hay ausencia de fronteras y, por tanto, puntos de control que permitan aprehenderlos. Es evidente la necesidad de una cooperación internacional en este campo que se encarna en la iniciativa adoptada por la OCDE con los documentos *Marco de intercambio de información sobre criptoactivos y modificación del estándar común de intercambio de información* aprobado el 26 de agosto de 2022 y *Normas internacionales de intercambio automático de información en materia fiscal. Marco de intercambio de información sobre criptoactivos* de 8 de junio de 2023. España se ha comprometido, junto a otros 47 países, a la oportuna adaptación de la normativa al ordenamiento interno el 10 de noviembre de 2023 (Consúltese https://www.hacienda.gob.es/Documentacion/Publico/NormativaDoctrina/Tributaria/Acuerdos%20de%20Intercambio%20de%20Informaci%C3%B3n/Declaracion-conjunta-criptoactivos-CARF.pdf (última consulta 9 de abril de 2024) y se prevén los primeros cambios normativos para 2027. A su vez, esta iniciativa es origen de la acción de la UE a través de la Directiva 2023/226 de 17 de octubre de 2023 por la que se modifica la Directiva 2011/16/UE relativa a la cooperación administrativa en el ámbito de la fiscalidad incorporando un art. 8quinquies relativo al intercambio de información tributaria en materia de criptoactivos. En ambos casos hay una apuesta por el intercambio automático de información que han de procurar obtener los prestadores de servicios relacionados con criptoactivos de los usuarios o clientes.

de aplicación de tributos acoge a los conjuntos estructurados en determinadas áreas.

3. EL CONJUNTO ESTRUCTURADO DE DATOS COMO BIEN MUEBLE INTANGIBLE A EFECTOS TRIBUTARIOS: GARANTÍA DE LA OBLIGACIÓN TRIBUTARIA, VALORACIÓN Y PRUEBA

Los activos digitales basados en conjuntos estructurados de datos se han incorporado al patrimonio de los sujetos como un elemento gravable más. El epígrafe anterior ha girado en torno a conocer su existencia y extremos resaltando algunas carencias normativas y en este apartado ha de darse otro paso. Concretamente, se ha de dar respuesta a la cuestión de si el criptoactivo es un bien mueble intangible gravable ¿puede ser constituirse como garantía de la obligación tributaria? y, en su caso, dada su posible inestabilidad ¿cómo se gestiona el tema del valor? a lo que hay que añadir ¿cómo se prueban las circunstancias que rodean al bien?

3.1. El conjunto estructurado de datos como garantía del crédito tributario

En la normativa tributaria son diversas las ocasiones en las que se alude a la presentación de garantías relacionadas con tal o cual procedimiento. Como ejemplos pueden citarse el art. 65.3 junto con el 82 de la LGT para las deudas aplazadas o fraccionadas, el art. 224.2 para la suspensión de la ejecución del acto administrativo-tributario recurrido en reposición o el art. 233, apartados 2 a 5 de la misma ley por lo que hace a la suspensión de la ejecución del acto impugnado en vía económico-administrativa. En estas normas, el legislador muestra una clara preferencia por determinados tipos de garantía de la obligación tributaria. Los preceptos coinciden en prever el aval solidario de entidad de crédito o sociedad de garantía recíproca o el certificado de seguro de caución como mejor medio de asegurar el cumplimiento de la obligación. Los referidos a la suspensión aluden también al depósito de dinero o valores públicos. En su defecto, pueden admitirse otras como la hipoteca, la prenda, la fianza personal y solidaria o, incluso, otra que se estime suficiente de acuerdo con el desarrollo reglamentario.

La cuestión para contestar es si los conjuntos de datos estructurados pueden desempeñar esta función de garantía. La respuesta ha de partir de una realidad y es que el criptoactivo, como ya se ha comentado, hace alusión a una categoría de bienes que pueden tener diferente naturaleza. El activo mueble intangible que se estructura a través de un código de datos puede tener las características que la persona que los crea considere oportunas. En este sentido, cabe que sean

representaciones de la realidad o creaciones digitales a modo de NFT, cabe que sean representaciones de activos financieros como pueden ser las acciones de una corporación o, quizá siendo la forma más conocida, medios para el intercambio de bienes o servicios aceptados como dinero. En consecuencia, habrá que estarse a la naturaleza de cada activo digital para poder considerar su utilidad como garantía de una obligación tributaria.

El hecho de que el criptoactivo se constituya con un conjunto estructurado de datos no es impedimento para dejar de considerar la naturaleza del bien jurídico que soporta y, por ende, comprender su viabilidad para afectarlo al pago de créditos mediante el mecanismo garantista oportuno. Naturalmente, y como no puede ser de otra manera, habrá de estarse a la regulación propia de cada garantía para ver si es posible su constitución. Esta afirmación, no obstante, no ha de apartar la vista de la idea de que entre los criptoactivos se diferencian dos tipos. Primero, aquellos que soportan bienes, derechos o valores tradicionales (por ejemplo, participaciones en capitales de personas jurídicas o valores que representen su cesión a terceros) para los que no habrá más que seguir la normativa aplicable en torno a la constitución de garantías. Segundo, los que, constituyendo la novedad, representen nuevas formas de bienes en sí mismos (por ejemplo, criptomonedas o NFT) y para los que hay que hacer alguna consideración.

Una de las garantías mencionadas anteriormente es el depósito de dinero y valores públicos (vid. art. 224.2.a) o 233.2.a) de la LGT). No parece que, en este caso se puedan albergar dudas de que los criptoactivos no son viables, en cualquier caso. Por lo que hace al dinero, entre los activos digitales se encontrarían la criptomoneda la cual, siguiendo el art. 1.5 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, se identifica con *"(…)representaciones digitales de valor no emitidas ni garantizadas por un banco central o autoridad pública, no necesariamente asociada a una moneda legalmente establecida y que no posee el estatuto jurídico de moneda o dinero, pero que es aceptada como medio de cambio y puede ser transferida, almacenada o negociada electrónicamente."* El no reconocimiento legal como dinero *fiat* de ese tipo de bienes impide plantear que se ofrezcan en depósito para los fines previstos en la norma. Así mismo, por lo que hace a los valores, se ha de considerar que si bien los criptoactivos podrían ser el sustrato que representase este tipo de efectos, el hecho de que deban ser públicos extiende el impedimento anterior a este elemento. No obstante, la versatilidad de estos bienes y su tecnología no impiden que lleguen a ser utilizados por las autoridades para representar dinero de curso legal o los valores mencionados. Piénsese en las ya citadas más arriba *Central Bank Digital Currencies* en tanto que se identifican con dinero de curso legal o la posibilidad de que se lleguen a representar los títulos valor públicos mediante la tecnología propia de los criptoactivos. En estas situaciones, dada la oficialidad y reconocimiento jurídico de los elementos, no habría obstáculos a presentarlos como garantía a los efectos oportunos.

Para los criptoactivos privados que son bienes en sí mismos se analiza si la hipoteca mobiliaria o la prenda son las garantías con las que se pueden relacionar. Centrando la atención en la primera y dada la naturaleza de bien mueble del activo digital parecería que no hay impedimento a que se relacionen ambos conceptos. El obligado, ante la imposibilidad de presentar las garantías que expresamente recoge la normativa citada, podría constituir una hipoteca sobre sus criptoactivos con el fin de obtener el aplazamiento o la suspensión. Ahora bien, de acuerdo con lo dispuesto en el art. 82.1 segundo párrafo o el art. 233.3 de la LGT ha de ser la Administración la que estime la suficiencia de la garantía presentada. Siguiendo el art. 48.4 del Real Decreto 939/2005, de 29 de julio, por el que se aprueba el Reglamento General de Recaudación (en adelante RGR) el principio de suficiencia tiene una doble vertiente: cuantitativa o económica y normativa o jurídica. Es en este último punto en el que se observa un obstáculo dado que, siguiendo el art. 12 de la Ley de 16 de diciembre de 1954 sobre hipoteca mobiliaria y prenda sin desplazamiento de posesión, solo pueden ser hipotecados determinados bienes[17] entre los que no se encuentran los criptoactivos. Sea por una razón histórica o de adecuación, no se ha previsto que los conjuntos estructurados de bienes puedan ser objeto de una hipoteca mobiliaria por lo que el juicio de la Administración tributaria sobre la suficiencia jurídica habrá de ser negativo.

Dado que la hipoteca presenta problemas de inadecuación por razones legales, se abre el camino de la prenda como derecho real de garantía en favor de la Administración tributaria. Siguiendo el art. 1864 del CC. está puede constituirse en relación con *"(…) todas las cosas muebles que están en el comercio, con tal que sean susceptibles de posesión."* Esta garantía, siguiendo el art. 1866 del CC. es susceptible de ser retenida por parte del acreedor hasta el pago del crédito y, según el art. 1867 del CC. este debe comportarse diligentemente en el cuidado y conservación de la cosa. Junto a la prenda con desplazamiento descrita, está la regulada por los arts. 52 a 66 de la Ley de 16 de diciembre de 1954 que permite que el pignorante conserve la posesión de la cosa en determinadas circunstancias.

En relación con los criptoactivos, dado su carácter de bienes muebles intangibles, no parece que existan problemas de índole jurídica para considerar viable la garantía pignoraticia. Si bien no es un elemento físico, sí que es, dentro de la red, trasladable de un punto a otro. No obstante, es necesario hacer preci-

17. Según el precepto únicamente podrán ser hipotecados: a) los establecimientos mercantiles, b) los automóviles y otros vehículos de motor, así como los tranvías y vagones de ferrocarril de propiedad particular, c) las aeronaves, d) la maquinaria industrial y e) la propiedad intelectual y la industrial. No obstante, en este último caso, el hecho de que sean representables digitalmente obras originales sobre las que puedan ejercerse derechos por parte de la persona creadora y que se sustenten en la tecnología que constituye un criptoactivo (pensemos en obras digitales) puede ser una posibilidad, aunque singular, de constituir un derecho de hipoteca sobre un criptoactivo con el que se garantice una deuda tributaria.

siones sobre dos aspectos[18]. El primero es relativo a los conceptos de propiedad y posesión de los criptoactivos. Ambos irán vinculados cuando un sujeto o usuario se identifica a través de sus contraseñas en la red para gestionar y operar con los criptoactivos. Mediante ellas, el sujeto puede acceder al espacio virtual o físico (*hardware*) en el que estén los bienes y, de esa manera, ejercer las potestades dominicales que emanan de la propiedad sin interferencias de terceros. Para constituir la prenda, la posesión de los efectos no requiere la comunicación de los datos que constituyen las contraseñas de acceso a los espacios del sujeto, sino que se limitará a la transferencia de los efectos a los espacios que la Administración tenga habilitados para ello. Precisamente, el espacio para el depósito es el segundo aspecto para precisar. Este habrá de ser adecuado para este tipo de bienes habilitándose un sistema de hardware propio de la Administración, la propia Caja General de Depósitos a estos efectos o una entidad que preste servicios de caja. En relación con esto último destaca el art. 9.4.c) del RGR que establece que para los servicios de caja o como entidad colaboradora, al lado de las entidades de crédito (bancos, cajas de ahorro y cooperativas de crédito), estarán las entidades de dinero electrónico, las de pago o "c) Cualquier otra que se establezca por el titular del Ministerio de Hacienda". Esta última previsión abre la posibilidad de que aquellas entidades que presten servicios relacionados con los criptoactivos puedan desempeñar la función de entidad depositaria[19].

Las reflexiones en torno a los criptoactivos como garantía se completarían con una referencia a que el administrado no solo tiene la oportunidad de presentar una serie de garantías, sino también puede solicitar de la Administración que adopte medidas cautelares en sustitución (art. 82.1 de la LGT). Siguiendo la exploración que se está realizando hay que plantear si los criptoactivos pueden jugar algún papel en este caso. Del art. 81.4.b) de la LGT se extrae la posibilidad del embargo preventivo de bienes y derechos del que se practicará, en su caso, la anotación preventiva. Como se conoce, el embargo supone la retención de bienes propiedad del obligado tributario en un montante suficiente que cubra el pago del montante de la deuda. En este sentido, si se califican los conjuntos estructurados de datos como bienes muebles intangibles, no hay a priori impedimento a que pueda darse su traba y retención. No obstante, dada la coincidencia, algunos pormenores alrededor del embargo de estos bienes serán tratados más tarde.

---

18. La posibilidad que esquiva estas precisiones sería la de la constitución de una prenda sin desplazamiento. Pero los artículos 52 a 54 de la Ley de 1954, como ha sucedido con la hipoteca, no prevén que estos bienes estén entre los que pueden ser objeto de esta garantía. No obstante, esta afirmación no ha de conducir directamente a la conclusión de que no es posible una prenda sin desplazamiento sobre estos activos en el caso que puedan ser capaces de representar derechos que, como los de crédito, puedan ser pignorados.

19. En este punto la Administración tributaria ya tiene experiencia en tanto que es posible la pignoración de valores como las acciones. Estas ya no son títulos físicos, sino que son representadas mediante algo tan inmaterial como las anotaciones en cuenta que pueden ser depositadas en entidades financieras que realicen la función de custodia de valores.

3.2. Valoración del conjunto estructurado de datos a efectos tributarios

Un aspecto trascendental a la hora de tratar los criptoactivos y la aplicación de los tributos y que es una cuestión recurrente en este tema, es el de su valoración. No resulta ajeno entender que se trata de un hecho decisivo para la tributación del bien y la determinación de su gravamen; pero, como ya se ha comprobado antes por lo que hace a la identificación de los bienes como a la constitución de una garantía con su base, es una circunstancia importante por lo que hace al desarrollo de procedimientos tributarios.

La valoración de los conjuntos estructurados de datos es un tema complejo en tanto que depende de muchos factores a poco que se observen las plataformas en las que estos elementos cotizan. Deriva de factores internos como es la tecnología en la que se basan o en factores externos como el proyecto en que se encuadran. Así mismo, y por supuesto, el factor también depende de la naturaleza del producto que encarnan o de la propia ley de la oferta y la demanda. Añádase que también dependerá de si el criptoactivo representa un valor tradicional que está en un mercado consolidado o se trata de una criptomoneda que está respaldada por una entidad financiera u otro activo (*stablecoin*).

En cualquier caso, el legislador ha establecido algunas pautas para considerar qué valor atribuir para fines tributarios, a estos elementos. Volviendo a traer aquí el art. 39.2 bis del RGGIT se observa que es necesario traducir el valor de la moneda virtual a euros y para ello *"(…) los sujetos obligados tomarán la cotización a 31 de diciembre que ofrezcan las principales plataformas de negociación o sitios web de seguimiento de precios (…)"* en su defecto, han de proporcionar una estimación razonable del valor de mercado en euros en la misma fecha, indicando la cotización o valor utilizado. Por su parte, el art. 39ter.2 RGGIT indica que el valor de las operaciones con monedas virtuales ha de ser informado en euros si es en esa moneda como se valora la operación. Ahora bien, en caso de que la contraprestación no sea en moneda fiduciaria, se ha de tomar la cotización en las principales plataformas o se proporcionará una estimación razonable de forma paralela a lo que ocurren en el caso anterior. Es evidente que la regulación doméstica adolece de algunas imprecisiones, aunque no se han de achacar más que a la novedad que implica el bien que se está tratando. La primera, insistiendo en algo ya apuntado, es que solo abarca a las criptomonedas o monedas virtuales, lo que deja huérfanos de criterios a otros criptoactivos como los NFT. La segunda es que, como se dijo, se alude a conceptos como 'principales plataformas' o 'estimación razonable' que habrá de determinar y presentar el obligado y valorar y aceptar la Administración, lo que no habrá de darse necesariamente en cualquier caso.

En esta cuestión, desde la normativa europea y los trabajos de la OCDE se aproximan nuevos conceptos de la idea de valor. La Directiva 2023/2226 de 17 de octubre de 2023 por la que se modifica la Directiva 2011/16/UE relativa a la cooperación administrativa en el ámbito de la fiscalidad, conocida como DAC 8, aporta el art. 8bis quinquies. Este precepto utiliza dos conceptos de valor cuyo

uso depende de la operación que se realice. Cuando se trata de la adquisición de criptoactivos con moneda fiduciaria o su transmisión a cambio del mismo efecto, el valor a usar es el 'importe bruto agregado pagado o recibido'. Cuando se trata intercambio entre criptoactivos, operaciones minoristas o transferencias el valor se determina con el 'valor de mercado agregado'. Tanto el primer concepto, como el segundo se harán con referencia a la moneda fiduciaria. Ninguna de estas guías previstas para la métrica valorativa aparece definida en la directiva. Aproximarse a la primera lleva a identificarla con la totalidad de la contraprestación dada o recibida por el criptoactivo que se trate. La segunda, en cambio, vuelve a hacer una alusión al concepto de 'mercado' lo que conduce a repetir la reflexión anterior: estará claro el concepto si se trata de mercados tradicionales, pero no tanto el supuesto de conjuntos estructurados de datos cotizando en plataformas diversas.

La valoración de los conjuntos estructurados de datos deriva hacia otra cuestión como es que la Administración lleve a cabo una valoración de los bienes. Como es conocido, el art. 134.1 de la LGT regula la función de la comprobación de valores, estableciendo la facultad de la Administración de proceder a ello de acuerdo con los medios que explicita el art. 57 de la LGT. Ante la ausencia de una publicación oficial de valoraciones (la cual, como sea dicho, no debería desestimarse para casos futuros evitando controversias y reforzando la seguridad) la Administración puede establecer un valor de estos bienes basada en diferentes medios. La conveniencia de utilizar uno u otro para determinar el valor de los criptoactivos dependerá, lógicamente, de la naturaleza del bien que se esté considerando. Habrá aquellos conjuntos estructurados de datos que soportan bienes y derechos tradicionales (por ejemplo, participaciones en capital). Para estos, no habrá mayor problema que usar los métodos de valoración que normalmente se utilizan según el bien. Junto a ellos, estarán los nuevos bienes como las criptomonedas o los NFT que necesitan algún análisis detenido para su valoración pues se carece de publicaciones oficiales, pero sí de conceptos definitorios de necesaria interpretación.

Unos conceptos que, en cambio, no están en el art. 57 de la LGT. Este no prevé la valoración siguiendo 'principales plataformas de negociación o sitios web de seguimiento de precios', definiendo el 'valor razonable', estableciendo el 'importe bruto agregado' o el 'valor de mercado agregado', aspectos que la normativa deja al entendimiento del obligado y, en su caso, a la aceptación por la Administración. Esta, ante la ausencia de una adaptación del precepto a la nueva realidad que implican los bienes, puede acudir a métodos de aproximación de valores basados en los precios de medios en el mercado (art. 57.1.c) LGT), si bien este concepto puede ser difuso pues depende de varias plataformas como ya se sabe o, incluso, de las características del bien[20]. Consideraciones similares

20. En el Considerando 10 del Reglamento (UE) 2023/1114 de 31 de mayo de 2023 relativo a los mercados de criptoactivos, más conocido como MiCA, se hace el apunte de que el valor de los NFT depende de las características únicas de cada criptoactivo y a la utilidad que otorga al titular. Incluso,

pueden hacerse si el valor surge de cotizaciones en mercados nacionales y extranjeros (art. 57.1.d) LGT) pues se redunda en el problema de definir mercados. La valoración mediante un dictamen de peritos de la Administración (art. 57.1.e) LGT) es adecuado dadas las circunstancias en tanto que los especialistas podrían fijar un valor a estos efectos que se basase en una definición establecida sobre los conceptos con los que ha empezado este párrafo. Finalmente, puede utilizarse el precio o valor declarado correspondiente a otras transmisiones de este bien realizadas en el plazo de un año (art. 57.1.h) LGT) si bien no en cualquier caso si se atiende al art. 158.4 RGGIT. Para que el método sea viable, durante un año han de mantenerse circunstancias físicas, jurídicas o económicas lo que no se da, como ya se ha dicho, en el caso de las monedas virtuales por la volatilidad de su valoración.

La fijación de una metodología para la valoración, como se conoce, ha de estar motivada recogiendo la normativa aplicada y el detalle de su aplicación. En este sentido, está abierta a la controversia si se atiende al art. 135 de la LGT. Los interesados pueden promover una tasación pericial contradictoria para corregir los criterios que se hayan utilizado en la comprobación de valores. En tal caso, necesariamente habrá un peritaje de la Administración del bien en cuestión cuyo criterio podrá ser debatido, como se sabe, por el perito que haya designado el obligado y, en su caso, habrá de arbitrar un tercero. Sin embargo, aquí la cuestión es identificar qué competencias ha de tener la persona experta en los casos de bienes novedosos basados en conjuntos estructurados de datos, dadas las características tanto digitales como económicas que confluyen en ellos[21]. La dificultad de identificarla está solucionada expresamente para el caso del perito tercero, pues el precepto ya ofrece una solución a un posible vacío. De no existir colegio, asociación o corporación profesional competente, por la naturaleza de los bienes o derechos a valorar, o profesionales dispuestos a actuar como peritos terceros, se puede solicitar al Banco de España la designación de una sociedad de tasación inscrita en registro oficial.

La valoración de los criptoactivos, en general, es un tema que, a juzgar por las normas analizadas, se deja en manos de los obligados a informar o tributar a los que se da unos referentes normativos. Con su referencia habrán de dar un

---

cuando el criptoactivo representa servicios o activos físicos únicos y no fungibles como los bienes inmuebles es difícil determinar su valor. Si bien podrían negociarse en mercados, no se trata de bienes de fácil canje y su valor relativo no puede determinarse por comparación con un mercado existente o con un activo equivalente.

21. Sobre esta cuestión ANEIROS (2005: 16-17) exponía que*: "Así pues, serán las condiciones del bien las que determinen, a su vez, las condiciones que debe reunir el perito elegido para decidir la controversia. La práctica demuestra que normalmente se acude a arquitectos o arquitectos técnicos, cuando se trata de inmuebles urbanos, a ingenieros agrícolas o a ingenieros técnicos agrícolas, cuando se trata de inmuebles rústicos o forestales, o a economistas cuando se trata de negocios. Debe realizarse para ello un juicio de razonabilidad para acudir a aquel experto que mejor pueda decidir la controversia."* En el caso de criptoactivos ¿será un economista que fije los valores o también puede ser un informático en tanto hay que determinar el valor que derivan de las características digitales del bien o un sujeto en el que confluyan ambos campos de conocimiento?

resultado que es un elemento fáctico que, en cualquier caso, habrá de sustentarse en elementos probatorios de las circunstancias sobre las que se construye.

3.3. El conjunto estructurado de datos y la prueba

Sobre este tema es habitual recordar que la carga de probar unos hechos recae sobre el sujeto que tiene la intención de hacer valer su derecho (art. 105.1 LGT). Aquellos podrán ser acreditados mediante los medios admitidos en Derecho (art. 106.1 LGT). Entonces, ambas reglas habrán de ser aplicadas para el caso de los conjuntos estructurados de datos[22] y la prueba de las circunstancias que los rodeen como: a) sus titulares, b) cantidades y tipos de los que son propietarios, c) su valoración o d) las operaciones que con ellos se realicen.

La realidad de los diferentes extremos podrá ser presumida cierta si procede de las declaraciones, comunicaciones y demás documentos presentados por los obligados tributarios (art. 108.4 de la LGT), si bien no serán datos vinculantes para la Administración a la hora de realizar sus liquidaciones (art. 101.1 de la LGT). La certeza se extiende también a los datos que se incluyan en declaraciones o contestaciones a requerimientos de información en el marco de los arts. 93 y 94 de la LGT (recuérdese el deber de informar sobre monedas virtuales ya visto antes).

En este sentido, la puesta en conocimiento de los datos relacionados con los criptoactivos se realizará principalmente a través de los formularios que la Administración prevea a los efectos de cumplir con la obligación de declaración. Ello, no obstante, no es óbice para que no se dé un debate entre administrado y administración en relación con las circunstancias que rodean a un criptoactivos. En este sentido, reforzar la posición que sustente el obligado pasaría por presentar medios de prueba alternativos. Estos, por ejemplo, serían los documentos privados que podrían encarnar certificaciones de diferentes extremos emitidos por entidades relacionadas con los criptoactivos (art. 299.1. 3º de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, en adelante LEC). Estos documentos tienen fuerza probatoria plena en el proceso (art. 326 LEC), salvo impugnación por la parte perjudicada, lo que implica que el hecho, acto o estado de cosas que contenga el documento, así como su fecha y las personas que intervengan en ella serán ciertas (art. 319.1 LEC) a los efectos oportunos.

No obstante, hay precisiones para añadir en este apartado. Una entidad que haga funciones de intermediación puede emitir un documento privado en el que se dé constancia de los elementos anteriores. Pero esto no es obstáculo para que la libertad probatoria sea limitada por lo que hace a determinadas circunstancias relacionadas con la tributación de un criptoactivo. Esto se evidencia en el caso

22. En este sentido, se puede traer la consulta vinculante 975-22 de 4 de mayo. Hace alusión genérica a la prueba mediante medios reconocidos en Derecho a los efectos de valorar criptomonedas.

de que el objetivo sea probar su pérdida de valor. En este sentido son un ejemplo las Consultas Vinculantes 1979-15 de 25 de junio o la 2603-15 de 8 de septiembre. En la primera de ellas se pone de manifiesto que la pérdida por impago de una plataforma de inversión solo es asumible en el IRPF si es definitiva. Esto solo se considerará si media el carácter de crédito vencido y no cobrado, lo que depende de un procedimiento judicial de carácter concursal o ejecutivo cuyo resultado determina la imputación a un ejercicio determinado. En la segunda, la pérdida es producida por, según el consultante, una estafa por lo que presenta denuncia ante la Guardia Civil. La respuesta de la Administración es semejante a la anterior en tanto solo es imputable una pérdida en el momento en que el derecho de crédito resulte judicialmente incobrable. En consecuencia, en estos casos, la pérdida no se prueba tanto por declaraciones o documentos que pueda aportar el contribuyente como por el hecho de que, judicialmente, se considere inviable el cobro del crédito.

Un problema probatorio también puede sobrevenir por la pérdida de claves (por ejemplo, por un olvido o una pérdida de memoria del titular) o por su sustracción por un tercero que le permita ejercer las potestades de un propietario. Como se sabe, ese elemento resulta esencial a la hora de atribuir la titularidad a un sujeto determinado de los conjuntos de datos estructurados que pueda tener en un espacio virtual. A este respecto, podría evitarse un problema si se trata de supuestos en los que un prestador de servicios tiene mecanismos para que un cliente pueda reestablecer sus medios de acceso. Diferente, en cambio, si se trata de criptoactivos sobre los que el obligado tributario puede actuar sin intermediarios (recordemos los *wallet* dentro de memorias USB, por ejemplo). La pérdida de claves o de dispositivos implica la pérdida de los bienes muebles intangibles por lo que ¿cómo se prueba este hecho en el caso de que el obligado, en un momento previo, hubiera puesto en conocimiento de la Administración que poseía criptoactivos sobre los que ya no tiene posibilidades de acceso? En este sentido, recuérdese el art. 33.5 a) de la LIRPF cuando prevé que las pérdidas patrimoniales no justificadas no habrán de computar para la determinación de la base imponible del impuesto lo que, lógicamente, se relaciona con la prueba que ha de aportar el sujeto para justificar la pérdida. Esta circunstancia devuelve la cuestión al origen de este apartado: quien quiera ejercer su derecho habrá de probar los hechos sobre los que se sustenta por los medios admitidos en Derecho[23].

Con este apartado se han añadido a las reflexiones sobre la información en torno a criptoactivos cuestiones relacionadas con las garantías, la valoración y la prueba. Con el que sigue dedicado a la extinción de la deuda tributaria y los criptoactivos se completan las reflexiones que se ofrecen con estas líneas.

---

23. Esta afirmación discurre paralela a la Consulta Vinculante 3081/23 de 24 de noviembre cuando indica que para demostrar las pérdidas de juego se pueden utilizar los medios de prueba generalmente admitidos en Derecho, que habrán de valorar los órganos administrativos que correspondan. Criterio semejante es el que recoge la Consulta 1621/03 de 13 de octubre para el caso de probar pérdidas en relación con bienes inmuebles.

4. LA EXTINCIÓN DE LA DEUDA TRIBUTARIA MEDIANTE CÓDIGOS ESTRUCTURADOS DE DATOS

La obligación tributaria, como obligación de dar, se extinguirá principalmente mediante la entrega de bienes. El art. 60 de la LGT prevé que el pago de la deuda se efectuará en efectivo lo que se identifica, lógicamente, con moneda de curso legal. Por la remisión del precepto al RGR, estos pagos se pueden realizar mediante diversos medios como el cheque, la tarjeta de crédito, la transferencia bancaria o la domiciliación, además de otros que autorice el Ministerio de Economía y Hacienda.

Considerando el pago como medio de extinción cuando se cubre el montante de la deuda con el valor de la moneda entregada, la primera cuestión a resolver es qué ha de suceder con los criptoactivos que puedan equipararse a dinero desde un punto de vista económico. La respuesta negativa ha de ser inmediata por lo que hace a las criptomonedas que deriven de proyectos de emisión privados en tanto que no tienen, por lo menos en nuestro ordenamiento, reconocimiento como moneda de curso legal con la que puedan satisfacerse deudas tributarias. El matiz a una tan inmediata respuesta lo ponen aquellos bienes muebles intangibles que puedan identificarse con dinero *fiat* o CBDC (por ejemplo, un futuro euro digital[24]) pues es de presumir que tengan la característica de ser inmediatamente aceptables a estos efectos[25].

Las criptomonedas privadas y los criptoactivos en general no son medios con los que pueda extinguirse la deuda tributaria de forma directa e inmediata pues su entrega no equivaldría al pago mediante efectos considerados dinero. Ante este obstáculo se explora una alternativa basada en una idea de dación en pago de manera que, a modo de pago en especie (art. 60.1 LGT), pueda ser valorada. Sin embargo, con base en el art. 40 RGR se puede eventualmente rechazar esta opción ya que habría que contar con la valoración por parte del Ministerio de Cultura u órgano competente. En este sentido, solo en el supuesto de que el conjunto estructurado de datos ofrecido pudiera caer en los parámetros de ser un bien de interés, cabría plantear la extinción de la deuda tributaria para su entrega.

La cuestión de la extinción de la deuda tributaria mediante estos bienes muebles intangibles no tiene, al menos de momento y sin perjuicio de la apari-

24. A este respecto la Unión Europea ya cuenta con una Propuesta de Reglamento del Parlamento europeo y del consejo relativo a la prestación de servicios en euros digitales por parte de los proveedores de servicios de pago constituidos en Estados miembros cuya moneda no es el euro y por el que se modifica el Reglamento (UE) 2021/1230 del Parlamento Europeo y del Consejo COM(2023) 368 final.

25. Cabe añadir, en este sentido, que estas monedas permiten acciones como su trazabilidad por la autoridad central que las emite, su inhabilitación para su uso o su embargo en caso de impago de tributos. RONCO (2023: 132-134). Así mismo, según SÁNCHEZ (2024: 18), no ha de haber inconveniente en admitir este tipo de moneda para la extinción de la deuda tributaria en tanto que serán de curso legal.

ción de algunos que puedan ser viables para el pago, una respuesta positiva. Ello, no obstante, conduce a considerar la posibilidad de que se pueda dar una *cesio pro solvendo* de manera ejecutiva. En otros términos, se presenta que mediante el procedimiento ejecutivo de apremio se obtengan los bienes del deudor que, posteriormente, habrán de ser enajenados para que, con su producto, se cubra la deuda tributaria. En este sentido, recuérdese el art. 162.1 cuando indica que el obligado tributario debe poner en conocimiento de la Administración, si lo requiere, bienes y derechos integrantes de su patrimonio entre los que pueden estar, pues no se excluyen, los criptoactivos de los que sea titular.

Dentro del procedimiento de apremio, como es sabido, se puede producir el embargo de los bienes del contribuyente que se identifican con los relacionados en el art. 169.2 de la LGT. En primer término, habrán de hacerse efectivas las garantías lo que reconduce la atención hacia lo que se ha considerado más arriba en torno a ellas y los criptoactivos. En segundo término, se han de embargar bienes siguiendo el orden acordado entre Administración y administrado y, en su defecto, el que fija el precepto citado. En él, el dinero es lo que aparece en primer lugar —pues es más un bien recaudable que embargable— y, como se ha dicho, solo sería viable por lo que respecta a las criptomonedas equivalentes a dinero de curso legal. Por lo que hace a los otros bienes que se relacionan, pueden coincidir con lo que se representan mediante los códigos estructurados de datos (por ejemplo, títulos valor). La cuestión, en línea con lo tratado en otras ocasiones a lo largo del trabajo, se plantea para aquellos criptoactivos que son bienes no identificables con los tradicionales. Por supuesto que no ha de pensarse que esto los pueda hacer inviables para el embargo, en tanto que se reconocen como bienes muebles intangibles a los que se adjudica un valor (aunque de difícil determinación en ocasiones), lo que permite presumir que han de ser susceptibles de embargo y enajenación como cualquier otro bien del mercado. La cuestión es otra, por tanto, consistente en asimilarlos a los bienes que aparecen en el art. 169.2 de la LGT. Sería la categoría más cercana la de la letra h) del precepto que alude a bienes muebles de lo que resultaría, no obstante, que bienes como las criptomonedas o los NFT pudieran estar en las últimas posiciones de un listado que se organiza siguiendo un principio de fácil enajenación e inmediata liquidez. Esta reflexión podría ser la razón para introducir una modificación en el precepto por la cual se identificase y se situase en el orden de bienes la categoría de los criptoactivos[26].

Hay que advertir que esta línea de interpretación que acerca a los conjuntos estructurados de datos a los bienes muebles intangibles facilitando comprender su embargo no será pacífica para todos los casos. De acuerdo con la Consulta Vinculante de 2274-22 de 27 de octubre la venta de ilustraciones en formado

26. La Resolución de 6 de febrero de 2023, de la Dirección General de la Agencia Estatal de Administración Tributaria, por la que se aprueban las directrices generales del Plan Anual de Control Tributario y Aduanero de 2023 establece como objetivo que se potenciarán las actuaciones de localización de nuevos bienes susceptibles de actuaciones de embargo, con especial enfoque hacia los criptoactivos y monedas virtuales.

NFT constituye una prestación de servicios lo que aleja al activo del concepto de bien y, por ende, de la posibilidad de ser considerado embargable. Se puede tomar como una muestra más de la necesidad de ordenar normativamente los extremos en torno a los conjuntos estructurados de datos que funcionan como bienes cuando se insertan en los procedimientos tributarios.

Pero, en este caso, la problemática no es solo si el bien mueble intangible puede ser o no embargado o en qué orden, sino también llevar a cabo su previa traba. De forma básica, el embargo consiste en la identificación de determinados bienes del deudor y la afección al pago de una deuda que mantiene con el acreedor. En consecuencia, mediante su traba, el deudor ve limitada la disponibilidad de los bienes. Siguiendo el art. 170 de la LGT cada actuación de embargo ha de documentarse y notificarse convenientemente al obligado tributario o a tercero titular, poseedor o depositario. En el supuesto que los bienes sean susceptibles de registrarse en un Registro Público, la Administración puede contar con una anotación preventiva de embargo previo mandamiento al registrador. No hay que descartar que esta posibilidad se dé dada la versatilidad de los criptoactivos, pero sí hay que hacer una precisión. Si bien la tecnología en que se basan los criptoactivos es la de los Registros Distribuidos la cual, precisamente, facilita su singularidad y las transacciones, no pueden ser identificados con registros públicos y, por lo tanto, no cabe realizar anotaciones de embargo en sus registros.

Entonces, si bien la traba no podrá ser hecha en cualquier caso mediante una anotación preventiva, pues se carece de registro público, se han de explorar otras vías de acceso a los bienes para hacerla efectiva. En términos generales, el art. 76 del RGR disciplina la práctica de los embargos y, en su apartado 1, se encuentran indicaciones sobre esta cuestión. En primer término, el embargo se basa en el conocimiento de la Administración de la existencia del bien y su identificación lo que pasa con contar con la información necesaria a estos efectos. En segundo lugar, la Administración procede a la recaudación ejecutiva, personándose en el lugar en que se encuentren los bienes y dirigiéndose al obligado tributario o a tercero que sea dependiente o haga las funciones de depositario. En tercer lugar, los bienes habrán de quedar a disposición mediante su entrega a la Administración quien procederá a su enajenación de acuerdo con la normativa al efecto.

La LGT y el RGR desarrollan normativa específica para determinados bienes como el dinero, las cuentas bancarias, valores, salarios, inmuebles etc… En consecuencia, habrá de estarse a las disposiciones específicas que regulan la traba de esos bienes en el supuesto de que los criptoactivos se identifiquen con ellos. En el caso de que no exista identidad y se pueda categorizar el conjunto estructurado de datos acudiendo a su esencia de bien mueble intangible habrá que acudir a lo que dispone el art. 92 del RGR. Del precepto se desprende que la Administración se personará en el domicilio del obligado o en el lugar donde se encuentren los bienes. La cuestión que se origina aquí es que los criptoactivos que se traten estarán en el domicilio del obligado claramente si en él se encuentra el dispositivo electrónico que los almacene o se podrá acceder a ellos a

través del dispositivo correspondiente con el uso de las claves del usuario[27]. A continuación, habrá que proceder a la entrega de esos bienes lo que técnicamente habrá de pasar por, o bien, la transferencia por parte del obligado a los depósitos que pueda habilitar la Administración o a la entrega de las claves de acceso para que se pueda llevar a cabo la misma operación. Dadas las implicaciones que puede tener con respecto a la privacidad la entrega de claves, es más adecuada la segunda opción basada en la transferencia de los bienes a depósitos de titularidad administrativa adecuados a estos efectos (recuérdese lo ya dicho entorno al art. 9.4 RGGIT). Una variante sería, de forma paralela a lo que ocurre con las cuentas en entidades financieras, considerar que las plataformas gestoras de criptoactivos, cuando hacen la función de depósito, sean receptoras de los requerimientos administrativos lo que podrá ser viable directamente si están domiciliadas en España, pero que requerirá de aplicación de normativa sobre asistencia mutua si se encuentran domiciliadas en el extranjero.

Por lo que hace al depósito de este tipo de bienes, el art. 170.4 de la LGT se remite a la normativa reglamentaria para que la Administración pueda disponer de él. Según el art. 94 RGR, el órgano de recaudación competente designa el lugar para el depósito hasta la realización del bien. Si se trata de bienes que ya están en entidades de crédito u otras que ofrezcan garantías de seguridad y solvencia, seguirán depositados en ellas. En esta línea podrían situarse las entidades que prestan servicios en materia de criptoactivos y que cumplan las exigencias que marca el art. 62 del Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos para ser entidades autorizadas. Para el supuesto de no encontrarse en tales entidades, el apartado 3 del art. 94 indica una serie de recintos y locales físicos sin especificar uno expresamente acorde con la naturaleza digital de los conjuntos estructurados de datos. La solución vendría de modificar el precepto para contemplar este supuesto o, en su caso, comprender la posibilidad de que las entidades citadas antes puedan ser elegidas destinatarias a los efectos de depósito de los bienes muebles intangibles que constituyen los criptoactivos, sin perjuicio de que la Administración habilite sus propios espacios virtuales.

Tras la traba y el embargo llega el momento de la enajenación o de convertir los bienes muebles intangibles en dinero de curso legal para cubrir el montante de la deuda tributaria. Es lógico pensar que no hay una previsión expresa de cómo proceder en relación con estos bienes y que habrá de aplicarse a estos efectos la normativa que establece el RGR. No obstante, hay que advertir que la valoración de los bienes puede volver a suponer un problema a considerar en este punto. El art. 97.1 del RGR establece que son los órganos competentes de recaudación los que valoran los bienes a precios de mercado y de acuerdo con criterios habituales de valoración. No hay que extenderse en este tema y sea

27. En este sentido el Plan Anual de Inspección de 2023 hace alusión que se han de potenciar las actuaciones de localización de nuevos bienes susceptibles de actuaciones de embargo con especial enfoque hacia los criptoactivos y las monedas virtuales.

suficiente remitirse a lo ya tratado en materia de valoración del que se ha destacado que no es un tema sencillo dado que hay diferentes referentes para establecerlo.

Sobre los criptoactivos se han expuesto pareceres sobre cuestiones relativas a la investigación tributaria, las garantías, la valoración, la prueba y la extinción de la deuda tributaria siendo el momento de plantear conclusiones.

5. CONCLUSIONES

Primera: La combinación de diversas tecnologías como el registro descentralizado, la *blockchain*, la criptografía e Internet permiten en la actualidad dar un paso más en la utilización de los datos. De ser elementos sobre los que se construye el conocimiento pasan a ser conjuntos estructurados de datos a modo de bienes muebles intangibles o criptoactivos que pueden ser objeto de relaciones económicas. Desde ese momento son de interés para el Derecho tributario tanto desde la perspectiva del gravamen de las acciones económicas que con ellos se realizan, como desde la regulación de los procedimientos tributarios de carácter aplicativo.

Segunda: No se puede afirmar que los criptoactivos sean la causa para un replanteamiento de toda la materia tributaria relativa a ese aspecto. De hecho, la circunstancia de que sean códigos estructurados de datos que pueden sustentar o representar derechos, valores y bienes considerados tradicionales lleva a la conclusión que la normativa puede acogerlos sin alteraciones de calado. No obstante, sí que se sugieren cambios en estas líneas en diversos aspectos, sobre todo para aquellos bienes muebles intangibles de carácter novedoso de los que son una muestra las monedas virtuales o criptomonedas o los NFT.

Tercera: Esta modalidad de criptoactivos plantean algunas situaciones que no encuentran un encaje ajustado en el ordenamiento dedicado a la aplicación de los tributos. En algunos casos esto motiva que se incorpore nueva regulación como ocurre en el caso de los deberes de información en materia de criptoactivos. En otros casos no parece que haya reacción del legislador que, cabe pensar, espera a ver si un problema adquiere una determinada dimensión para actuar. Entre tanto, acoge el fenómeno con la normativa existente lo que necesita una lógica actividad exegética.

Cuarta: El ecosistema económico que se ha ido formando en torno a los conjuntos estructurados de datos ha tenido como característica singular el de la libertad individual y el de la privacidad, lo que ha dado lugar también a espacios de inseguridad desde un punto de vista jurídico. En este sentido, se introducen medidas para aumentar la transparencia de las acciones emprendidas de las que son ejemplo el incremento para los obligados tributarios de los deberes de información y la aportación de datos.

Quinta: El deber de información en materia de criptoactivos que, por el momento, se ha incluido en la normativa española se limita a una de sus manifestaciones: las monedas virtuales. Más concretamente, su titular ha de informar

sobre las que posea en el extranjero —lo que se determina en función de donde se sitúe el prestador de servicios— y los prestadores de servicios residentes sobre aquellos efectos que gestionen. Este especifico deber de informar no alcanza a otros conjuntos estructurados de datos como los NFT y tampoco a aquellos que puedan estar en dispositivos electrónicos individuales multifuncionales (ej: flash drivers).

Sexta: Los dispositivos electrónicos individuales multifuncionales presentan una problemática singular en tanto que pueden estar encuadrados dentro de un derecho individual y fundamental a un entorno digital sin intromisiones indebidas. En este sentido, se habría de garantizar, mediante la correspondiente autorización judicial, la efectividad de principios de finalidad justificada, necesidad y proporcionalidad en el acceso a información contenida en los citados dispositivos, asegurando la obtención únicamente de la que tenga trascendencia tributaria.

Séptima: La utilización de un conjunto estructurado de datos a modo de garantía de la obligación tributaria depende de qué bien representa. En este sentido, hay dos posibilidades. La primera es que sostenga bienes o valores tradicionales lo que llevará a que se constituya la garantía del crédito de acuerdo con su naturaleza y la regulación vigente. La segunda es que represente bienes novedosos (criptomonedas o NFT, por ejemplo) no previstos como bases de garantías reales de la deuda del obligado tributario. En ese sentido, la prenda es una garantía viable que podría constituirse con base en este segundo tipo de conjunto estructurado de datos, si bien habría de ser con desplazamiento y habilitando depósitos adecuados.

Octava: Un elemento que cruza todo este tema es el de la valoración se los conjuntos estructurados de datos caracterizado para algunos de ellos por su inestabilidad. Sobre esta circunstancia se ha encomendado al obligado la tarea de determinarlo haciendo uso de diversos referentes como cotizaciones en plataformas, valor razonable, importe bruto agregado o valor de mercado agregado. En este sentido, podría evitarse un potencial campo de conflicto optando por soluciones ya practicadas para otros efectos como es la de publicaciones oficiales de valores a efectos tributarios. Las medidas se piensan para dar seguridad al obligado tributario en esta novedosa materia ya que el funcionamiento de los códigos estructurados de datos como bienes muebles intangibles requiere de una serie de habilidades (por ejemplo, de conocimiento del entorno inversor o de las características técnicas del producto) de las que pueden disponer un cierto número de interesados, pero no el común de los obligados tributarios. Así pues, desde un punto de vista tributario, estas líneas abogan por una mayor implicación de las autoridades a la hora de marcar las pautas con las cuales la tributación de los bienes muebles intangibles sea pacífica proporcionando al obligado referentes claros tal y como ocurre con otros casos (por ejemplo, las cotizaciones medias de valores a efectos del IP o el valor de vehículos usados a los efectos de gravar su transmisión).

Novena: En relación con la prueba, podrán ser utilizadas las admitidas en Derecho entre las que se encuentran los documentos a modo de formularios por

los que el sujeto comunica unos datos que se presumen ciertos o los certificados que puedan emitir los prestadores de servicios sobre circunstancias como titulares, valores o tipo de bienes. No obstante, hechos como la pérdida de claves o el extravío de elementos que funcionen como depósitos de bienes son de difícil justificación debido a las estrictas exigencias legales vigentes.

Décima: Los conjuntos estructurados de datos no son directamente utilizables como medios de pago de la deuda tributaria ni cuando son monedas. Esta posibilidad queda condicionada a su admisión como moneda de curso legal. Otra cuestión es que constituyan pagos en especie, lo que también está restringido en nuestro ordenamiento a aquellos bienes sobre los que puede haber un interés público por sus características. Sin embargo, todo ello no es obstáculo para considerarlos bienes susceptibles de traba, embargo y enajenación mediante subasta. No obstante, los bienes muebles intangibles de carácter novedoso quedarían en una posición de embargo —salvo acuerdo con el obligado— alejada de considerarla en función de su liquidez o, incluso, fuera de su incautación ejecutiva si, como sucede con los NFT, se consideran como prestaciones de servicios.

Undécima: El fenómeno de los códigos estructurados de datos como bienes muebles intangibles ha venido para quedarse a juzgar por el interés que suscitan entre el público y las reacciones regulatorias que se están adoptando de las que es un ejemplo el Reglamento (UE) 2023/1114 de 31 de mayo relativo a los mercados de criptoactivos (MiCA). Es por ello por lo que, una apuesta para su desarrollo requiere regulación que dote de seguridad en los diversos ámbitos en los que inciden, entre los cuales está el tributario. No obstante, esta demanda no deja de ser una paradoja si se atiende al origen de las criptomonedas, representantes canónicos de los novedosos bienes. La libertad que las fundamenta basada en empoderar a los individuos ante autoridades financieras y administrativas, tras convertirse en instrumentos para la desaforada especulación o de operaciones fraudulentas, ha de delimitarse para no desvirtuar el desarrollo de los códigos estructurados de datos como un elemento más en la economía y entre las manifestaciones de riqueza.

BIBLIOGRAFÍA

ANEIROS PEREIRA, J (2005). El perito tercero como fórmula arbitral en el ámbito tributario, *Revista española de Derecho financiero*, *127*: 1-22.

BARRIO ANDRES, M. (2021). Concepto y clases de criptoactivos, en M. Barrio Andrés (dir.): *Criptoactivos. Retos y desafíos normativos*, (pp. 37-62), Wolters Kluwer.

BURLADA ECHEVESTE, J.L. (2020). Las garantías de la deuda tributaria, *Revista Quincena Fiscal*, *15-16:* 1-41

CAMPOS MARTÍNEZ, Y.A. (2023). *La tributación de los datos: ¿última distopía tributaria,* ed. Aranzadi, Cizur Menor.

CEDIEL, A. (2023). *Tributación 4.0: los criptoactivos*, ed. Tirant lo Blanch, Valencia.

CEDIEL, A. y Pérez Pombo, E. (2020). *Fiscalidad de las criptomonedas*, ed. Atelier, Barcelona.

CHAUM, D. (1983). Blind signatures for untraceable payments, en D. Chaum, R. L. Rivest, A. T. Sherman (eds): *Advances in Cryptology*, (109-203) Springer.

FERNÁNDEZ AMOR, J.A (2021). ¿Dónde está la moneda virtual? Comentarios a la modificación de la Disposición Adicional 18ª de la LGT, en Dtor. Merino Jara, I. y Coord. Suberbiola Garbizu, I. *Prevención y Fraude: nuevas medidas tributarias*, (457-492) Wolter Kluwer:

GALLEGO LÓPEZ, J.B (2022). El intercambio automático de información tributaria ante el reto de los criptoactivos, *Revista española de Derecho Financiero, 193*: 1-39.

GARCÍA CARACUEL, M. (2024). Avances en la normativa relativa al intercambio de información sobre operaciones con criptoactivos. La DAC como complemento a la CARF, *Quincena Fiscal, 7:*

GIL SORIANO, A. (2018). Monedas virtuales: aproximación jurídico-tributaria y control tributario, *Actualidad Jurídica Uría Menendez, 48*: 72-81.

HERENCIA ANTON, J. (2021). Fundamentos tecnológicos de los criptoactivos, en M. BarrioAndrés (dir.): *Criptoactivos. Retos y desafíos normativos*, (63-78), Wolters Kruwer.

MARIAN, OMRI Y. (2013). Are Cryptocurrencies 'Super' Tax Havens?, *Michigan Law Review First Impressions 38*, Available at SSRN: https://ssrn.com/abstract=2305863

MATA SIERRA, Mª T (2019). La dación en pago de la deuda tributaria: una necesaria revisión, *Revista española de Derecho financiero, 182*: 1-41

MIRAS MARÍN, N. (2024). La importante diferenciación entre criptomonedas y criptoactivos y su incidencia en las obligaciones de información, *Revista española de Derecho Financiero, 202*: 1-44.

MONTESINOS OLTRA, S. (2022). La pragmática incoherencia de la calificación de las criptomonedas a efectos tributarios. *Crónica Tributaria, 183*: 101-135.

NAVARRO CARDOSO, F. (2019). Criptomonedas (en especial, bitcoin) y blanqueo de dinero, *Revista Electrónica de Ciencia Penal y Criminología*, *21-14*: 1-45.

RUÍZ GARIJO, M. (2021). El desafío de la fiscalidad de las criptomonedas: las obligaciones de información en el IRPF, *Nueva Fiscalidad, 3*: 19-36.

SEDEÑO LÓPEZ, J.F (2020). El control tributario de las criptomonedas: calificación jurídica, localización geográfica y pseudoanonimato, *Nueva Fiscalidad, 1*: 207-233.

SÁNCHEZ JIMÉNEZ, M. (2024). El pago de la deuda tributaria por medios electrónicos: perspectiva ante el euro digital, *Revista Quincena Fiscal, 6*: 1-21.

La digitalización tiene un impacto significativo en la empresa, pues afecta a su organización interna, a sus relaciones laborales y a sus interacciones con terceros. Desde este punto de partida, este libro aborda preguntas como: ¿la digitalización repercute sobre las soluciones que plantea el Derecho a conflictos de intereses que surgen en la empresa?, ¿cómo se regula el teletrabajo?, ¿puede la empresa constituirse *online* en sociedad?, ¿dónde está a efectos legales si es de comercio electrónico o una plataforma de contenido audiovisual?, ¿qué sucede con los datos de consumidores?, ¿ha de responder civilmente si utiliza la inteligencia artificial en sus servicios, especialmente si es del sector sanitario?, ¿cómo afecta la regulación del mercado de productos digitales?, ¿se la apoya fiscalmente en el proceso de digitalización?, ¿la Administración tributaria usa la inteligencia artificial para perfilarla? o ¿cómo asumen los procedimientos administrativo-tributarios los nuevos bienes muebles intangibles o criptoactivos que puedan figurar en su balance? Estas páginas ofrecen rigurosas reflexiones sobre estos interrogantes con el objetivo de ayudar a la persona interesada en estos temas a comprender las relaciones entre Digitalización, Empresa y Derecho.

ISBN 978-84-10174-99-3

www.atelierlibrosjuridicos.com